EUROPÄISCHE UNION
Europäischer Fonds für
regionale Entwicklung

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Matthias Hartmann (Hrsg.)

IT-SICHERHEIT FÜR HANDWERK UND MITTELSTAND

Empfehlungen zur Digitalisierung

Handwerkskammertag
Land Brandenburg

Handwerkskammer
Berlin

IHK Industrie- und Handelskammern
in Berlin-Brandenburg

Berliner
Wissenschafts-Verlag

Matthias Hartmann (Hrsg.)

IT-SICHERHEIT FÜR HANDWERK UND MITTELSTAND

Empfehlungen zur Digitalisierung

BWV • BERLINER WISSENSCHAFTS-VERLAG

EUROPÄISCHE UNION
Europäischer Fonds für
regionale Entwicklung

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Hinweis: Sämtliche Angaben in diesem Fachbuch/wissenschaftlichen Werk erfolgen trotz sorgfältiger Bearbeitung und Kontrolle ohne Gewähr. Eine Haftung der Autoren, des Herausgebers oder des Verlags aus dem Inhalt dieses Werkes ist ausgeschlossen.

Markgrafenstraße 12–14, 10969 Berlin,
E-Mail: bwv@bwv-verlag.de, Internet: http://www.bwv-verlag.de

Druck: docupoint, Magdeburg
Gedruckt auf holzfreiem, chlor- und säurefreiem, alterungsbeständigem Papier.
Printed in Germany.

Herstellung: EFRE-Projekt: Digital Value Anwendungszentrum Hochschule für Technik und Wirtschaft (HTW) Berlin

Redaktionsschluss: Oktober 2017

ISBN Print: 978-3-8305-3820-2
ISBN E-Book: 978-3-8305-2980-4

Vorwort des Herausgebers

Matthias H. Hartmann
Hochschule für Technik und Wirtschaft (HTW) Berlin

Anlass für die Herausgabe dieses Buches war der 6. IT-Sicherheitstag Mittelstand am 14. September 2017 an der Hochschule für Technik und Wirtschaft (HTW) Berlin. 190 Teilnehmer aus Berlin und Brandenburg hörten die Fachvorträge, erlebten die Vorführungen zum Livehacking und besuchten die Ausstellungen von renommierten Anbietern und Start-ups rund um das Thema IT-Sicherheit. Die positive Resonanz der Teilnehmer war Motivation, die Erkenntnisse des 6. IT-Sicherheitstag Mittelstand 2017 in einem Buch zu verdichten.

Dieses Buch basiert auf der sehr guten Zusammenarbeit zwischen den Handwerkskammern (HWK) sowie Industrie- und Handelskammern (IHK) aus Berlin und Brandenburg, der Zentralen Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt Berlin und der Hochschule für Technik und Wirtschaft (HTW) Berlin. In einem von der Europäischen Union geförderten Projekt (EFRE) unterstützt die HTW Berlin insbesondere Kleine und Mittlere Unternehmen sowie Handwerksbetriebe bei der Digitalisierung ihrer Geschäftsmodelle und Geschäftsprozesse. Der Herausgeber ist gleichzeitig Projektleiter des als „Digital Value Anwendungszentrum" bezeichneten Unterstützungsangebots. Dieses Buch soll ein Nachweis für die fruchtbare Zusammenarbeit anwendungsorientierter Forschung an einer Hochschule mit der Praxis insbesondere kleiner und mittlerer Unternehmen sein. Die Handwerkskammern sowie die Industrie- und Handelskammern leisten hierbei wertvolle Koordinationsarbeit zwischen Hochschule und Unternehmen.

Das vorliegende Buch ist grundsätzlich in vier Teile gegliedert. In den ersten Beiträgen geht es um die IT-Sicherheitstage im Allgemeinen und den 6. IT-Sicherheitstag Mittelstand 2017 im Besonderen. Im anschließenden Teil werden Gefährdungspotenziale aufgezeigt und Warnhinweise gegeben. Der folgende Teil beschäftigt sich im Schwerpunkt mit Checklisten und Regelungen.

Abschließend stellen Autoren Unterstützungsangebote für Kleine und Mittlere Unternehmen sowie Handwerksbetriebe vor.

Die einzelnen Beiträge sollen insbesondere Kleine und Mittlere Unternehmen sowie Handwerksbetriebe ansprechen. Lesbarkeit und Informationsgehalt sollen im Vordergrund stehen. Auf ein technologisches Schaulaufen oder die Präsentation möglichst komplexer IT-Sicherheitsprojekte wurde verzichtet. In diesem Sinne soll das Buch zum Stöbern anregen, um Anwendungsmöglichkeiten für die Cyber-Sicherheit in den Betrieben zu finden.

Abschließend ist es dem Herausgeber ein Anliegen, den vielen Autoren für ihre schnelle Reaktion im Nachgang des 6. IT-Sicherheitstags am 14. September 2017 zu danken. Alle Beiträge wurden in der vereinbarten Zeit geschrieben, sodass das Buch noch 2017 erscheinen konnte. Damit verbunden sei auch der Dank an den Berliner Wissenschafts-Verlag.

Für den Druckkostenzuschuss sei der Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg und der Handwerkskammer Berlin gedankt.

Letztlich sei meinem Team für den Dauereinsatz rund um den 6. IT-Sicherheitstag gedankt. Namentlich sind dies meine wissenschaftlichen Mitarbeiter Frau Diplom-Kauffrau (FH) Madlen Böer, Herr Leonhard Gebhardt (M.A.) und Herr Ralf Waubke (M.A.) sowie meine studentischen Mitarbeiter Herr Tim Bodung und Herr Nils Halecker. Ein besonderer Dank geht an Herrn Leonhard Gebhardt, der die Tagungsorganisation und die Buchredaktion verantwortete.

Berlin, im Oktober 2017 Prof. Dr. Matthias Hartmann

Grußwort

Uwe Hoppe, Hauptgeschäftsführer
Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg

Das Thema IT-Sicherheit bekommt einen immer höheren Stellenwert. Insbesondere gilt das für die Themen Industrie 4.0 und Handwerk 4.0, natürlich für die Wirtschaft insgesamt, jedoch auch für die Bereiche Produktion und Dienstleistungen, die immer mehr im Zeichen globalisierter Wertschöpfungsketten stehen.

In der im Auftrag des Bundesministeriums für Wirtschaft und Energie erstellten Studie zu IT-Sicherheit für die Industrie 4.0 mit Stand Januar 2016 wird erwähnt, dass laut VDE-Trendreport 2015 (VDE=Verband der Elektrotechnik, Elektronik und Informationstechnik) die gegenwärtige Vision von Industrie 4.0 (I4.0) bis zum Jahr 2025 Realität geworden sein wird. Schon heute bestimmen IT-Infrastrukturen in zunehmendem Maße die industriellen Prozesse und sind in fast allen Bereichen unverzichtbar.

Zukünftig werden komplexe IT-Infrastrukturen – bestehend aus mobilen und stationären Komponenten – die gesamte industrielle Wertschöpfungskette durchdringen und heute kaum vorstellbare Flexibilitäts- und Effizienzsteigerungen ermöglichen.

Weiterhin wird darauf verwiesen, dass für die Zuverlässigkeit derartiger Systeme und zum Schutz betriebs- und personengebundener Daten ein hohes Maß an IT-Sicherheit unabdingbar ist. Der Schutz vor Cyberattacken zur illegalen Aneignung von Daten oder zur Sabotage IT-basierter industrieller Prozesse betrifft neben einzelnen Teilnehmern ganze Wertschöpfungsketten bzw. -netzwerke, die vielfach global organisiert sind.

Die heute weitgehend noch fehlende IT-Sicherheit wird laut VDE-Trendreport 2015 derzeit als das weitaus größte Hindernis für den Einzug von Industrie 4.0 in die produzierenden Betriebe Deutschlands gesehen.

Aus diesem Grund wird es immer wichtiger, dass die Unternehmen alles daran setzen, ihre Daten und vor allem ihr Know-how zu schützen. Mit Nachdruck

möchte ich betonen, dass dies einmal mehr auch für die vielen Unternehmen des Handwerks gilt.

Der 6. IT-Sicherheitstag Mittelstand 2017, in dessen Nachgang dieser Band zusammengestellt wurde, gab einen detaillierten Überblick zur aktuellen Bedrohungslage und machte deutlich, wie häufig und „verschlungen" Angriffswellen auf jede Firma hereinbrechen können. Neben den klassischen Versorgern für Energie, Wasser und Kommunikation sind auch Branchen wie Transport, Finanzen, Gesundheit und Ernährungswirtschaft inzwischen Ziel der massiven Angriffe. Jedes Unternehmen kann Teil der sogenannten kritischen Infrastruktur sein, ohne sich dessen bewusst zu sein. Als Auftragnehmer oder Kunde stehen auch kleine Firmen, Dienstleister und Handwerker im Fokus der Cyberkriminellen.

In diesem Zusammenhang wird Ihnen der vorliegende Band eine praktische Handreichung sein, um die Gefahren im Themenbereich IT-Sicherheit erstens besser abschätzen zu können und zweitens die entsprechenden Maßnahmen (auch in Kooperation z.B. mit den Handwerkskammern) zu ergreifen, um im Zeitalter der Digitalisierung bestens gerüstet zu sein.

Frankfurt (Oder), Oktober 2017 Uwe Hoppe

Ansprechpartner IT-Sicherheit für die Region Berlin/Brandenburg

Landeskriminalamt Berlin
Zentrale Ansprechstelle Cybercrime
Martin-Luther-Str. 105
10825 Berlin

Olaf Borries
Tel.: 040 4664-924924
ZAC@polizei.berlin.de

außerhalb der Bürodienstzeit:
Tel.: 030 4664-4664

Landeskriminalamt Brandenburg
Cyber-Competence-Center
Zentrale Ansprechstelle Cybercrime
16225 Eberswalde
Tramper Chaussee 1
Tel.: 03334 388-8686
ZAC@polizei.brandenburg.de

Denny Speckhahn
Tel.: 03334 388-8600
Denny.Speckhahn@polizei.brandenburg.de

Mark Le Corre
Tel.: 03334 388-1121
Mark.LeCorre@polizei.brandenburg.de

außerhalb der Bürodienstzeit:
Tel.: 0331 283-3035

Handwerkskammer Berlin
10961 Berlin
Blücherstraße 68

Kerstin Wiktor
Beauftragte für Innovation und Technologie
Tel.: +49 30 25903 392
Wiktor@hwk-berlin.de

Handwerkskammer Cottbus
Außenstelle Königs Wusterhausen
15711 Königs Wusterhausen
Cottbuser Straße 53
Handwerkskammer Cottbus
03046 Cottbus
Altmarkt 17

Dr. Heiko Vesper
Beauftragter für Innovation und Technologie Tel.: 03375 2525-63
vesper@hwk-cottbus.de
Torsten Hilsky Gruppenleiter IT
Tel.: 0355 7835-117
hilsky@hwk-cottbus.de

Stefan Pesker
IT-Administrator
Tel.: 0355 7835-226
pesker@hwk-cottbus.de

Handwerkskammer Frankfurt (Oder)
Region Ostbrandenburg
15230 Frankfurt (Oder)
Bahnhofstraße 12

Henrik Klohs
Beauftragter für Innovation und Technologie
Tel.: 0335 5619-122
Henrik.klohs@hwk-ff.de

Handwerkskammer Potsdam
Zentrum für Gewerbeförderung Götz
Am Mühlenberg 15
14550 Groß Kreutz (Havel)

Dr. Maria Baumann-Wilke
Team Technik und Innovation
Tel. +49 33207 34-205
maria.baumann-wilke@hwkpotsdam.de

IHK Berlin
10623 Berlin
Fasanenstraße 85
Tel.: 030 315100
service@berlin.ihk.de

IHK Ostbrandenburg
15236 Frankfurt (Oder)
Puschkinstraße 12b
Tel.: 0335 5621-0
info@ihk-ostbrandenburg.de

AKUS – Arbeitskreis für Unternehmenssicherheit Brandenburg
Geschäftsstelle IHK Ostbrandenburg

IHK Potsdam
14467 Potsdam
Breite Str. 2a-c Tel.: 0331-2786-0
Fax: 0331-2786-111
info@potsdam.ihk.de

Vanessa Grühser
Fachkräfte und Innovation
Tel.: 030 31510-459
vanessa.gruehser@berlin.ihk.de

Thomas Herrschelmann
Referent International/Enterprise Europe Network
Tel.: 0335 5621-1325
herrschelmann@ihk-ostbrandenburg.de

Jens Jankowsky
Referent Technologie/Innovation
Tel.: 0335 5621-1332
jankowsky@ihk-ostbrandenburg.de

Marco Albrecht
Referent Technologie und Innovation
Tel.: 0331 2786-287
marco.albrecht@ihk-potsdam.de

Johannes Ginten
Referent Wirtschafts- und Verkehrspolitik / Infrastruktur
Tel.: 0331 2786-209
johannes.ginten@ihk-potsdam.de

HTW Berlin
EFRE Anwendungszentrum
Digital Value
Treskowallee 8
10318 Berlin

Prof. Dr. Matthias Hartmann
Projektleiter
Matthias.Hartmann@HTW-Berlin.de

(Stand Oktober 2017)

Inhaltsverzeichnis

Teil 1: IT-Sicherheitstage in Brandenburg und Berlin

1. Rückblick IT-Sicherheitstage

Henrik Klohs, Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg

Abstract

Die Themen wie IT-Sicherheit, Datensicherheit und Datenschutz nehmen für die Digitalisierung der Wirtschaft einen immer höheren Stellenwert ein. Mit der immer stärker ansteigenden Bedeutung der Informations- und Kommunikationstechnologien wächst auch die Bedrohung durch Computerkriminalität und Wirtschaftsspionage. Die notwendige und erfolgreiche Digitalisierung braucht IT-Sicherheit. Als Auftragnehmer oder Kunde stehen auch kleine Firmen, Dienstleister und Handwerker im Focus der Cyberkriminellen.

1.1 Zunehmende Nachfrage nach IT-Sicherheit

Informations- und Kommunikationstechnologien (IKT) schaffen immer neue, effektivere und komfortablere Anwendungen. Damit einhergehen allerdings auch erhöhte Sicherheitsanforderungen, die bei Nichtbefolgen durchaus existenzbedrohend sein können. Gerade das Handwerk und die kleinen und mittleren Unternehmen aus Industrie und Handel verfügen meist nicht über eigene IT-Mitarbeiter oder gar IT-Abteilungen, die sich mit den Fragestellungen, die im Zusammenhang mit der Nutzung moderner IT-Technologien auftreten, auseinandersetzen können. Auch die zeitlichen und personellen Ressourcen der meisten Handwerksbetriebe sind knapp bemessen, um sich derartigen Fragestellungen zu widmen.

Genau aus diesen Gründen hat die Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg mit ihrem damaligen Projekt „eBusiness Lotse Ostbrandenburg" und den Konsortialpartnern F1 GmbH, der Technischen Hochschule Wildau, der Hochschule für nachhaltige Entwicklung Eberswalde und der IHK

Ostbrandenburg im Jahre 2013 die jährliche Veranstaltungsreihe „IT-Sicherheitstag" gestartet.

1.2 Inhalte der bisher fünf durchgeführten IT-Sicherheitstage

Kleine Betriebe aus Industrie, Handel und Handwerk sollen praxisnah informiert und bei der Suche nach bezahlbaren und praktikablen IKT-Lösungen unterstützt werden.

Unter dem Motto *„IT-Sicherheitstag Regional"* führte der eBusiness-Lotse Ostbrandenburg in Zusammenarbeit mit dem Network & Information Security Netzwerk (NIS-Group) am 5. Dezember 2013 an der Technischen Hochschule Wildau den **1. IT-Sicherheitstag** durch. Dass das Thema IT-Sicherheit von hoher Aktualität ist, zeigte die große Resonanz mit knapp 90 Teilnehmern aus Unternehmen und Einrichtungen in Ostbrandenburg.

Da die Nachfrage unerwartet hoch war, wurde unter dem Motto *Regionale und überregionale IT-Sicherheitsaspekte – „Wie sichere ich meine IT-Umgebung?"* am 22.05.2014, diesmal im Audimax und weiteren Vortragsräumen mit parallelen Vorträgen an der Technischen Hochschule Wildau, der **2. IT-Sicherheitstag** durchgeführt.

Die Themenpalette reichte von allgemeinen Praxistipps für die Sicherheit in Unternehmens-IT-Netzwerken über die Bedeutung von Informations-Sicherheits-Management-Systemen (ISMS) bis hin zu der Frage, was moderne Firewall-Systeme heute leisten.

Darüber hinaus wurde u.a. folgenden Fragen nachgegangen:

- Wie kann das Mitarbeiterverhalten die IT-Sicherheit beeinflussen?
- Welche Chancen und Risiken birgt der Einsatz von privaten und mobilen IT-Geräten im Unternehmen?
- Wie kann ich meine Daten sichern und bei Verlust wiederherstellen?
- Wie können Nachrichten verschlüsselt werden?
- Wie kann man per De-Mail sicher digital kommunizieren und
- Wie erkennt man aktuelle Cyberangriffe?

Vertreter des Landeskriminalamtes Brandenburg informierten über die aktuelle Lage und Phänomene im Bereich Cybercrime. Weiterhin wurden zum Abschluss der Veranstaltung in einem „Live-Hacking" die Möglichkeiten und Methoden von Angriffen auf IT-Systeme von Unternehmen demonstriert.

Für über 140 Beteiligte war es ein inhaltsreicher, informativer und spannender Tag, der am 29.01.2015, diesmal im Ludwig-Erhard-Haus in Berlin, seine Fortsetzung als **3. IT-Sicherheitstag Mittelstand** hatte.

Unter dem Motto *„Schutz von Unternehmen gegen Angriffe aus der digitalen Welt*" wurde eine breite Palette Themen zu IT-Sicherheit vorgestellt:

- Wirtschaftsspionage über Sicherheit in der Cloud,
- Missbrauchsschutz von Laptops,
- Datenschutz und Datenspuren,
- Sicherheit von mobilen Endgeräten,
- Organisation der IT-Sicherheit,
- IT-Service Management,
- Privatsphäre und Email bis hin zur Firewall.

Höhepunkte des 3. IT-Sicherheitstages Mittelstand waren u.a. die Keynote von Peter Schaar, dem ehemaligen Bundesbeauftragten für Datenschutz und Informationsfreiheit und heutigem Vorsitzenden der Europäischen Akademie für Informationsfreiheit und Datenschutz sowie der Abschlussvortrag von Tobias Schrödel, einem ausgewiesenen IT-Sicherheitsexperten und Deutschlands ersten IT-Comedian, der den Anwesenden auf eindrucksvolle und zugleich unterhaltsame Weise vorführte, wie einzelne IT-Systeme angegriffen werden können. Zugleich gab Herr Schrödel den Teilnehmern wertvolle Tipps mit auf den Weg, wie sie die Sicherheit ihrer Daten, Geräte und Firmennetze erhöhen können.

Zu den Organisatoren und Partnern diese Events zählten neben der Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg mit ihrem eBusiness-Lotsen Ostbrandenburg die eBusiness-Lotsen aus Westbrandenburg, Potsdam, Südbrandenburg, Berlin, Magdeburg, Mitteldeutschland, „Nordost", Thüringen und Mecklenburg-Vorpommern, der Handwerkskammertag Land

Brandenburg, die IHK Berlin und Berlin Partner für Wirtschaft und Technologie.

Nach den großen Erfolgen der bisher drei durchgeführten IT-Sicherheitstage an der TH Wildau mit 90 Teilnehmern in 2013 und knapp 140 in 2014 sowie Anfang 2015 im Ludwig Erhardt Haus in Berlin mit knapp 200 Teilnehmern hat der eBusiness-Lotse Ostbrandenburg am 29. September 2015 im WISTA-Veranstaltungszentrum in Berlin Adlershof seinen **4. IT-Sicherheitstag Mittelstand 2015** unter dem Motto *„Wie können sich Unternehmer gegen Angriffe aus dem digitalen Netz schützen?*" mit mehr als 130 Teilnehmern durchgeführt.

Mitveranstalter waren wieder weitere eBusiness-Lotsen aus Berlin und Brandenburg sowie Kompetenzträger aus dem Bereich IT-Sicherheit.

In spannenden Kurzvorträgen und praktischen Demonstrationen von hochkarätigen Experten deckte dieser IT-Sicherheitstag wieder eine breite Palette an wichtigen Themen rund um die IT-Sicherheit ab:

- Schutz sensibler Daten und Kommunikationswege,
- Schutz des Know-hows der Unternehmen,
- Organisation der IT-Sicherheit,
- Anforderungen und Haftung im Datenschutzrecht,
- IT-Service Management,
- Welche Schutzmechanismen bieten moderne Firewallsysteme sowie
- Sicherheitsaspekte im Rahmen von Industrie 4.0 und Handwerk 4.0.

Die Höhepunkte des 4. IT-Sicherheitstages Mittelstand waren u.a.

- die Keynote mit einem praxisbezogen Vortrag aus Sicht eines Betroffenen,
- der Vortrag „Industrielle IT-Sicherheit: live-Hacking einer SPS",
- die verschiedenen parallelen Vorträge in den Räumen 1 und 2 sowie
- das Live-Hacking und der Abschlussvortrag von Tobias Schrödel, der wie auf dem 3. IT-Sicherheitstag auf eindrucksvolle und zugleich unterhaltsame Weise vorführte, wie einzelne ungeschützte IT-Systeme angegriffen werden können.

Die Förderung des bundesweiten Projektes „eBusiness-Lotse", worüber die IT-Sicherheitstage vom BMWi finanziell mit unterstützt wurden, wurde zum 30.09.2015 beendet.

Die Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg steht aber weiterhin als eBusiness-Lotse Ostbrandenburg für die Klärung zu Fragen zum elektronischen Geschäftsverkehr und IT-Sicherheit mit ihren BIT weiter zur Verfügung.

Gemeinsam mit der Mittelstand 4.0 - Agentur Prozesse, der F1 GmbH und weiteren brandenburgischen Handwerkskammern, Industrie- und Handelskammern sowie Hochschulen und Kompetenzträgern aus dem Bereich IT-Sicherheit organisierte und führte die Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg am 22.09.2016 ihren nun schon **5. IT-Sicherheitstag Mittelstand 2016** an der TH Wildau durch. Über 100 Teilnehmer aus Handwerk, Industrie und Handel, Kommunen und Institutionen aus den neuen Bundesländern und Berlin informierten sich auf dieser kostenfreien Veranstaltung zu *"Cyber-Risiken und Angriffsszenarien und möglichen Schutzmaßnahmen*". Die Themenpalette dieser ganztägigen Veranstaltung reichte von allgemeinen Praxistipps für die Sicherheit in IT-Netzwerken über die Bedeutung von Datenschutz und -sicherheit bis hin zu Cloud und Industrie 4.0.

Weitere Themen waren:

- Mobile Sicherheit - Einsatz von mobilen Endgeräten in Unternehmen,
- Verschlüsselung und Signatur,
- Schutz sensibler Daten und Kommunikationswege,
- Sicherheitsaspekte im Rahmen von Industrie 4.0 und Handwerk 4.0 sowie
- Schutz des Know-hows der Unternehmen.

Praxisnah und verständlich wurde aufgezeigt, wie man seine eigenen Unternehmensdaten effektiv vor Angriffen schützen kann. Zum Anfang und Abschluss der Veranstaltung wurden in einem „Live-Hacking" die Methoden von Hackerangriffen auf IT-Systeme von Unternehmen demonstriert.

Die Teilnehmer gaben durchgehend dem 5. IT-Sicherheitstag Mittelstand ein positives Feedback und Hinweise für weitere Themen. Bei der Planung des

6. IT-Sicherheitstag Mittelstand 2017 wurden diese Themenwünsche mitberücksichtigt.

1.3 Hohe Bedeutung von IT-Sicherheit

Mit der immer stärker ansteigenden Bedeutung der Informations- und Kommunikationstechnologien wächst auch die Bedrohung durch Computerkriminalität und Wirtschaftsspionage. Aus diesem Grund wird es immer wichtiger, dass die Unternehmen alles daransetzen, ihre Daten und vor allem ihr Know-how zu schützen. Durch die Digitalisierung der Prozesse in der Industrie, im Handwerk bzw. allgemein in der Wirtschaft nimmt die IT-Sicherheit einen immer höheren Stellenwert ein.

Vielen Unternehmen, Institutionen und Verwaltungen mangelt es aber an finanziellen Mitteln und qualifiziertem Personal. Bei der steigenden Anzahl von Cyberattacken sowie von Datenklau und Datenmissbrauch bleibt aber festzuhalten, dass man auch für die IT-Sicherheit finanzielle und personelle Ressourcen einplanen muss. Gerade in der Zeit der Digitalisierung muss zu jedem Zeitpunkt die IT-Infrastruktur funktionieren.

2. Der 6. IT-Sicherheitstag Mittelstand 2017 an der HTW Berlin

Matthias Hartmann, Madlen Böer, Ralf Waubke, Leonhard Gebhardt;
HTW Berlin

2.1 Gestaltung der Konferenz

Abbildung 1: Begrüßung der Teilnehmer vom IT-Sicherheitstag durch den Hauptgeschäftsführer der HWK Frankfurt (Oder). © O. Borries

Der 6. IT-Sicherheitstag Mittelstand 2017 fand am 14.09.2017 an der HTW Berlin statt. Ein Dutzend verschiedener Partner ermöglichte die Fachkonferenz für Datenschutz, Informations- und IT-Sicherheit im Zeitalter der Digitalisierung.

Hauptprogramm I

09.30 Uhr	Einlass
10.00 Uhr	Begrüßung *Prof. Matthias Hartmann* Dekan, HTW Berlin
10.05 Uhr	Grußwort *Uwe Hoppe* (Bild links)
10.15 Uhr	Phänomen Cybercrime *KOK Olaf Borries,* ZAC – LKA Berlin
11.00 Uhr	Pragmatische IT-Sicherheit für KMU aus Industrie, Handel & Handwerk *Prof. Matthias Hartmann und Ralf Waubke*, HTW Berlin
11.50 Uhr	Kurzvorstellung der IT-Security-Start-ups und Referenten
12.45 Uhr	Live-Hacking – Manipulation industrieller Steuerungen *Roland Hallau und Mike Wäsche*

Feedback von Teilnehmer_innen I

„Kompliment für die […] gelungene, informative und nutzbringende Veranstaltung."

Parallele Vorträge I

13.30 Uhr Datenschutz / IT-Sicherheit: Die neue EU-Datenschutz-Grundverordnung
Heiko Behrendt, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

14.15 Uhr Verwaltung von Daten im Unternehmen – Sicherer Umgang mit digitalen Daten
Rechtsanwalt Gerd M. Fuchs

15.00 Uhr Besichtigung der Ausstellung

15.45 Uhr Sicherer Einsatz von Cloud Computing in kleinen und mittleren Unternehmen (KMU)
Richard Hawthornthwaite, Bundesdruckerei

16.30 Uhr Social Engineering Preisgabe von vertraulichen Informationen
Knut Kricke, VERTEXakademie GmbH

Parallele Vorträge II

13.30 Uhr IT-Sicherheit und Usability:
Benutzbare IT-Sicherheit in Systemen
Hartmut Schmitt, HK-Business Solutions

14.15 Uhr Sichere IT-Infrastruktur
Tim Lange und Thore Bischoff, Netz-Werker AG

15.00 Uhr Besichtigung der Ausstellung

15.45 Uhr Wie lassen sich kritische Infrastrukturen sichern? Ein praktischer Erfahrungsbericht aus der Arbeit des DiSiNet!
Jörn Kinzel, Netzwerkmanager des Netzwerkes DiSiNet

16.30 Uhr Sicherheit im digitalen Zeitalter – Cyberschutz
Veikko Ullmann, Leiter Firmengeschäft, Vertriebsdirektion Berlin, Filialdirektor Allianz Beratungs- und Vertriebs-AG

Feedback von Teilnehmer_innen II

„Der IT-Sicherheitstag hat mir inhaltlich sehr gut gefallen. Auch vom Aufbau fand ich alles sehr gut gelungen. […] Ich plane auf jeden Fall, beim nächsten IT-Sicherheitstag ein, wieder dabei sein zu können."

Parallele Vorträge III

13.30 Uhr Aktuelle Cybercrime-Phänomene, Schwerpunkt Ransomware
KK Mark Le Corre, ZAC Brandenburg

14.15 Uhr Cybercrime: Backup-Strategie und Notfall-Management
KOK Olaf Borries, ZAC Berlin

15.00 Uhr Besichtigung der Ausstellung

15.45 Uhr Social Engineering am Beispiel „CEO-Fraud"
KK Silvio Berner, ZAC Sachsen

16.30 Uhr Vorstellung BSI / Was bietet das BSI für KMUs?
KOK Olaf Borries, ZAC Berlin

Hauptprogramm II

17.15 Uhr Live-Hacking am Haus „Tag der offenen Tür mal anders" Das Haus als Angriffsziel – Was tun? Ein Livehacking mit Antworten!
F1 GmbH / TelcoTech gemeinsam mit Werner Alarmanlagen GmbH und VDS (*Christian Schottmüller*)

18.00 Uhr Der 6. IT-Sicherheitstag – Gemeinsames Fazit.
Diskussion mit den Referenten und Vorstellung „Handbuch Wirtschaftsgrundschutz"
Prof. Timo Kob, ASW Bundesverband

18.30 Uhr Ausklang | Networking, Ausstellungsbesichtigung, Diskussion & Gespräche mit Referenten

Feedback von Teilnehmer_innen III

„Eine sehr schöne Veranstaltung. Vielen Dank und bis zum nächsten Mal."

2.2 Impressionen und Eindrücke

Folgende Bilder geben einen visuellen Eindruck zum 6. IT-Sicherheitstag.

Abbildung 2: : Beginn der Veranstaltung und Auditorium. © T. Dirsat.

190 Teilnehmer nahmen an dem Konferenztag teil. Die letzten Gäste mussten aufgrund des großen Andrangs auf den Treppen Platz nehmen. Im Vergleich zum Vorjahr stieg die Teilnehmeranzahl auf fast das Doppelte.

Abbildung 3: Dr. M. Hartmann, H. Klohs und Dr. H. Vesper (v.l.n.r.). © T. Dirsat.

Abbildung 4: Intensive Diskussion in den Breakout-Sessions mit circa 50 Teilnehmern zu speziellen Problemen der IT-Security: Die Landeskriminalämter aus drei Bundesländern klären auf. © T. Dirsat.

Abbildung 5: R. Hallau präsentiert beim Live-Hacking die Steuerungsübernahme eines Roboters. © T. Dirsat.

2.3 Meinungsbild zur IT-Sicherheit

Das Forschungsteam um Prof. Dr. Matthias Hartmann führte anlässlich der Tagung eine Umfrage zur IT-Sicherheit durch. Die quantitative Umfrage adressierte Fragestellungen zur IT-Sicherheit und zur digitalisierten Zukunft. Die Fragen lassen sich in den Bereich der Zukunftsforschung einordnen und geben erste Einschätzungen für zukünftige IT-Sicherheitsthemen.

2.3.1 Methodischer Ansatz

Die Erhebung erfolgte mittels Fragebogen, der an die Teilnehmer des IT-Sicherheitstages in Papierform ausgeteilt wurde. Der Fragebogen folgt einem explorativen Ansatz. Aufgrund der heterogenen Teilnehmerzahl kann dadurch ein breites Stimmungsbild erfasst werden.

Zu Beginn des Fragebogens wurden sogenannte Eisbrecherfragen platziert, die zum einen vom Schwierigkeitsgrad her leicht zu beantworten sind und zum anderen vom Inhalt her grundsätzliche Einschätzungen und Kenntnisse erheben. Zum Ende des Fragebogens wurden Daten zu den Teilnehmern und dazugehörigen Unternehmen erhoben. Im Pretest des Fragebogens ergab sich eine maximale Bearbeitungszeit des Fragebogens von zehn Minuten.

Von den 190 Teilnehmern haben 102 den Fragebogen ausgefüllt. Dies entspricht einer Rücklaufquote von 53,7%.

In den folgenden Abschnitten werden auszugsweise einige Ergebnisse der Erhebung dargestellt.

2.3.2 Zahlen und Fakten zu den Teilnehmern des IT-Sicherheitstages

In Summe nahmen 190 Teilnehmer am 6. IT-Sicherheitstag teil. Der Schwerpunkt der Teilnehmer kam dabei aus Berlin und Brandenburg. Einige Teilnehmer kamen auch aus anderen Bundesländern wie Sachsen-Anhalt, Mecklenburg-Vorpommern, Sachsen oder Bayern.

Abbildung 6 zeigt die Teilnehmerverteilung in Deutschland und darüber hinaus innerhalb Brandenburgs und Berlins. Die Einteilung erfolgte dabei anhand der ersten beiden Ziffern der Postleitzahlen.

Die Konzentration in Berlin und Brandenburg ist jedoch wenig überraschend, da die veranstaltenden Organisationen im Großteil in Berlin und Brandenburg aktiv sind und somit ein ausgeprägtes regionales Netzwerk besitzen.

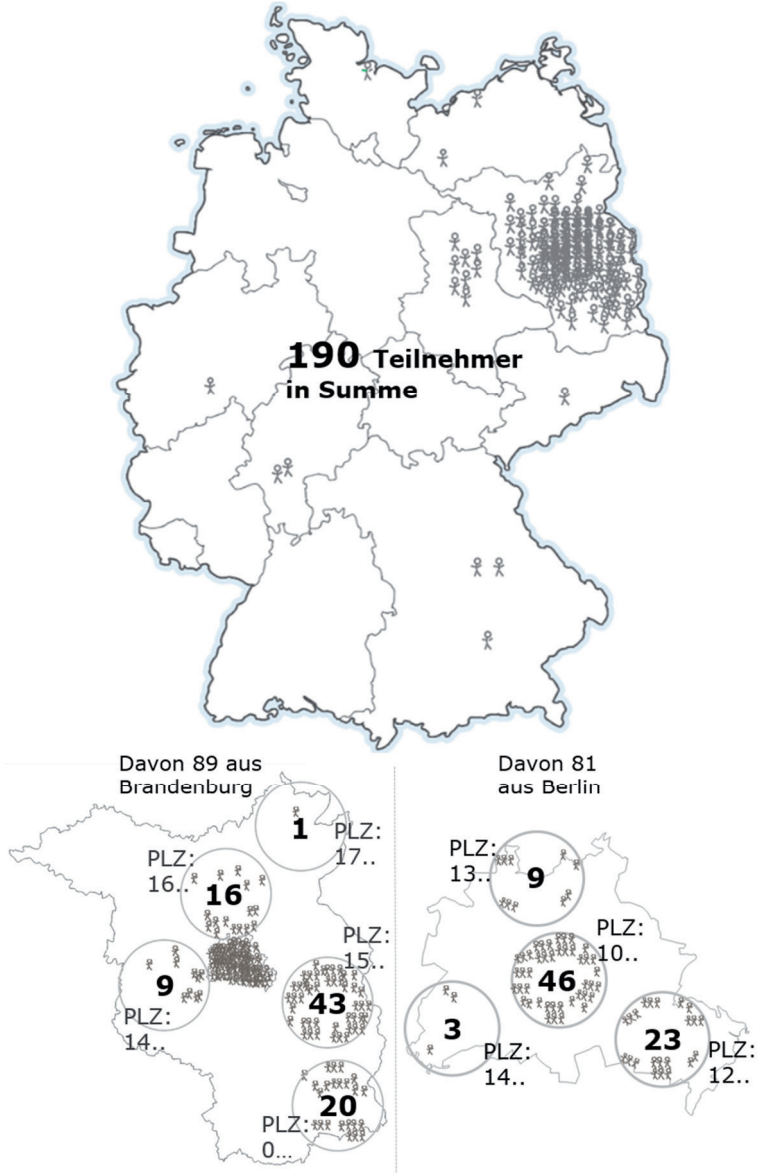

Abbildung 6: Verteilung der Teilnehmer nach Regionen; eigene Darstellung.

Von den 190 Teilnehmern haben in Summe 102 den Fragebogen ausgefüllt, wovon wiederum 100 die Frage beantworteten, welche Position sie innehaben.

Im Schwerpunkt nahmen an der Tagung Personen mit leitenden Tätigkeiten teil. Geschäftsführer stellen mit Abstand den größten Teil der Teilnehmer dar. Dies zeigt, dass IT-Sicherheit Chefsache ist oder zumindest von Führungspersonen hoch priorisiert wird. Abbildung 7 zeigt die Ergebnisse zur Verteilung der Teilnehmer nach Position.

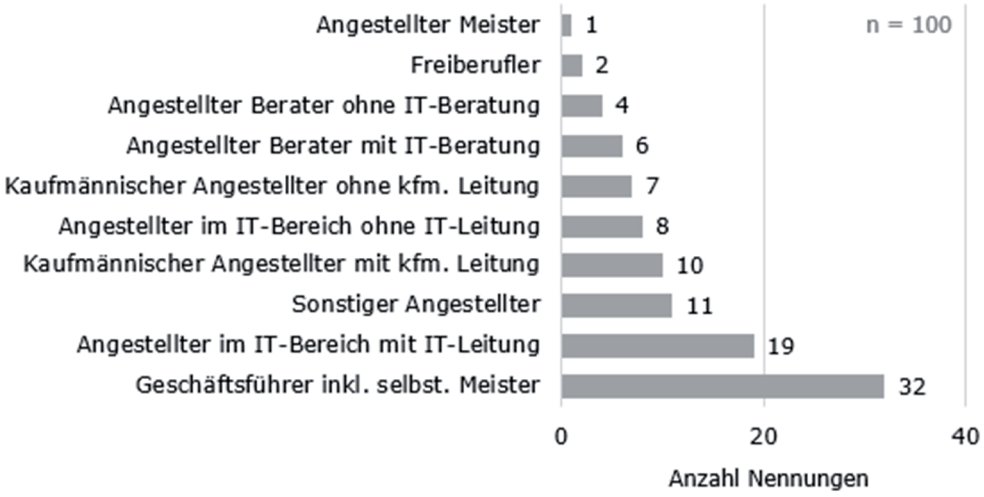

Abbildung 7: Verteilung der Teilnehmer nach Positionen; eigene Darstellung.

Eine weitere Auswertung wurde hinsichtlich der Größe der Unternehmen, in denen die Befragten arbeiten, unternommen. Teilnehmer von Kleinstunternehmen (1-9 Mitarbeiter) sind dabei am häufigsten vertreten. Teilnehmer von Großunternehmen (ab 251 Mitarbeiter) sind hingegen am geringsten vertreten.

In Summe machten 88 Vertreter von Kleinen und Mittleren Unternehmen (KMU) und neun Vertreter von Großunternehmen Angaben zur Unternehmensgröße. Details zur Verteilung finden sich in Abbildung 8.

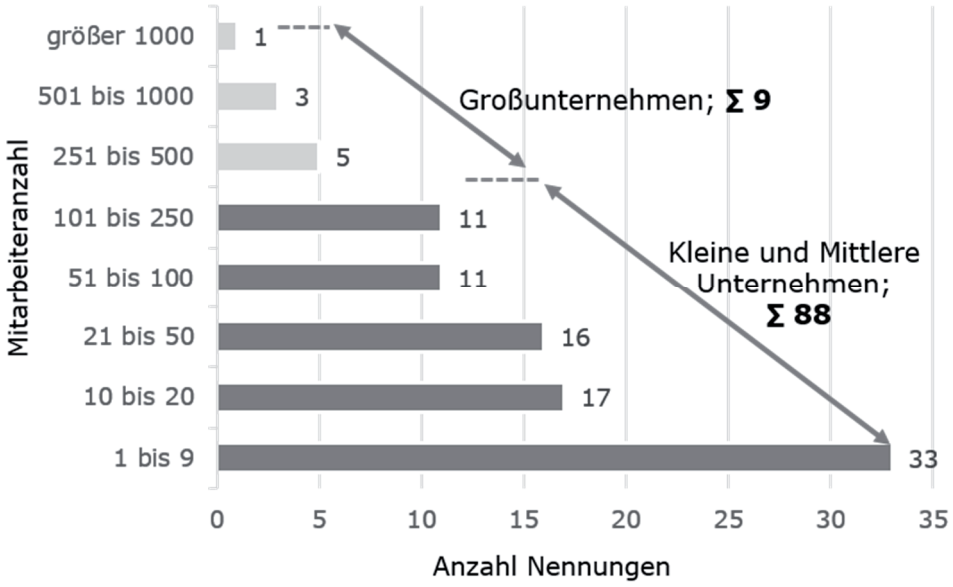

Abbildung 8: Verteilung der Teilnehmer nach Unternehmensgröße; eigene Darstellung.

Eine letzte Auswertung bezüglich der Teilnehmer wurde hinsichtlich der Branchenzugehörigkeit durchgeführt. Dabei dominieren Teilnehmer von IT nahen Unternehmen sowie von Unternehmen, die den unternehmensnahen Dienstleistungen zuzuordnen sind wie Unternehmensberatungen und Finanzberatungen. Das verarbeitende Gewerbe und Baugewerbe inkl. des Handwerks folgen und sorgen zusammen für ca. 28% der Teilnehmer.

Abbildung 9 zeigt die Branchenzugehörigkeit detailliert.

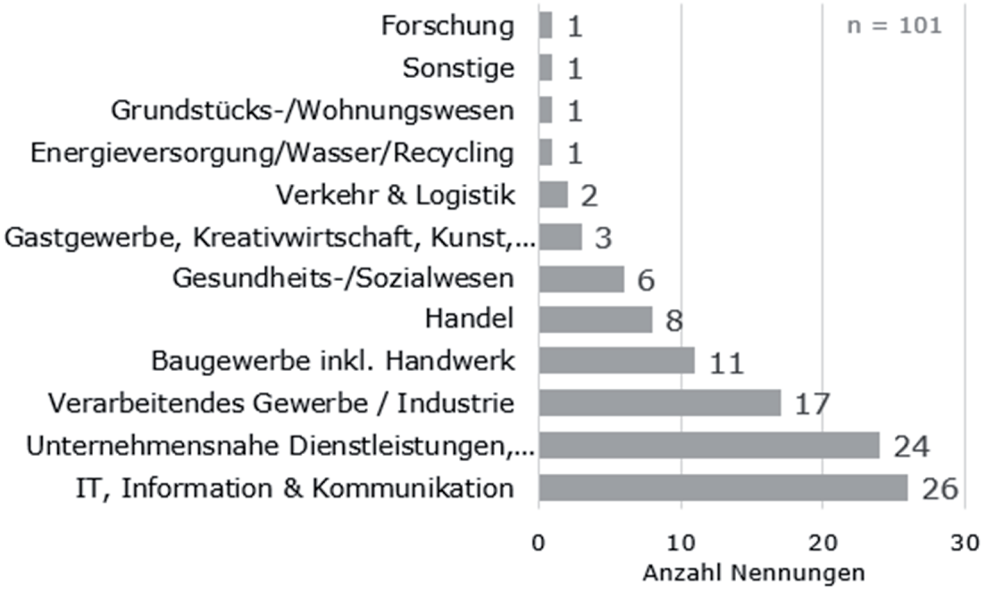

Abbildung 9: Verteilung der Teilnehmer nach Branchenzugehörigkeit; eigene Darstellung.

2.3.3 Ergebnisse zur IT-Sicherheit

Immer mehr Schadsoftware wird über das Internet verbreitet, so auch im Jahr 2017. Dabei ist vor allem die Schadsoftware „Wannacry" in 2017 zu zweifelhaften Ruhm gelangt. Nahezu sämtliche Medien griffen das Thema auf und berichteten ausführlich über den Virus.

Von den Teilnehmern der Umfrage kannten 74 „Wannacry", wohingegen 28 den Virus nicht kannten. Diese Anzahl an Verneinungen überrascht dahingehend, da das Publikum der Tagung grundsätzlich als affin für IT-Sicherheit eingestuft werden muss.

Die Teilnehmer (74), die „Wannacry" kannten, sollten dazu eine Einschätzung vornehmen, wie Sie „Wannacry" empfanden. Von diesen wiederum beantworten 70 die Frage. Dabei zeichnete sich deutlich ab, dass der Großteil erschrocken war über das schlechte Absicherungsniveau von Unternehmen und Privatpersonen, welche reihenweise dem Schadprogramm zum Opfer gefallen waren. Details dazu finden sich in der folgenden Abbildung 10.

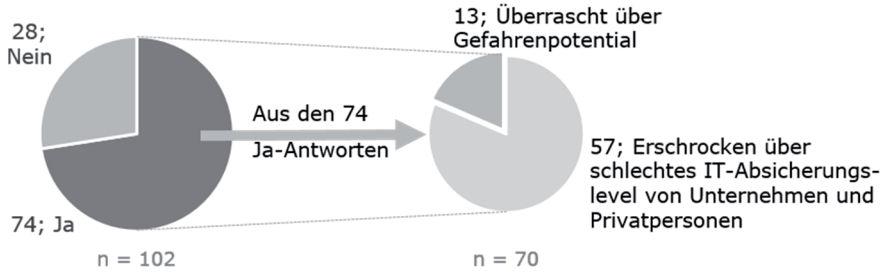

Abbildung 10: Kenntnis und Einschätzung „Wannacry"; eigene Darstellung.

Zum besseren Schutz vor Sicherheitsverletzungen wie bei „Wannacry" offerien einige Institutionen sinnvolle Informationsmaterialen, Leitfäden oder Kataloge. Genannt seien hier beispielhaft der BSI mit seinem IT-Grundschutz, die ISO 27001ff., die VdS Schadenverhütung oder die US-amerikanischen Institutionen SANS, die die 20 CIS Controls empfehlen sowie NIST[1].

Abbildung 11 zeigt den Kenntnisstand der in Deutschland sehr bekannten Kataloge vom BSI und der ISO sowie der SANS. Grundsätzlich zeigt sich, dass weder SANS, die ISO 27001ff. noch der BSI-Grundschutz sehr bekannt sind. So findet sich die Masse der Befragten bei den Kategorien „nicht bekannt" und „Grundkenntnisse" ein.

Unter diesen drei ist SANS am wenigsten bekannt (73x nicht bekannt). Beim BSI-Grundschutz haben zumindest 17 Befragte einen guten Kenntnissstand. Expertenniveu erreichen lediglich zwei Befragte bei der ISO 27001 und vier Befragte beim BSI-Grundschutz.

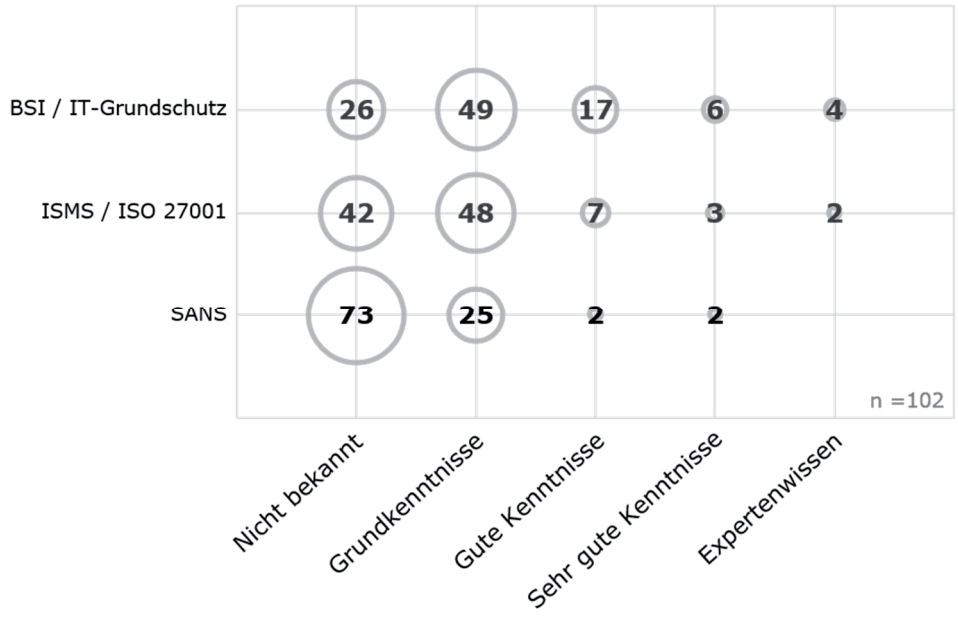

Abbildung 11: Kenntnisniveau BSI, ISMS und SANS; eigene Darstellung.

Der grundsätzlich überraschend schlechte Kenntnisstand der Befragten wirft die Frage auf, wie sich die Befragten im Allgemeinen über das Thema IT-Sicherheit informieren. Abbildung 12 gibt hier einen tieferen Einblick.

Es zeigt sich deutlich, dass vor allem Artikel aus dem Internet sowie Fachzeitschriften genutzt werden. Demgegenüber informieren sich die Befragten eher selten über Hochschulen, soziale Medien und Verbände.

Somit wird deutlich, dass diese Organisationen entweder nicht als Wissensträger für diese Themenstellungen wahrgenommen werden und/oder die Barrieren, mit diesen Organisationen in den Kontakt zu treten, als zu hoch erscheinen.

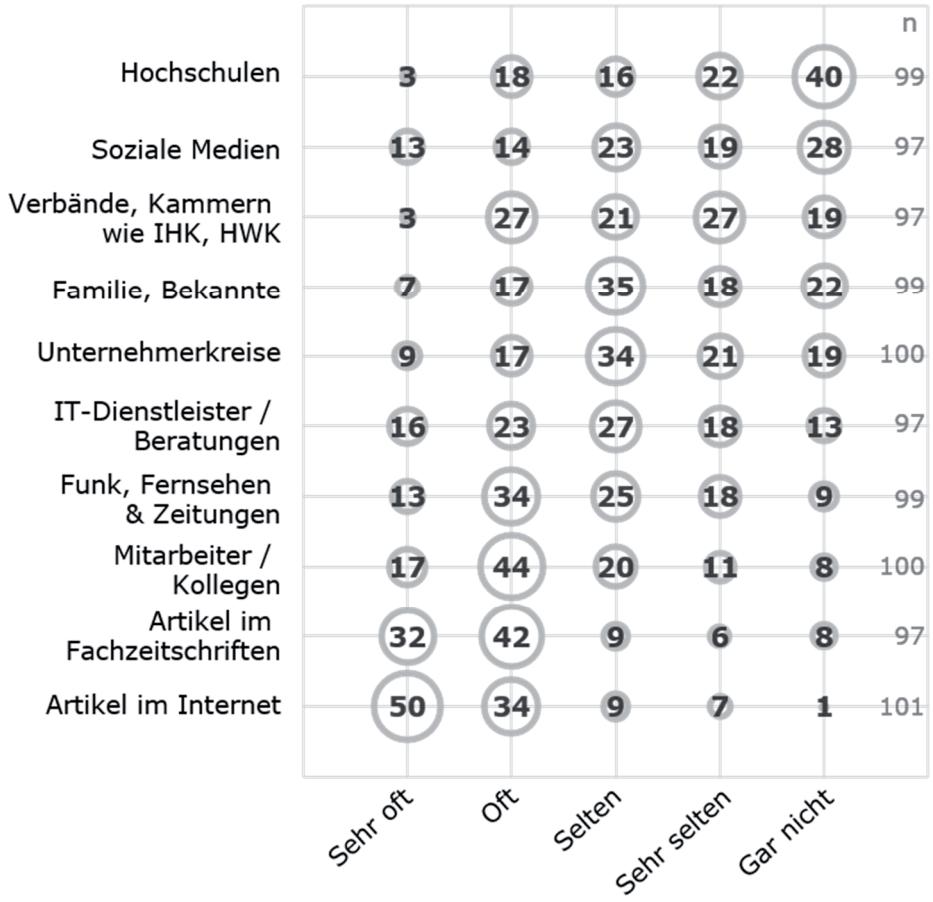

Abbildung 12: Informationskanäle zum Thema IT-Sicherheit; eigene Darstellung.

An der Umfrage war die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Berlin nicht enthalten. Wir dürfen an dieser Stelle die ZAC explizit empfehlen.

Lessons Learned

- Die 6. IT-Sicherheitstagung Mittelstand 2017 war abwechslungsreich, hat Spaß gemacht und viele Gespräche und neue Kontakte gefördert.
- Die Tagung hat ernüchternd und zum Teil schockierend gezeigt, wozu kriminelle Energie fähig ist.
- Die Teilnehmer sind zum Teil schlecht über IT-Sicherheitsthemen informiert.
- Es werden hauptsächlich Internetartikel und Artikel aus Fachzeitschriften genutzt, um sich über Sicherheitsthemen zu informieren.

---

[1] Nähere Informationen zu den genannten Institutionen finden sich in diesem Band innerhalb des Beitrags von Hartmann und Waubke „Pragmatische IT-Sicherheit für Kleine und Mittlere Unternehmen (KMU)."

Teil 2: Gefährdungspotentiale und Hinweise

3. Aktuelle Cybercrime-Phänomene aus polizeilicher Sicht

Olaf Borries, ZAC des LKA Berlin mit Unterstützung der ZAC Brandenburg und ZAC Sachsen

Abstract

Es passiert ständig – Cyberkriminelle greifen die IT-Systeme eines Unternehmens an. Bei allen Landeskriminalämtern der Bundesländer und beim Bundeskriminalamt wurden für Unternehmen, Behörden und Verbände jeweils Zentrale Ansprechstellen Cybercrime (ZAC) eingerichtet, um bei IT-Sicherheitsvorfällen als kompetente Ansprechpartner zu fungieren und zeitnah Erstmaßnahmen zu treffen. Darüber hinaus werden sie bei der Klärung von IT-Sicherheitsfragen beratend und präventiv tätig.

3.1 Einleitung

Glauben Sie noch, Sie sind alleine, wenn Sie mit Ihrem Smartphone oder Computer im Internet surfen? Oder glauben Sie, ausgerechnet Ihre IT sei sicher vor Angriffen von jugendlichen Computerfreaks, organisierten Kriminellen oder sogar staatlich unterstützten Hackern?

Wenn ich an einem mit dem Internet verbundenen Computer alleine in meinem Büro sitze, bin ich trotzdem nicht alleine. Im „globalen Dorf" hat jede/r tatsächlich Milliarden von „Nachbarn" und längst nicht alle wollen ihr oder sein „Bestes". Die Angriffe auf private Computer und Firmennetzwerke nehmen stark zu. Es wird infiziert, ausspioniert, verändert und erpresst. Der Digitalverband Bitkom veröffentlichte am 21.07.2017 eine Studie[1], wonach 53% der Unternehmen in Deutschland Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl in den letzten beiden Jahren geworden sind. Dadurch sei ein Schaden von rund 55 Milliarden Euro verursacht worden.

Der Begriff „Sicherheit" ist trügerisch. Eine absolute Sicherheit kann und wird es im Internet genauso wenig wie im Straßenverkehr geben. Deshalb sollte man sich, ähnlich wie im Straßenverkehr, auch als Internetnutzer so gut wie möglich schützen und die „Verkehrsregeln" beherrschen.

Zu den einfachsten Maßnahmen, ähnlich wie beim Auto die Bremsen, Airbags, Sicherheitsgurte usw., gehören die Verwendung von aktueller Software (insbesondere Betriebssystem, Firewall, Antivirus-Programme), ein adäquates Rollen-Rechte- und Zugriffs-Management (nicht jeder im Betrieb muss auf alle Daten zugreifen können) mit entsprechender Authentifizierung (Passwörter, gegebenenfalls 2-Faktor-Authentifizierung) und besonders wichtig: die regelmäßige Erstellung von *Backups*. Bei größeren Unternehmen mit eigenen IT-Abteilungen sollte deutlich mehr Aufwand betrieben werden. Es empfiehlt sich, u.a. SIEM (Security Information and Event Management), IDS (Intrusion Detection System), IPS (Intrusion Prevention System) oder Fraud-Detection-Systeme zu verwenden.

3.2 Ransomware

Stellen Sie sich vor, Sie sitzen in Ihrem Büro am Computer und erhalten eine E-Mail-Bewerbung von einer Isabell Schneider. Passender Weise suchen Sie auch gerade neues Personal und haben im Vorfeld eine Stellenanzeige im Internet geschaltet. Die E-Mail wurde von isi.schneider90@gmx.de versendet. Beigefügt sind ein Foto mit einer sympathisch lächelnden, jungen Frau, ein Anschreiben in fehlerfreier deutscher Rechtschreibung sowie Grammatik und die Bewerbungsunterlagen. Im Anschreiben berichtet die Bewerberin, dass sie sich auf die ausgeschriebene Stellenanzeige bewirbt und die Stelle optimal ausfüllen kann. In den Bewerbungsunterlagen informiert sie zudem ausführlich über die Vorteile, welche sie dem Unternehmen bringt. Die herunterzuladenden Bewerbungsunterlagen sind in einem ZIP-Archiv komprimiert, sonst wären die Dateien ja zu groß. Sie laden die Datei herunter, entpacken sie und öffnen die in dem Archiv enthaltene Datei „Isabell Schneider – Bewerbung – Mai 2017.pdf". Sie warten einen kurzen Moment, aber nichts passiert. Mit einem Mal hören Sie, eine Stimme sagen:

„Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!".

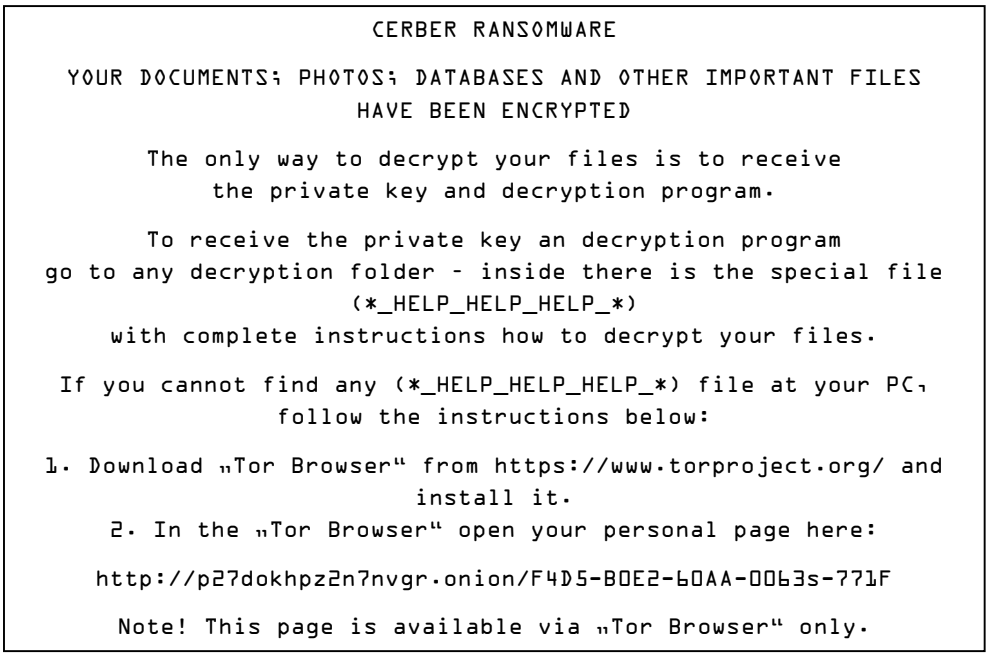

Abbildung 13: Bildschirmansicht Cerber-Ransomware; eigenes Bild.

Ab diesem Zeitpunkt können Sie sich sicher sein: alle Ihre wichtigen Dateien wurden mit einem kryptografisch sicheren Verfahren verschlüsselt!

Eine Anleitung der Täter zur Entschlüsselung befindet sich auf dem Desktop. Sie können dieser folgen und einen gewissen Betrag in der virtuellen Währung Bitcoin an die Täter transferieren. Allerdings können Sie nicht davon ausgehen, dass Ihre Dateien dadurch vollständig entschlüsselt werden.

Wir raten grundsätzlich von Zahlungen an Kriminelle ab (siehe auch Projekt „NO MORE RANSOM"[2]).

Das beschriebene Phänomen wird Ransomware genannt. Der Begriff setzt sich aus dem englischen Wort für Lösegeld („ransom") und Software zusammen. Die ersten in Deutschland verbreiteten Varianten (ab 2011) überlagerten regelmäßig den Desktop mit einem Bild, wodurch der Eindruck eines gesperrten Computers entstand. Zur „Entsperrung" wurde der Betroffene

häufig zu einer Zahlung mittels Paysafecards aufgefordert. Dies war jedoch oft nicht nötig. Meistens ließ sich der Computer mit etwas Aufwand bereinigen.

Seitdem haben sich die Ransomware-Varianten deutlich verändert. Die Dateien auf dem Computer werden tatsächlich kryptografisch sicher verschlüsselt. Auch an den Computer angeschlossene sowie sich im eigenen Netzwerk befindliche Geräte oder eingebundene Cloud-Speicher können verschlüsselt werden. Ebenfalls sind Smartphones oder mit dem Internet verbundene Geräte (z.B. Fernseher) gefährdet.

Aus polizeilicher Sicht handelt es sich bei Ransomware um ein relativ neues Massenphänomen, bei dem der Download der Schadsoftware überwiegend mittels E-Mail-Anhänge oder von Webseiten erfolgt.

Achtung: dieses Phänomen kann zu einer unternehmerischen Krisensituation führen und ist unbedingt ernst zu nehmen! Sollten Sie betroffen sein, zögern Sie nicht, die ZAC Ihres Bundeslandes zu kontaktieren.

Zentrale Ansprechstellen Cybercrime (ZAC)

- *Sind miteinander vernetzte, polizeiliche Kontaktstellen des Bundes und der Länder.*
- *Sie wurden speziell für Unternehmen sowie öffentliche und nichtöffentliche Institutionen eingerichtet.*
- *Sie fungieren als kompetenter Ansprechpartner für die Entgegennahme von IT-Sicherheitsvorfällen mit strafrechtlichem Bezug („Cybercrime*").*
- *Sie leiten zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen ein.*
- *Sie werden bei der Klärung von IT-Sicherheitsfragen beratend und präventiv tätig.*

*Cybercrime umfasst die Straftaten, die sich gegen Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Infomationstechnik begangen werden.

Für Sie werden im nächsten Kapitel die wichtigsten präventiven Maßnahmen erläutert.

3.3 Backup-Strategien und Notfall-Management

3.3.1 Backup-Strategien

Zunächst einmal ist es wichtig, dass sich jedes Unternehmen darüber im Klaren wird, welche Daten für den Fortbestand der Firma entscheidend sind, also die Identifizierung der sogenannten „Kronjuwelen". Diese Daten müssen besonders geschützt werden – vor fremden Zugriff, vor unbewusster oder unberechtigter Veränderung und vor Verlust, sei es durch Schadsoftware (vgl. 3.2 Ransomware), Ausspähung oder technischen Defekt.

Unsere Erfahrung der letzten zwei Jahre zeigt, dass in vielen Fällen ein aktuelles Backup die Existenz des Unternehmens retten konnte. Leider wissen wir auch z.B. von einer Arztpraxis und einer Rechtsanwaltskanzlei, die aufgrund von Datenverlusten durch einen Verschlüsselungstrojaner Insolvenz anmelden mussten.

Das Backup-Medium, z.B. die Festplatte, darf nicht dauerhaft mit dem zu sichernden Gerät verbunden sein, da Schadsoftware häufig alle im Netzwerk vorhandenen logischen Geräte, inzwischen auch Cloud-Laufwerke, verschlüsselt.

Bei kleineren Firmen kann es als erstes ausreichend sein, zwei externe USB-Festplatten im Wechsel als Backup-Medien anzuschließen.

Folgende „W"-Fragen sollte sich jede Firma stellen:

a) Welche Daten sollen wie, wie lange und in welchem zeitlichen Abstand gesichert werden? Welcher Datenverlust wäre (noch) akzeptabel? Welche finanziellen und rechtlichen Konsequenzen drohen bei Verlust der Daten?
b) Wann und wie oft müssen die Daten wieder verfügbar sein? (Recovery/Restore)
c) Wer ist für die Datensicherung verantwortlich?
d) Wie soll die Datensicherung erfolgen? Wird die Wiederherstellung der Daten aus dem Backup (regelmäßig) getestet?

e) Wo werden die Backups aufbewahrt? Eine physikalisch getrennte Lagerung empfiehlt sich, um auch bei Brand, Diebstahl oder Hochwasser auf der sicheren Seite zu sein.
f) Welche Art der Datenstrategie ist für mich passend?
g) Wieviel kostet die Backup-Lösung in der Anschaffung und im laufenden Betrieb?

Die rechtlichen Verpflichtungen zum Vorhalten der Daten können sich u.a. aus § 91 Aktiengesetz, §§ 238, 239 und 257 Handelsgesetzbuch, §§ 146, 146a und 147 Abgabenordnung sowie aus den „Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD) ergeben.

3.3.2 Notfall-Management

Prävention – jede Firma sollte ein Sicherheitskonzept erstellt und umgesetzt haben; dieses sollte regelmäßig fortgeschrieben und angepasst werden.

Das Sicherheitsbewusstsein der Mitarbeiter kann durch regelmäßige Schulungen auf ein hohes Niveau gebracht werden. Prozessabläufe sollten verbessert oder neu eingeführt werden, z.B. ein Vier-Augen-Prinzip bei Überweisungen oder sogenanntes „Whitelisting" von erlaubten Internetseiten oder Bankverbindungen. Im Unternehmen sollte eine aktuelle Liste mit Erreichbarkeiten der Geschäftsführung (siehe 3.4 CEO-Fraud), der IT- und Rechtsabteilung, gegebenenfalls von externen IT-Security-Spezialisten und Ermittlungsbehörden[3] vorhanden sein.

Warum die Strafermittlungsbehörden eingeschaltet werden sollten:

- Nur wenn Unternehmen Angriffe melden, können die Sicherheitsbehörden ein realitätsnahes Lagebild erstellen, Abwehrstrategien entwickeln und andere Firmen rechtzeitig warnen.
- Ermittlungsbehörden können nur dann erfolgreich arbeiten, wenn sie auch Kenntnis von Delikten haben (siehe Ransomware).
- Nur durch die Zusammenarbeit mit staatlichen Stellen können Täter überführt und so zukünftige Delikte verhindert werden.

Detektion – je nach Unternehmensgröße und Bedeutung der IT (verfügbares Budget) können hier verschiedene Maßnahmen, wie in der Einleitung angedeutet, zum Einsatz kommen.

Reaktion – hier werden im Ernstfall die zuvor erstellten Handlungsketten oder Prozessabläufe abgearbeitet.

Problem: Nicht selten überschätzen die Verantwortlichen im Vorhinein ihre eigenen Fähigkeiten, situativ schnell sowie zielführend zu reagieren und unterlassen im Vorfeld die Erstellung eines geeigneten Notfallplans.

Vorbereitung ist immer deutlich besser, d.h. zielführender und billiger als hektische Reaktionen in einer Notfallsituation!

3.4 CEO-Fraud

Die Polizeien verzeichnen seit Ende 2013 in den deutschen Bundesländern ein speziell gegen Unternehmen gerichtetes Betrugsphänomen, bei dem hochprofessionell agierende Täter gezielt bspw. die Abwesenheit der Geschäftsführung in Unternehmen ausnutzen, indem sie mit gefälschten E-Mails und Anrufen autorisierte Mitarbeiter der Buchführungs- und Finanzabteilungen veranlassen, hohe Geldbeträge auf vorgegebene Zielkonten im Ausland zu überweisen. Das bereits aus dem europäischen Ausland bekannte Phänomen wird zumeist als „CEO-Fraud" bezeichnet und ist ein Teilphänomen des Betruges mittels Social Engineering. Diese Betrugsform beinhaltet eine zwischenmenschliche Beeinflussung mit dem Ziel, die Person zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. Dabei werden das persönliche Umfeld des Opfers ausspioniert und falsche Identitäten vorgetäuscht, um geheime Informationen oder Firmeninterna zu erlangen.

Zum Schutz vor dieser Betrugsmasche rät die Polizei:

a) Sensibilisieren Sie Ihre Mitarbeiter.
b) Achten Sie auf die genaue Schreibweise der Absender-E-Mail-Adressen. Nutzen Sie im E-Mail-Programm eher die Funktion „Weiterleiten" als „Antworten". Greifen Sie auf das firmeneigene

Adressbuch zu oder tippen Sie die gewünschte E-Mail-Adresse direkt ein.

c) Fragen Sie bei ungewöhnlichen oder angeblich sehr eiligen Überweisungen über einen anderen Kommunikationsweg nach. Je mehr Druck erzeugt wird oder je mehr auf Geheimhaltung bestanden wird, desto kritischer sollte man sein.
d) Ein Vier-Augen-Prinzip zur Genehmigung von Überweisungen oder das „Whitelisting" von Kontoverbindungen helfen ebenfalls.
e) Datensparsamkeit: Durch die Preisgabe von zu vielen Informationen z.B. auf der Internetseite des Unternehmens wird es Tätern oftmals sehr einfach gemacht, da die Ansprechpartner mit E-Mail-Adresse, Telefonnummer und Zuständigkeit zusammen veröffentlicht werden. Aber auch die einzelnen Mitarbeiter veröffentlichen teilweise in sozialen Medien (z.B. LinkedIn, XING, Facebook) sehr detaillierte Informationen über sich, ihre derzeitige und/oder früheren Aufgaben und damit einhergehend auch über das/die Unternehmen.

3.5 Das Bundesamt für Sicherheit in der Informationstechnik – BSI

Ein weiterer wichtiger Ansprechpartner im Bereich der Internet- oder Computer-Sicherheit ist das Bundesamt für Sicherheit in der Informations-Technik (BSI)[4]. Es ist beim Bundesministeriums des Innern angegliedert. Das BSI sieht sich als eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Die Aufgaben des BSI ergeben sich aus dem *„Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes*", kurz BSI-Gesetz[5].

Gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) wurde die Allianz für Cyber-Sicherheit[6] gegründet. Ziel ist es, aktuelle und valide Informationen zu Gefährdungen im Cyber-Raum bereitzustellen sowie eine Plattform für den Informationsaustausch zwischen den Teilnehmern zu ermöglichen.

Alle Unternehmen, nicht nur die Teilnehmer der Allianz für Cyber-Sicherheit, haben die Möglichkeit, Sicherheitsvorfälle und Cyber-Angriffe auf ihr Unternehmen zu melden[7]. Aus diesen Meldungen, die auch anonym möglich sind, wird regelmäßig ein Lagebild (vgl. 3.3.2) erstellt.

3.6 Fazit

Ein Cyberangriff auf die IT Ihres Unternehmens ist eine Frage der Zeit; also nicht ob, sondern nur wann es passiert – falls es nicht schon geschehen ist.

Eine adäquate Vorbereitung ist daher unabdingbar (vgl. 3.3.2). Dazu gehört insbesondere die Schulung von Mitarbeitern.

Eine einfache Backup-Lösung muss nicht zwangsläufig viel Geld kosten. Erfahrungsgemäß kann sonst ein IT-Sicherheitsvorfall – vor allem bei Verschlüsselung aller Daten – durchaus zur Insolvenz des Unternehmens führen.

Die Unternehmen stehen nicht alleine da – es gibt Unterstützung. Die Anzahl der Hilfsangebote im Internet ist groß! Deshalb seien hier nur einige behördliche Ansprechpartner genannt:

- Die zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes[8]
- Bundesamt für Sicherheit in der Informationstechnik (Prävention)
- Allianz für Cybersicherheit (BSI, Bitkom und weitere)
- Bundesverfassungsschutz (Spionageabwehr)

Lessons Learned

- Der regelmäßigen Sensibilisierung von Mitarbeitern und auch der Führungskräfte für IT-Sicherheitsfragen kommt ein sehr hoher Stellenwert zu.
- Eine adäquate, d. h. dem Unternehmen und den „Kronjuwelen" angepasste Backup-Strategie schützt und sichert Ihre Daten langfristig.
- Ein angepasstes Rollen- und Rechtemanagement verringert das Schadenspotential enorm. Hierbei sollte die Devise lauten: Zugriff auf so viel wie nötig, aber so wenig wie möglich.

[1] Achim Berg, Präsident Bitkom, Dr. Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz, „Wirtschaftsschutz in der digitalen Welt", Vorstellung der Studie, Berlin, 21.07.2017, verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html, Aufruf am 28.09.2017.

[2] Projekt „NO MORE RANSOM!" der National High-Tech Crime Unit der Polizei der Niederlande, Europol, Kaspersky Lab und MacAfee mit dem Ziel Opfern von Ransomware z.B. durch Entwicklung von Entsperrcodes zu helfen, abgerufen am 16.08.2017 unter www.nomoreransom.org.

[3] Internetauftritt des BKA mit einem Link zu den Erreichbarkeiten der ZAC des BKA und der 16 Bundesländer, abgerufen am 16.08.2017 unter https://www.bka.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html.

[4] Internetauftritt des BSI, Aufgaben, abgerufen am 16.08.2017 unter https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html.

[5] BSI-Gesetz, Gesetze im Internet, abgerufen am 16.08.2017 unter https://www.gesetze-im-internet.de/bsig_2009/.

[6] Internetauftritt der Allianz für Cybersicherheit, abgerufen am 16.08.2017 unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html.

[7] Internetauftritt der Allianz für Cybersicherheit mit dem Link zum online-Formular für die Meldung eines IT-Sicherheitsvorfalls oder Cyber-Angriffs, abgerufen am 16.08.2017 unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html.

[8] Internetauftritt des BKA (siehe Fußnote 3).

4. Die Digitalisierung des Verbrechens

Knuth Thiel, Jens Jankowsky; IHK Ostbrandenburg

Abstract

Die Untersuchung zur Kriminalitätsbelastung hat gezeigt, dass das Thema Sicherheit und Bedrohung durch Kriminalität (neben Fachkräftemangel und Energiekosten) einen hohen Stellenwert bei den Unternehmern der Region Berlin und Brandenburg einnimmt. Die Untersuchung im Jahr 2017 verdeutlicht, dass die Belastung der Unternehmer mit einzelnen Deliktskategorien wie Diebstahl oder Sachbeschädigung seit 2005 auf relativ konstantem Niveau verharrt. Nur bei Hackerangriffen wurde seit 2010 eine mehr als Verdopplung der Straftaten registriert.

4.1 Einleitung – Cyberkriminalität im Blick

Von Kriminalität bleiben auch weite Teile der Unternehmerschaft nicht verschont. Deshalb führen die Industrie- und Handelskammern der Länder Brandenburg und Berlin in regelmäßigen Abständen Unternehmensbefragungen zum Thema Kriminalität durch (Kriminalitätsbarometer). Dabei werden u. a. Einstellungen zum Thema Kriminalität, die tatsächliche Kriminalitätsbelastung, das Anzeigeverhalten der Unternehmer und die entstanden Schäden erfragt. Seit Beginn der Untersuchungen wurde besondere Aufmerksamkeit auf das Thema Cyberkriminalität gelegt.

Wie die Landeskriminalämter mitteilen, werden sich die Hackerangriffe in Zukunft noch weitere erhöhen. Besonders problematisch ist dies, da die Unternehmen an der Schwelle der durchgehenden Digitalisierung von Bestellabwicklung, Produktion, Lagerhaltung und Management stehen. Über die damit einhergehende Vernetzung von allen Unternehmensbereichen mit dem Internet eröffnen sich für Straftäter mehr Möglichkeiten die Unternehmen zu schädigen. Insofern war von besonderem Interesse, wie die Unternehmer aus Berlin und Brandenburg von Cyberattacken betroffen waren.

Im April 2017 erfolgte im Rahmen der Konjunkturbefragung von Unternehmen eine wiederholte Zusatzbefragung zur Kriminalitätsbelastung (Kriminalitätsbarometer). Insgesamt basieren die vorliegenden Ergebnisse auf 1.685 ausgewerteten Fragebögen. Die Stichprobe richtet sich an Unternehmen unterschiedlicher Größenklassen, Branchen und Regionen und erfüllt damit die Anforderungen nach Repräsentativität. Die Befragung zum Kriminalitätsbarometer wurde 2005 zum ersten Mal durchgeführt. Weitere folgten in den Jahren 2007, 2009, 2011 und 2015.

Auch wenn die Befragung im Jahr 2017 durchgeführt wurde, gaben die Unternehmer ihre Kriminalitätsbelastung für das Jahr 2016 an.

4.2 Belastung der Unternehmen mit Kriminalität

Wenn Unternehmen im Jahr 2016 von Straftaten betroffen waren, so waren die häufigsten Straftaten Diebstahl (35,4%), Vandalismus/Sachbeschädigung (32,2%), Hackerangriffe (27,4%), Einbruchdiebstahl (26,4%) und Betrug (23,7%). Straftaten wie Produkt- und Markenpiraterie, Wettbewerbsdelikte und Spionage nehmen, wie auch in den vorangegangenen Umfragen, eine eher untergeordnete Rolle ein. Die folgende Grafik (Abbildung 14) gibt einen Überblick über alle abgefragten Straftaten.

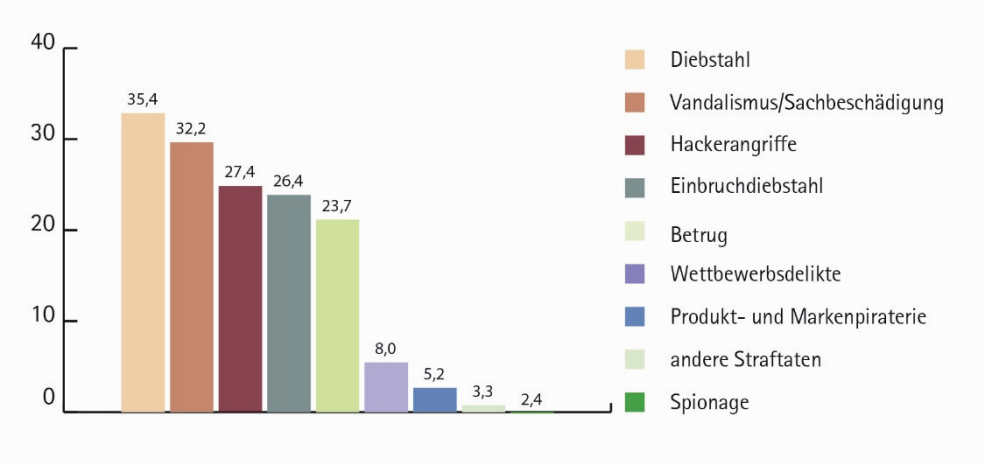

Abbildung 14: Von welchen Straftaten war Ihr Unternehmen im letzten Jahr (2016) betroffen (eigene Darstellung, in Anlehnung an Kriminalitätsbarometer Berlin-Brandenburg 2017)?

Durch die Betrachtung der einzelnen Straftaten im Zeitraum 2004-2016 zeigt sich, dass sich die Zahl der von Hackerangriffen betroffenen Unternehmen von 2010 mit 11,9 % bis 2016 auf 27,4 % mehr als verdoppelt hat. Damit verdrängen Cyberdelikte erstmalig klassische Deliktarten wie Betrug und Einbruchdiebstähle. Es ist anzunehmen, dass hier bei den Befragten nicht nur tatsächliche Hackerangriffe, sondern alle Delikte rund um die Computerkriminalität in die Antworten mit eingehen. Hier wird ein neues Phänomen deutlich. Trotz eigentlich stabilem Verhalten von Kriminalität verdrängt eine Deliktart, die bisher eher eine Randerscheinung war, klassisch häufig vorkommende Straftaten von den vorderen Positionen. Die Befragung wurde vor der weltweiten Cyberattacke mit der Schadsoftware „WannaCry" abgeschlossen. Damit kann der verfälschende Effekt durch starke Thematisierung in den Medien ausgeschlossen werden. Die Verringerung von Einbruchdiebstählen deckt sich mit der Tendenz in der offiziellen Kriminalstatistik.

4.3 Anzeigeverhalten der Unternehmer

Im Kriminalitätsbarometer wurde neben der Betroffenheit von Delikten auch das Anzeigen der Vorfälle bei der Polizei hinterfragt. Damit können nicht nur Aussagen wie in der offiziellen Kriminalstatistik (Hellfeld) getroffen, sondern Hinweise auf die Anzahl nicht angezeigter Vorfälle (Dunkelfeld) gewonnen werden.

Wie auch schon in den Vorjahren gab es große Unterschiede im Anzeigeverhalten der Befragten bei den einzelnen Delikten. Einbruchdiebstähle wurden zu rund 55 % angezeigt. Auf dem zweiten Platz liegt die Kategorie „andere Straftaten" mit über 38 % gefolgt von Anzeigen zum Diebstahl mit knapp 35 %. Vergleicht man das Anzeigeverhalten der vorangegangenen Befragungen mit den aktuellen Zahlen, ist die Bereitschaft zur Anzeige weiter zurückgegangen. Bei den Hackerangriffen ist eine leichte Steigerung der Anzeigen im Vergleich zu den vorangegangenen Umfragen zu verzeichnen.

Das bedeutet im Umkehrschluss, dass die Kriminalstatistik inzwischen je nach Delikt zwischen 45 % der Einbruchdiebstähle im Bereich der Wirtschaft und gar 100 % der Spionagefälle nicht erfasst. Damit ist anzunehmen, dass der

staatlichen Wahrnehmung ein großer Teil der tatsächlichen Kriminalität verborgen bleibt.

Bei Einbruchdiebstählen wurden noch vor 10 Jahren knapp 85 % angezeigt. Damit lag das Dunkelfeld bei nur 15 %. 2016 erstatteten die Unternehmen nur noch in knapp 55 % der Fälle Anzeige bei der Polizei. Damit werden rund 45 % der Einbruchdiebstähle bei Unternehmen in Berlin und Brandenburg nicht in der Kriminalstatistik erfasst.

Bei Vandalismus/Sachbeschädigung sind bei der letzten Umfrage knapp 28 % der Delikte von den Unternehmen angezeigt worden. Hier lag der Anteil der im Dunkelfeld liegenden Straftaten etwa bei 27 %. 2006 zeigten immerhin noch knapp 59 % der Unternehmen die Straftat an.

4.4 Schäden durch Kriminalität

Der Schadensbegriff ist schwer zu definieren. Tatsächliche Schadenshöhen können nur annähernd ermittelt werden. Oftmals bleiben bei der Bezifferung der Schäden in Unternehmen die Folgeschäden etwa durch Produktionsausfall oder auch durch die Weitergabe von Firmengeheimnissen unberücksichtigt. Demzufolge kann hier nur ein grober Überblick über die Entwicklung der Schadenshöhen gegeben werden. Dazu wurde auch bei den Ergebnissen der aktuellen Umfrage ein Median der Schadenshöhen errechnet. Der Median ist das Zentrum der Verteilung der Schadenswerte. Es wird der Wert genommen, der genau in der Mitte aller angegebenen Schadenswerte liegt. So kann ein aussagekräftigerer Mittelwert gebildet werden, der nicht so anfällig ist für extrem hohe Schäden oder auch Bagatellschäden, die nur einmal genannt werden.

Im Vergleich zur vorherigen Umfrage hat sich bei den Einbruchdiebstählen die Schadenssumme pro Delikt erheblich verringert (Tabelle 1). Trotzdem bleibt es die Schadensgruppe mit den höchsten Schäden pro Delikt. Bei Hackerangriffen ist die Schadenssumme pro Delikt bei gleichzeitiger Zunahme der Betroffenheit der Unternehmen gleich hoch geblieben.

Delikt	2006	2008	2010	2014	2016
Einbruchdiebstahl	3.780	5.000	4.000	10.000	5.000
Vandalismus/ Sachbeschädigung	2.500	3.000	2.000	2.000	2.000
Hackerangriffe	800	2.000	900	2.000	2.000
Betrug	2.000	4.500	2.500	2.250	1.000
Ladendiebstahl	1.300	1.000	600		
Diebstahl				2.000	2.000

Tabelle 1: Durchschnittlicher Schadenswert in Euro (Median, gerundet).

4.5 Fazit

Kriminalität bleibt für die Wirtschaft in Berlin und Brandenburg ein sehr bedeutendes Thema. Die Betroffenheit von Delikten und der Schutz vor Straftaten binden erhebliche finanzielle, materielle und personelle Ressourcen, die den Firmen bei der Unternehmensentwicklung fehlen. Hier ist der Staat in seiner ordnungspolitischen Funktion stärker denn je gefordert, die Entwicklung der Wirtschaft ohne störende Einflüsse durch Kriminalität zu gewährleisten. Das gilt vor allem dann, wenn Handel und wirtschaftliche Kooperation über Grenzen hinweg künftig stärker durch Cyberangriffe oder auch terroristische Bedrohungen gefährdet scheinen. Um hier Wirtschaft und Gesellschaft ausreichend zu schützen gilt es, Augenmaß zu bewahren, damit die Einschränkungen durch das erhöhte Schutzbedürfnis nicht am Ende größer sind, als die Einschränkungen durch die Bedrohung selbst. Aber auch die Unternehmen dürfen in ihrem Engagement beim Schutz vor Straftaten nicht nachlassen. Sei es, dass sie zum Beispiel ihre Mitarbeiter sensibilisieren, ihre Gewerberäume ausreichend absichern oder ihre Computersysteme auf aktuellem Stand halten. Hier helfen die IHKs und ihre Partner durch Informationen und Veranstaltungen.

Alle Straftaten anzeigen

Für weitere sinkende Anzeigewilligkeit der Unternehmen gibt es viele Ursachen. Zum Beispiel kann es Ansicht oder Erfahrung der Unternehmen sein,

dass die Ordnungsbehörden die Täter nur schwer ermitteln können. Aber auch die mangelnde Zahlungsbereitschaft von Versicherungen im Schadensfall kann ein Grund für das im Vergleich zu den vorangegangenen Befragungen weiter wachsende Dunkelfeld sein. Um dem Ruf nach mehr Präsenz der Sicherheitsbehörden Nachdruck verleihen zu können, ist es aber erforderlich, dass die betroffenen Unternehmer künftig alle Straftaten anzeigen.

Digitalisierung der Wirtschaft fördern und schützen

Die Veränderung der Kriminalität und die Digitalisierung des Verbrechens haben erhebliche Auswirkungen auf die Wirtschaft. Das World Wide Web eröffnet Straftätern neue Möglichkeiten. Das Internet der Dinge, vernetzte Produktionstechnik, Fernwartungszugänge für Computersysteme und Maschinen werden die Straftäter in den kommenden Jahren verstärkt nutzen, um Schaden anzurichten. Die Unternehmer sind darauf nicht genügend vorbereitet. Viele sind gerade dabei, ihre Firmen für die Herausforderungen des 21. Jahrhunderts und Wirtschaft 4.0 fit zu machen und ihre Technik zu vernetzen. An eine Folgenabschätzung für den Einsatz der neuen Technik haben die wenigsten Unternehmen, Privatpersonen oder auch Behörden gedacht. Hier gilt es nun, sachlich zu analysieren was der Einsatz neuer Technik neben vielen positiven Aspekten auch an Angriffsfläche für Verbrechen bietet. Die Ergebnisse der Analyse müssen für die Sensibilisierung der Wirtschaft genutzt werden. Hier darf staatliche Technologieförderung nicht nur auf die finanzielle Unterstützung der Unternehmen bei der Investition in neue Technik beschränkt bleiben. Förderung bedeutet auch die Unterstützung beim Schutz der neuen Technik in den Unternehmen.

Lessons Learned

- KMUs sind zunehmend mit IT-Sicherheitsangriffen konfrontiert.
- Sicherheit ist (neben Fachkräftesicherung und Energieversorgung) eines der wichtigsten Managementthemen für KMU.
- Die weitere Sensibilisierung der breiten Unternehmerschaft zu Schutzmaßnahmen im IT-Bereich ist insbesondere bei der zunehmenden Digitalisierung von Geschäftsprozessen notwendig.

5. Sicherheitsrisiken von Internetanwendungen

Michael Hendrix, TH Wildau

Abstract

Die allermeisten Angriffe auf IT-Systeme geschehen heute über die Anwendungsebene und nicht über die Netzwerkebene. Gegen diese Angriffe hilft weder eine Firewall noch ein Intrusion Detection System. Die bedeutendsten Angriffstypen werden kurz erläutert und Schutzmaßnahmen gegen diese diskutiert. Auch wenn die meisten und teilweise wirkungsvollsten dieser Schutzmaßnahmen nur vom Betreiber bzw. Entwickler einer Webanwendung implementiert werden können, hat auch der Nutzer von Webanwendungen Möglichkeiten, sich gegen Angriffe auf der Anwendungsebene zu schützen.

5.1 Motivation

Laut dem Bundesamt für Sicherheit in der Informationstechnik ist die Infektion mit Schadsoftware über Internet und Intranet die Nummer 1 unter den Top 10 Bedrohungen in 2014. Angriffe auf Netzwerke bzw. der dahinterliegenden Infrastruktur verlagern sich mehr und mehr auf die Anwendungsebene. Angriffsversuche über die Netzwerkebene lassen sich heute durch Firewalls, Intrusion Detection Systeme etc. gut verteidigen.

Die Anwendungsebene besteht aus allen sich im Netzwerk befindlichen Anwendungen. Nachfolgend sollen die wichtigsten Angriffstypen auf der Anwendungsebene vorgestellt und geeignete Abwehrmaßnahmen diskutiert werden.

5.2 Überblick

Laut des Sicherheitsunternehmens Vendor waren 2013 von den getesteten realen Webanwendungen 96% angreifbar und es waren im Durchschnitt 14 verschiedene Angriffsmöglichkeiten pro Anwendung vorhanden. Laut der Studie sind die häufigsten vorhandenen Angriffsmöglichkeiten in Webanwendungen die Folgenden:[1]

- Cross Site Scripting (25%)
- Information Leakage (23%)
- Authentication and Authorization (15%)
- Session Management (13%)
- SQL Injection (7%)
- Cross Site Request Forgery (CSRF) (6%)
- Sonstige (11%)

5.3 Schutz einer Webanwendung vor geläufigen Angriffen

Zum Schutz vor den vorgestellten Angriffsmöglichkeiten und zur Vermeidung von angreifbaren Schwachstellen werden im Folgenden die aufgezählten Angriffsmöglichkeiten bzw. sinnvolle Maßnahmen zu Schutz erläutert:

- Authentifizierung
- Stehlen einer Session
- Cross-Site-Request-Forgery (CSRF)
- Cross-Site-Scripting
- SQL-Injection
- Rainbow-Table-Angriffe
- Pufferüberlauf
- Brute-Force-Angriff
- Man-in-the-Middle-Attack

Was Schutzmaßnahmen betrifft, wird zwischen serverseitigen und nutzerseitigen Schutzmaßnahmen unterschieden. Auf serverseitige Schutzmaßnahmen hat der Nutzer einer Webanwendung keinen Einfluss. Diese können nur vom Betreiber der Webanwendung oder vom Entwickler der Anwendung umgesetzt werden. Nutzerseitige Schutzmaßnahmen sind Maßnahmen, die nur vom Nutzer der Webanwendung vorgenommen werden können.

Fast allen nutzerseitigen Schutzmaßnahmen gemeinsam ist die Verwendung eines aktuellen Virenscanners, um die Wahrscheinlichkeit zu verringern, dass das eigene Rechnersystem mit Viren, Würmern, Trojanern etc. infiziert wird. Zu achten ist darauf, dass Updates sowohl des Virenscanners selbst als auch der Signaturdatei automatisch vorgenommen werden. Vorteilhaft ist ein Virenscanner mit proaktiver Erkennung.

Auch regelmäßige Backups von wichtigen Dateien sollten zu den routinemäßigen Schutzmaßnahmen zählen. So ist es eventuell im Falle eines erfolgreichen Angriffs möglich, diese Dateien wieder ins System zurückzuspielen. Achten sollte man darauf, dass das Medium für ein Backup (in der Regel ein Speichermedium, das man über USB mit seinem IT-System verbinden kann) räumlich vom eigentlichen IT-System getrennt ist. Ferner sollte man hin und wieder die auf dem Backup-System gespeicherten Dateien in ein gesondertes Laufwerk auf dem IT-System zurückspielen. Es gibt wohl im Falle eines Datenverlustes keine unangenehmere Überraschung als die Feststellung, dass das Zurückspielen des Backups nicht funktioniert.

5.3.1 Authentifizierung

Eine Webanwendung kann neben öffentlichen und somit ungeschützten Ressourcen auch geschützte Ressourcen beinhalten, für die sich ein Nutzer authentifizieren muss. Das meist verwendete Authentifizierungs-Verfahren ist die Eingabe von Nutzernamen und Passwort.

Serverseitige Schutzmaßnahmen

Bei besonders sicherheitskritischen Anwendungen ist aufgrund der möglichen signifikanten Folgen eines Missbrauchs, eine zweistufige Authentifizierung in Erwägung zu ziehen. In einer ersten Stufe könnte die Eingabe von Nutzername und Passwort erfolgen. Wichtig ist, dass die Übertragung vom Client zum Server verschlüsselt (https) geschieht, da ansonsten auch das Passwort unverschlüsselt über das Netz übertragen wird. Eine zweite Stufe der Authentifizierung könnte ein Zertifikat sein, das z.B. auf einem USB-Dongel oder auf einer Chipkarte gespeichert ist.

Nutzerseitige Schutzmaßnahmen

Zu beachten ist, dass das Passwort ausreichend lang ist (mindestens 8 Zeichen) und sowohl aus Buchstaben, Ziffern und Sonderzeichen besteht. Um einem Wörterbuchangriff vorzubeugen, sollte das Passwort aus einer „zufälligen" Kombination von Zeichen bestehen.

5.3.2 Sessing-Hijacking

Das Stehlen einer Session basiert zunächst einmal auf dem Stehlen der Session-ID des Nutzers einer Webanwendung. Aufgrund der Zustandslosigkeit von HTTP wird eine Session-ID benötigt, um eine Sitzung auf der Serverseite einem Request zuzuordnen. Eine Session-ID wird auf der Clientseite in einem Cookie hinterlegt. Hat der Benutzer seine Cookies deaktiviert, so wird die Session ID als GET-Parameter an die URL angehängt. Gelangt der Angreifer in den Besitz der Session-ID, so bildet er den Cookie bzw. URL GET-Paramater nach und übernimmt die Session. Der Angreifer ist dadurch mit den Rechten des Opfers an der Webanwendung angemeldet und kann diesen Rechten entsprechende Operationen durchführen.

Um an die Session-ID zu gelangen, gibt es viele Möglichkeiten. Die geläufigsten sind:

- Cross-Site-Scripting (XSS) mit dem Ziel, die Session-ID im Browser auszulesen
- URLs aus dem Browserverlauf oder Server-Logs, die die Session-ID beinhalten
- Man-in-the-Middle Angriff
- Sniffer-Programme auf dem Client

Serverseitige Schutzmaßnahmen

Eine der wirkungsvollsten Maßnahmen gegen das Ausspähen der Session-ID ist eine Verschlüsselung der HTTP-Verbindung durch SSL. Der Angreifer müsste dann zunächst einmal diese Verschlüsselung knacken, um dann nach der Session-ID zu sniffen. Trotzdem sollte man das Mitführen der Session-ID über die URL deaktivieren und ein Session-Timeout einführen. Ebenso sollte die Webanwendung gegen Cross-Site-Scripting Angriffe durch entsprechende Validierung und Maskierung der Input-Daten immun sein. Bei wichtigen bzw. sicherheitsrelevanten Operationen wie z.B. das Herunterfahren von Turbinen etc. sollte eine Re-Authentifizierung verlangt werden.

Nutzerseitige Schutzmaßnahmen

Die Einstellungen im Browser sollten so gewählt sein, dass Cookies für die Webanwendung erlaubt sind. Ist dies nicht der Fall, eröffnet sich durch das Mitführen der Session-ID in der URL eine weitere Möglichkeit zum Ausspähen. Das versehentliche Mitschicken der Session-ID in einer URL, die in eine E-Mail kopiert wurde, entfällt durch die Verwendung von Cookies ebenso. Dass man Sessions auch durch XSS-Lücken hijacken kann, liegt daran, dass man mittels JavaScript den Cookie aus dem Document Object Model (DOM) mit dem Befehl document.cookie auslesen kann. Auch auf der Clientseite können XSS-Attacken erkannt und verhindert werden, durch entsprechende Browser-Plugins wie z.B. NoScript (Firefox) bzw. ScriptSafe (Google Crome), die die Input-HTML-Elemente und URLs auf Cross-Site-Scripting untersuchen.

5.3.3 Cross-Site-Request-Forgery (CSRF)

Bei einem CSRF-Angriff wird dem Benutzer ein Befehl für eine Webanwendung (z.B. ein Link in einem Gästebuch) von einem Angreifer übermittelt. Klickt der Benutzer nun diesen Link an, wird der Befehl an die Webanwendung gesendet und im Kontext des Benutzers ausgeführt. Falls nun dieser Benutzer an dieser Webanwendung angemeldet ist, wird die Vertrauensstellung des Benutzers gegenüber der Webanwendung ausgenutzt und der Befehl mit den Rechten des Benutzers ausgeführt.

Serverseitige Schutzmaßnahmen

Bei einem CSRF-Angriff muss ein gültiger HTTP-Request nachgestellt und an das Opfer übermittelt werden. Ein solcher HTTP-Request kann z.B. durch eine URL auf die Webanwendung abgebildet werden (z.B. http://meine-webapp.tld/updateUser? name=benutzer).

Als Schutz gegen solche Angriffe kann unter anderem ein geheimer Token helfen, der bei jedem Seitenaufruf der Webanwendung vorzugsweise in einem Hidden-Field eines Formulars mitübertragen wird.

Auch das Referrer-Feld im HTTP-Request, das die URL der Webanwendung enthält, kann als ein Sicherheitsmerkmal benutzt werden.

Die Sicherheitsmechanismen zum Schutz vor CSRF-Angriffen, die auf das Referrer-Feld oder einen zusätzlichen Token basieren, können durch Cross-Site-Scripting-Angriffe umgangen werden. Deswegen ist die korrekte Filterung von Benutzerdaten entscheidend für die Wirksamkeit der Sicherheitsmaßnahmen zum Schutz vor CSRF-Angriffen.

Nutzerseitige Schutzmaßnahmen

Die einfachste Möglichkeit, solche Angriffe zu erschweren, sind Sicherheitsmechanismen, die es ermöglichen, beabsichtigte Seitenaufrufe des Benutzers von unbeabsichtigt weitergeleiteten Befehlen Dritter zu unterscheiden. Für den Nutzer einer Webanwendung bedeutet dies, dass er, während er mit der Webanwendung verbunden ist, keine Links außerhalb der Webanwendung anklickt. Falls die Webanwendung einen LogOut-Button besitzt, sollte dieser unbedingt betätigt werden.

5.3.4 Cross-Site-Scripting (XSS)

Beim Cross-Site-Scripting handelt es sich um Angriffe, die die clientseitige Skriptausführung (JavaScript) unerlaubterweise verwenden. Möglich wird dies durch ungefilterte Benutzereingaben, die an den Webserver gesendet und beim erneuten Seitenaufbau im HTML verankert werden. Dieser Schadcode wird anschließend unerkannt ausgeführt. Dadurch können kleine Schadprogramme eingeschleust werden, die oftmals Identitätsdaten stehlen oder Cookies auslesen. Diese Schadprogramme können auch Keylogger sein, die die Benutzereingaben abgreifen. Auch ein Zugriff auf Anwendungsdaten und deren Manipulation ist möglich.

Serverseitige Schutzmaßnahmen

Um Cross-Site-Scripting zu verhindern, muss man zunächst einmal immer davon ausgehen, dass sämtliche Nutzereingaben in der Webanwendung mögliche Angriffe sein können. Deshalb sollte eine Webanwendung Nutzereingaben auf Gültigkeit bzw. Plausibilität prüfen.

Besonderes Augenmerk sollte auch auf die serverseitige Maskierung der Daten gelegt werden, die zurück an den Nutzer übermittelt werden. Damit ist gemeint, dass sämtliche Zeichen, die zur Ausführung eines Scripts innerhalb

des Browsers verwendet werden können, serverseitig maskiert werden (z.B. wird < durch < ersetzt). Zeichen, die der Interpreter zum Ausführen von JavaScript benötigt, werden zwar korrekt im Browser angezeigt, jedoch verbirgt sich dahinter eine Maskierung, sodass die Ausführung eines Skripts nicht möglich ist.

Nutzerseitige Schutzmaßnahmen

Außer dem Abschalten von JavaScript im Browser kann der Nutzer nicht viel tun, um XSS zu verhindern. Dies ist in der Regel aber keine sinnvolle Lösung, da mit dem Abschalten von JavaScript eine größere Anzahl von Webanwendungen nicht mehr korrekt funktioniert.

Eine Alternative zum Abschalten von JavaScript ist die Verwendung von Browser-PlugIns wie NoScript (Firefox) oder ScriptSafe (Google Crome). Diese PlugIns können konfiguriert werden, sodass man festlegen kann, von welchen Webseiten JavaScript blockiert bzw. erlaubt ist. Neben JavaScript können auch andere Mechanismen wie z.B. iFrames, Adobe Flash etc. blockiert werden.

5.3.5 SQL-Injection

Bei dieser Angriffsmethode geht es darum, dass SQL-Befehle, getarnt als POST- oder GET-Parameter, in die Webanwendung eingeschleust werden und dort unerwünschte SQL-Statements absetzen. Dadurch kann der Angreifer z.B. Daten erzeugen, auslesen, ändern oder löschen.

Serverseitige Schutzmaßnahmen

Um SQL-Injection zu verhindern, sollte auch hier, wie beim Schutz gegen XSS, Augenmerk auf die Validierung und Maskierung sämtlicher Benutzereingaben gelegt werden.

Eine weitere serverseitige Schutzmaßnahme ist die Verwendung von vorkompilierten SQL-Befehlen (Prepared Statements) bzw. die Nutzung von objektrelationalen Abstraktionen.

Nutzerseitige Schutzmaßnahmen

keine

5.3.6 Rainbow-Table-Angriff

Passworte sollten aus Sicherheitsgründen nur als Hashwert in einer serverseitigen Datenbank gespeichert werden. Bei einem direkten Einbruch in die Datenbank wären damit die gestohlenen Nutzernamen und Passworte für einen Angreifer wertlos, da er sich mit dem Hashwert des Passwortes nicht bei einer Webanwendung authentifizieren kann. Ein Rainbow-Table-Angriff dient dazu, aus dem Hashwert eines Passwortes wieder das Klartext-Passwörter zu bestimmen.

Bei einer Rainbow-Table handelt es sich um eine ganz bestimmte Strukturierung bzw. Abbildung von Wertepaaren (Klartext – Hashwert) mit dem Ziel, einen guten Kompromiss zwischen einer schnellen Suche nach dem Klartext-Passwort und einer nicht zu großen Anzahl von Wertepaaren zu finden.

Serverseitige Schutzmaßnahmen

Die Generierung von Rainbow-Tables kann serverseitig mittels Salt und/oder Pepper unwirtschaftlich gemacht werden. Sowohl bei Salt als auch bei Pepper werden zufällig generierte Werte an das Passwort gehängt, bevor der Hashwert ermittelt und dann in der Datenbank gespeichert wird. Das Salt wird zusammen mit dem Hashwert des Passwortes gespeichert, das Pepper ist für alle Passworte dasselbe. Sowohl Salt als auch Pepper führen dazu, dass die Rainbow-Table deutlich größer wird als ohne diese Zutaten.

Der Aufwand, der getrieben werden muss, um ein gehashtes Passwort wieder in seinen Klartext zu überführen, kann auch durch mehrfaches Hashen mit Salts drastisch erhöht werden.

Nutzerseitige Schutzmaßnahmen

Um eine Webanwendung gegen Rainbow-Table-Angriffe sicherer zu machen, sollte das verwendete Passwort möglichst lang gewählt werden, da die Größe einer Rainbow Table mit der Länge der Passwörter steigt und die Berechnung je nach Hashverfahren ab einer gewissen Passwortlänge nicht mehr wirtschaftlich ist.

5.3.7 Pufferüberlauf

Ein Pufferüberlauf (eng. buffer overflow) entsteht, indem es einem Angreifer gelingt, über Eingabefelder mehr Daten in einen Speicherbereich zu schreiben als dieser maximal aufnehmen können sollte. Diese gezielt verursachten Überläufe von Speicherbereichen resultieren auf einem Programmfehler und führen u.a. dazu, dass Schadsoftware in andere Speicherbereiche geladen und ausgeführt wird.

Diese Art des Angriffs gilt als eine der gefährlichsten in der Netzwelt. Fast ausgeschlossen sind Pufferüberläufe jedoch in modernen Programmiersprache wie Java oder C#, da dort die Speicherblöcke von der Laufzeitumgebung dieser Programmiersprachen überwacht werden. Allerdings kann das Risiko eines Pufferüberlaufs auch bei modernen Sprachen aufgrund von möglichen Fehlern in deren Laufzeitumgebungen nicht gänzlich ausgeschlossen werden. Ältere Programmiersprachen wie C oder C++ bieten von sich aus keinen Schutz vor einem Pufferüberlauf.

Serverseitige Schutzmaßnahmen

Wie bereits erwähnt, entstehen Pufferüberlauf-Schwachstellen durch Programmierfehler. Eine Möglichkeit, Pufferüberläufe weitgehen zu vermeiden, ist, die Länge eines Datenblocks zu überprüfen, bevor er in einen Puffer fester Größe kopiert wird. Diese Überprüfung muss softwaretechnisch umgesetzt werden.

Weitere Möglichkeiten, ein System vor den Folgen von Pufferüberlauf-Schwachstellen zu schützen, ist die Speicherung eines zusätzlichen canary-Parameters, die Data Execution Prevention (DEP) Technik oder das Address Space Layout Randomization (ASLR) Verfahren. Auf diese drei Möglichkeiten soll an dieser Stelle aber nicht näher eingegangen werden.

Nutzerseitige Schutzmaßnahmen

keine

5.3.8 Brute-Force-Angriff

Brute-Force-Angriffe werden von Angreifern durchgeführt, die versuchen, ein Passwort für eine Applikation zu entschlüsseln. Dabei entwerfen sie eine Software, die systematisch in einer schnellen Abfolge die verschiedensten Kombinationen von Zeichen ausprobiert, um somit an das Passwort zu gelangen.

Serverseitige Schutzmaßnahmen

Als Betreiber einer Webanwendung ist es möglich, den Benutzer durch Validierung dazu zu zwingen, ein sicheres Passwort zu erstellen. Darüber hinaus könnte der Server bei einem fehlerhaften Versuch der Passworteingabe den Zeitabstand zum nächstfolgenden Versuch kontinuierlich erhöhen.

Nutzerseitige Schutzmaßnahmen

Ein Mittel, um sich gegen solche Attacken schützen zu können, ist, ein sicheres Passwort zu erstellen. Ein sicheres Passwort sollte aus mindestens 8, besser aus mehr Zeichen, bestehen, wobei sowohl Klein- und Großbuchstaben als auch Ziffern als auch Sonderzeichen vorhanden sein sollten. Wichtig ist auch, dass das Passwort nicht in einem Wörterbuch steht (Stichwort: Wörterbuch-Angriff). Merksätze sind ein gutes Mittel, um Passworte zu erzeugen und auch zu behalten.

5.3.9 Man-in-the-Middle-Attacke

Als Man-in-the-Middle-Attack bezeichnet man die Positionierung eines Angreifers zwischen Nutzer und Webanwendung, um somit gegenüber dem Nutzer als Webanwendung und gegenüber der Webanwendung als Nutzer zu agieren. Durch eine Man-in-the-Middle (MITM) Attacke können Angreifer so die Kommunikation ausspionieren oder Daten nach Wunsch des Angreifers verändern, um z.B. Zugangsdaten, Session Cookies, Dateien etc. auszuspionieren und bspw. Steuerbefehle etc. zu verändern, sofern diese zwischen Nutzer und Webanwendung ausgetauscht werden. Diese Attacke ist für das Opfer und die Webanwendung schwer zu erkennen.

Serverseitige Schutzmaßnahmen

Die Implementierung einer verschlüsselten Verbindung zwischen Nutzer und Webanwendung per https ist eine der besten Abwehrmaßnahmen gegen MITM.

Nutzerseitige Schutzmaßnahmen

Bei sicherheitsrelevanten Aktionen wie z.B. Online-Banking sollte der Nutzer selbst darauf achten, dass der Zugriff auf den Bankserver mittels https geschieht und dass das entsprechende Sicherheits-Zertifikat tatsächlich zur Banking-Anwendung gehört. Auch bei allen Eingaben von z.B. Kreditkarteninformationen sollte der Nutzer darauf achten, dass die Kommunikation mit der Webanwendung via https abläuft.

Lessons Learned

- Es soll immer ein Passwort mit mindestens acht Zeichen gewählt werden. Dieses soll aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen bestehen und soll kryptisch sein. Verschiedene Webanwendungen verlangen verschiedene Passwörter.
- Der Virenscanner (bevorzugt mit proaktiver Erkennung) und die Signaturdatei sollen immer auf dem aktuellen Stand sein.
- Es sind regelmäßig Backups von wichtigen Dateien zu machen.
- Es ist überlegenswert, Browser-PlugIns zur Verhinderung von Cross-Site-Scripting zu verwenden.
- Betriebssystem und verwendete Browser sollten auf dem aktuellen Stand sein. Automatische Updates sind meistens sinnvoll.
- Bei sicherheitskritischen Anwendungen (z.B. Online-Banking, Senden von Kreditkarteninformationen) soll darauf geachtet werden, dass eine https-Verbindung besteht. Es wird empfohlen, für sicherheitskritische Anwendungen einen separaten Browser zu nutzen.
- Cookies sollen im Browser nicht abgeschaltet werden.
- Während man mit einer Webanwendung kommuniziert, sollen keine externen Links angeklickt werden.

[1] Cenzic (2014). Application Vulnerability Trends Report. Aufgerufen am 20.07.2017. Verfügbar unter https://www.infopoint-security.de/medien/cenzic-vulnerability-report-2014.pdf.

6. Datenlecks in Handwerksbetrieben

Heiko Behrendt, ISO 27001 Auditor

Abstract

Handwerksbetriebe setzen für die Kalkulation, Konstruktion und Fertigung ihrer Produkte komplexe und vernetzte IT-Systeme ein. Dabei entstehen viele sensible Daten, die immer mehr zum Rückgrat der Geschäftsprozesse des Handwerksbetriebs werden. Wer noch nicht bei der Datenverarbeitung dem Datenschutz und der Informationssicherheit ausreichend Rechnung trägt, geht hohe Risiken ein. Die Geschäftsführung sollte sich dann darüber im Klaren sein, dass bei einem Datenleck dem Handwerkbetrieb hohe finanzielle Schäden drohen.

6.1 Einleitung

Datenschutz und Informationssicherheit sollte im Handwerkbetrieb angemessen nach der Schutzbedürftigkeit der verarbeiteten Daten umgesetzt werden. Zu beachten sind dabei u.a. das Bundesdatenschutzgesetz und die ab dem 25. Mai 2018 geltende neue EU-Datenschutz-Grundverordnung für die Verarbeitung von personenbezogenen Daten sowie interne Betriebsvorgaben (Compliance) zur Sicherstellung der Aufrechterhaltung der Geschäftsprozesse. Für die Umsetzung der Anforderungen sind insbesondere technische und organisatorische Maßnahmen zu ergreifen, die vorhandenen Gefährdungen im Bereich der Gebäude, der Räume, der Maschinen, der Anwendungen mit Daten, der IT-Systeme und des Datenkommunikationsnetzes reduzieren.

Stellen Sie sich folgende Ereignisse vor:

- Ihre Kunden und/oder Lieferanten erhalten davon Kenntnis, dass die in Ihrem Handwerksbetrieb gespeicherten Daten in unbefugte Hände gelangt sind.

- Sie können Ihre Aufträge aufgrund von Datenverlusten, Datenmanipulationen oder einem längeren Ausfall Ihrer IT-Systeme und/oder Produktionsmaschinen nicht erwartungsgemäß erfüllen.
- Mitarbeiter oder Fremdpersonal ziehen die Angebotskalkulationsdaten von Ihren IT-Systemen ab und spielen sie der Konkurrenz zu.

Diese Szenarien möchte man niemandem wünschen, doch leider zeigt die Realität, dass auch in Handwerksbetrieben die Gefährdungen beim Einsatz von Informationstechnik zunehmen.

Nachfolgend einige typische Sachverhalte aus der Praxis für den Selbsttest:

Selbsttest mit 20 Fragen	Ist mir egal	Weiß ich nicht	In meinem Betrieb okay
1. Fremdpersonen können ungehindert ins Gebäude gelangen und sich ohne Aufsicht fortbewegen.	O	O	O
2. Ein Schlüsselbestandsbuch für Büro- und Funktionsräume wird nicht geführt, sodass nicht nachvollziehbar ist, wer über welche Zutrittsbefugnisse verfügt.	O	O	O
3. Einen Überblick über den Bestand und die Ausgabe der (General-)Schlüssel besteht nicht.	O	O	O
4. Konstruktions-, Angebots- und Kundenakten werden in den Büros außerhalb der Geschäftszeiten nicht in verschließbaren Behältnissen verschlossen.	O	O	O
5. Papierabfälle mit Geschäftsdaten werden durch Dritte (Reinigungsdienst) unkontrolliert in für Unbefugte zugängliche Papiertonnen entsorgt.	O	O	O
6. Der Reinigungsdienst verfügt über Generalschlüssel und reinigt außerhalb der Geschäftszeiten, wenn alle Mitarbeiter abwesend sind.	O	O	O

7. Die Mitarbeiter verwenden für den Zugriff auf die IT-Systeme und Anwendungen triviale Kennwörter.	O	O	O
8. Welchen Mitarbeitern welche Berechtigungen auf IT-Komponenten, Anwendungen und Daten zugewiesen wurden, können „Datenverantwortliche" nicht nachvollziehen.	O	O	O
9. Die Kennwörter für die Installation der IT-Komponenten wurden nicht geändert.	O	O	O
10. Die Administrationskennwörter für die einzelnen IT-Komponenten sind einheitlich und allen Administratoren und IT-Dienstleistern bekannt.	O	O	O
11. Es können ohne Einschränkungen private Speichermedien, wie z.B. Sticks oder Speicherkaten, an PCs, Notebooks und Smartphones angeschlossen und genutzt werden.	O	O	O
12. Die Mitarbeiter können selbständig Programme/Apps installieren.	O	O	O
13. Geschäftsdaten auf Datenträgern werden nur logisch gelöscht und können deshalb mit einfachen Tools wiederhergestellt werden.	O	O	O
14. Datenträger in Notebooks oder Sticks, die außerhalb des Handwerksbetriebs genutzt werden, sind nicht verschlüsselt.	O	O	O
15. Auf der Festplatte des Digitalkopierers werden alle Kopier- und Druckaufträge dauerhaft gespeichert, sodass nach Ablauf der Leasingzeit das Gerät mit allen Daten den Handwerksbetrieb verlässt.	O	O	O
16. Ein Viren- und Patchmanagement findet nur unregelmäßig statt.	O	O	O
17. Bei E-Mail- und Webnutzung können uneingeschränkt Dateien und Programme auf PCs, Notebooks und Smartphones gespeichert und genutzt werden.	O	O	O

18. Externe IT-Dienstleister haben aus der Ferne uneingeschränkten und unkontrollierten Zugang zu betrieblichen IT-Systemen.	O	O	O
19. Die Datensicherung wird unvollständig und unregelmäßig durchgeführt. Die Datensicherungsmedien werden nicht ausreichend sicher aufbewahrt.	O	O	O
20. Die Sicherheitseinstellungen auf der Firewall sind nur dem IT-Dienstleister bekannt und können von ihm ohne Absprache mit dem Handwerksbetrieb geändert werden.	O	O	O

Tabelle 2: Selbsttest zu potentiellen Gefährdungen in (Handwerks-)Betrieben.

Je mehr in der ersten oder zweiten Spalte von Ihnen angekreuzt wurde, desto höher ist die Gefahr, dass in Ihrem Handwerksbetrieb ein Datenleck entsteht bzw. Ihre Datenverarbeitung durch Störungen beeinträchtigt werden kann.

6.2 Datenschutz

Der Datenschutz in Handwerksbetrieben ist rechtlich dann von Bedeutung, wenn personenbezogene Daten verarbeitet werden, was wohl in den meisten Handwerksbetrieben der Fall sein dürfte.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse (z.B. Adresse, Telefonnummer, E-Mail-Adresse, Geburtsdatum, Fotos) einer bestimmten oder bestimmbaren Person (Mitarbeiter, Kunden oder Lieferanten). Auch Daten ohne direkten Personenbezug können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen Bezug genommen werden kann (z.B. Personalnummer, PC-Benutzerkennung). Die Datenschutzvorschriften wollen die Persönlichkeitsrechte der Betroffenen schützen.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist deshalb nur zulässig, wenn die Datenschutzvorschriften dies erlauben oder wenn der Betroffene freiwillig eingewilligt hat. Die Daten müssen für die Zwecke, für die sie erhoben und verarbeitet werden, relevant sein. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es der Zweck, zu dem sie

erhoben oder verarbeitet wurden, erfordert. Nicht mehr erforderliche Daten sind zu löschen und unrichtige Daten zu berichtigen.

Bei Verstößen gegen diese Vorschriften können dem Betrieb von den Aufsichtsbehörden der Länder empfindliche Geldbußen auferlegt werden. Hat der Handwerksbetrieb mindestens 10 Mitarbeiter, die mit personenbezogenen Daten im Betrieb arbeiten, ist sogar ein betrieblicher Datenschutzbeauftragter zu bestellen, der für die Einhaltung und Überwachung der Datenschutzvorschriften zuständig ist.

6.3 Hinweise zur neuen EU-Datenschutz-Grundverordnung (EU-DSGVO)

Die neue EU-Datenschutz-Grundverordnung verlangt von den Verantwortlichen die Einführung eines Datenschutz- und Informationssicherheitsmanagement zur Einhaltung der Datenschutzvorschriften. Dies bedeutet, dass im Gegensatz zu den bisherigen Datenschutzvorschriften (BDSG) strengere Regeln und höhere Anforderungen gelten. Insbesondere werden die Anforderungen an die Dokumentation der Datenverarbeitungsprozesse sowie die Umsetzung technischer und organisatorischer Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen mit der EU-Datenschutz-Grundverordnung erhöht. Darüber hinaus hat der von der Datenverarbeitung Betroffene deutlich mehr und umfangreichere Rechte als bisher. Auch wird die Aufsichtsbehörde in seiner Rechtsstellung und seinen Befugnissen deutlich aufgewertet, sodass zukünftig mit mehr Kontrollen und bei Verstößen gegen die Datenschutzvorschriften mit höheren Bußgeldern zu rechnen ist.

6.4 Informationssicherheit

Die Informationssicherheit verfolgt das Ziel, die Datenverarbeitung innerhalb der Geschäftsprozesse im Handwerksbetrieb vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung zu schützen. Gleichzeitig ist durch die Festlegung und Umsetzung von technischen und organisatorischen Maßnahmen darauf hinzuwirken, dass die Datenschutzvorschriften eingehalten werden.

Die richtigen und angemessenen Schutzmaßnahmen für den Handwerksbetrieb festzulegen, ist nicht trivial und erfordert viel Know-how im Bereich Datenschutz und Informationssicherheit. Experten auf diesem Gebiet sind in der Lage, für den Handwerksbetrieb ein passendes Konzept zu entwickeln.

Zu überlegen wäre auch, ob der Handwerksbetrieb anerkannte Informationssicherheitsstandards anwendet. Zu nennen wäre das Bundesamt für Sicherheit in der Informationstechnik (BSI), das den Grundschutzstandard entwickelt hat. Hierzu gehören Maßnahmen zur Erreichung und Aufrechterhaltung der Informationssicherheit. Das Konzept der Grundschutzvorgehensweise besteht in der Zugrundelegung elementarer Gefährdungen und sieht für sie entsprechende technische und organisatorische Schutzmaßnahmen vor. Bei vollständiger Umsetzung kann sogar eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz angestrebt werden.

Die Anwendung des Grundschutzstandards hat den Vorteil, dass z.B. für Infrastruktur, Systeme, Netz und Anwendungen bereits viele Maßnahmen in sogenannten Bausteinen vorgegeben werden. Allerdings bedarf das Handling des Grundschutzstandards Spezialkenntnisse auf diesem Gebiet, sodass kleinere und mittlere Handwerksbetriebe ohne fachliche Unterstützung oftmals mit der Umsetzung überfordert sind.

Mit Hilfe der Software „Verinice" werden die Infrastruktur, die IT-Systeme, das lokale Netz und die Anwendungen eines Handwerksbetriebs erfasst und ihnen nur elementare Schutzmaßnahmen der Grundschutzbausteine zugeordnet. Für den Handwerksbetrieb weniger bedeutsame Schutzmaßnahmen wurden hingegen nicht berücksichtigt. Mit dem neuen modernisierten Grundschutz wird das BSI ab 2018 auch ein Stufenmodell anbieten, sodass über eine sogenannte Basisabsicherung bedeutsame Geschäftsprozesse mit einem überschaubaren Maßnahmenbündel abgesichert werden können.

Über den Einsatz des Tools erhält der Handwerksbetrieb eine umfassende Transparenz der festgelegten Maßnahmen. Der Umsetzungsstand der Maßnahmen kann im Tool dokumentiert werden.

6.5 Was ist zu tun?

Der Umfang der umzusetzenden Schutzmaßnahmen hängt davon ab, wie viele Risiken Sie eingehen können bzw. wollen. Um es besser auf den Punkt zu bringen, sollte auf jeden Fall das Schutzniveau für die in Ihrem Handwerksbetrieb definierten Werte bzw. Objekte festgelegt werden. Dazu gehören nicht nur die IT-Systeme mit den Daten, sondern beispielsweise auch die Gebäude, die Räume und die Produktionsmaschinen. Anhand der Grundwerte „Verfügbarkeit", „Integrität" und „Vertraulichkeit" legen Sie nun jeweils für jedes Objekt fest, welchen Stellenwert es für die Aufrechterhaltung des entsprechenden Geschäftsprozesses bekommt.

Beispiel 1: Eine Produktionsmaschine darf nicht länger als drei Stunden ausfallen, weil jede Stunde Ausfall einen finanziellen Schaden von beispielsweise 5.000 Euro verursacht. Insofern werden an die Produktionsmaschine und an die mit ihr vernetzten IT-Systeme erhöhte Anforderungen an die Verfügbarkeit gestellt. Als technische und organisatorische Maßnahmen könnten z.B. eine abgesicherte Stromversorgung, das Vorhalten von Maschinenersatzteilen, der Betrieb redundanter IT-Systeme und eine regelmäßige Wartung umgesetzt werden.

Beispiel 2: Die Anwendungssoftware für die Konstruktion von Werkstücken muss exakte und richtige Berechnungen liefern. Die Integrität der erfassten Daten muss sichergestellt sein und darf nicht durch Fehler in der Software in Frage gestellt werden. Die zu ergreifenden Schutzmaßnahmen wären z.B. ein regelmäßiges Patch- und Updatemanagement für Software und Betriebssysteme, eine restriktive Berechtigungsvergabe und der Test der Funktionen der Anwendungssoftware auf einem Testsystem.

Beispiel 3: Die Entwicklungsdaten einer CNC-Anwendung für die Herstellung eines Werkstücks sind sehr vertraulich und dürfen auf keinen Fall in unbefugte Hände gelangen. Die Vertraulichkeit der Daten wird darüber hinaus vom Kunden erwartet und wurde vertraglich vom Handwerksbetrieb zugesichert. Die für die Anwendung/Daten zu ergreifenden Schutzmaßnahmen erstrecken sich aufgrund des im Handwerksbetrieb verwendeten Datenkommunikationsnet-

zes über alle daran angeschlossenen IT-Systeme. Dazu gehören z.B. die Absicherung der Schnittstellen am PC, Maßnahmen für den sicheren Anschluss an das Internet, eine Datenabschottung durch Berechtigungsvergabe bis hin zur Verschlüsselung der Daten.

So werden alle „Objekte", die für die Aufrechterhaltung eines Geschäftsprozesses notwendig sind, im Rahmen einer Gefährdungsanalyse betrachtet. In Abhängigkeit zu den einzelnen Objekten werden die ermittelten Gefährdungen auf ihre Eintrittswahrscheinlichkeit bewertet und ihnen entsprechende technische und organisatorische Maßnahmen zur Reduzierung des Risikos gegenübergestellt.

Im Ergebnis erhalten Sie so punktgenaue Schutzmaßnahmen für die in Ihrem Handwerksbetrieb zu schützenden Objekte bzw. für die Datenverarbeitung in papierener und digitaler Form.

6.6 Fazit

Um den Datenschutz und die Informationssicherheit vollständig und beständig in Ihrem Handwerksbetrieb zu implementieren, sollten Sie bzw. ein von Ihnen beauftragter Experte die nachfolgenden Lessons Learned umsetzen.

Lessons Learned

- Einrichtung von Zuständigkeiten und Aufgabenzuweisung für Datenschutz und Informationssicherheit sowie Schulung und Sensibilisierung aller Mitarbeiter.
- Bestandsaufnahme der Gebäude, der Räume, der Maschinen der Anwendungen mit Daten, der IT-Systeme und des Datenkommunikationsnetzes (Objekte).
- Festlegung des Schutzniveaus für die verifizierten Objekte.
- Lokalisierung von Gefährdungen und Priorisierung für ihre Beseitigung bzw. Reduzierung.
- Festlegung und Umsetzung von technischen und organisatorischen Maßnahmen in Anlehnung an das festgelegte Schutzniveau und unter Beachtung der Datenschutzvorschriften.
- Gegebenenfalls effiziente Anwendung des Grundschutzstandards des BSI unter Einsatz von "Verinice" oder anderen vergleichbaren Tools.
- Mit Tools können schützenswerten Objekte und einschlägige, umgesetzte Maßnahmen dokumentiert werden.

7. Viren und Trojaner: Übersicht und Abwehr

Manuela Püschel, Die Netz-Werker AG

Abstract

Hacker versuchen mit Ransomware (Erpressungssoftware), Trojanern und anderer Schadsoftware IT-Systeme zu infiltrieren. Neben den Schwachstellen in IT-Systemen helfen ihnen dabei häufig die Nutzer selbst durch ihre ausgeprägte Leichtsinnigkeit. Zwar ist es schwierig, sich gegen alle Angriffsszenarien vollständig zu schützen. Jedoch gibt es Mittel und Wege, es den Angreifern deutlich zu erschweren. Dieser Beitrag zeigt Möglichkeiten auf, wie dies in der Praxis gelingt.

7.1 IT-Sicherheit bei der Netz-Werker AG

Eine Kernkompetenz der Netz-Werker AG ist die Entwicklung von IT-Strategien für Unternehmen. Dabei besteht eine IT-Strategie aus vielen Bausteinen. Ein zentraler Baustein ist hierbei die IT-Sicherheit, die eng in eine IT-Strategie eingeflochten werden muss. Weitere Themenstellungen in denen Kernkompetenzen vorliegen, sind folgend aufgeführt:

- Systemintegration
- Netzwerksicherheit
- Virtualisierung
- Implementierung von Server based Computing
- Voice-over-IP Installation
- RZ-Hosting
- Erstellen von IT-Gutachten
- Hardware- und softwareseitige Betreuung

Der IT-Bereich gehört zu den schnelllebigsten überhaupt, weshalb regelmäßige Schulungen der Mitarbeiter sowie Zertifizierungen durchgeführt werden, um auf höchstem Niveau beraten zu können und als Premium-Partner aner-

kannt zu werden. Diese Qualität zeigt sich unter anderem in der ISO Zertifizierung und unzähligen Partnerschaften zu namhaften Herstellern von Hard- und Software wie HP, VMware, Veeam, Citrix, SonicWall, WYSE, Microsoft, Swyx Silvee. Dabei soll vor allem die Zusammenarbeit mit SonicWall im Bereich der IT-Sicherheit herausgestellt werden.

Die Arbeit mit unseren Kunden zeigt jedoch, dass es häufig erst notwendig ist, über Grundbegrifflichkeiten zu sprechen, um darauf aufbauend tiefer einzutauchen. Dies gilt umso mehr für die IT-Sicherheit, weshalb ebenso in diesem Beitrag zunächst Grundbegriffe geklärt werden.

7.2 Die Begrifflichkeit Virus

Seit 1985 sind Viren in Computernetzen bekannt, aber was ist ein **Virus** im Computerumfeld eigentlich? Ein Computervirus (lateinisch virus ‚Gift, Schleim) ist ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion.

Viren verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben. Ein teilweise defektes Virus wird „Intended Virus" genannt. Dieses bewirkt meist nur eine „Erstinfektion" einer Datei, kann sich jedoch nicht weiter reproduzieren.

Der Ausdruck Computervirus wird umgangssprachlich auch für Computerwürmer und Trojanische Pferde (kurz, wenn auch falsch: Trojaner) genutzt, da es oft Mischformen gibt und für Anwender der Unterschied kaum zu erkennen ist.

Ist ein Virus einmal gestartet, kann es Veränderungen am Betriebssystem oder an weiterer Software vornehmen (Schadfunktion), was mittelbar auch zu Schäden an der Hardware führen kann (z.B. Überhitzung). Dabei stellen Viren die älteste Malwareform (Schadsoftware) dar. Der Begriff Malware gilt als Oberbegriff.

7.3 Malwareinfektion und -Impfung

"Malwareinfektion"

Ein Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netze wie dem Internet und versucht, in andere Computer einzudringen.

Ein Trojanisches Pferd ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Programmteil, oft Spyware oder eine Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Eine Hintertür (Backdoor) ist eine verbreitete Schadfunktion, die üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Sie ermöglicht Dritten einen unbefugten Zugang („Hintertür") zum Computer, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt, um den kompromittierten Computer als Spamverteiler oder für Denial-of-Service-Angriffe (kurz: DoS) zu missbrauchen.

Ransomware[1] (von englisch ransom für „Lösegeld"), auch Erpressungstrojaner, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

Ransomware kann auf den gleichen Wegen wie ein Computervirus auf einen Computer gelangen. Zu diesen Wegen zählen präparierte E-Mail-Anhänge, die Ausnutzung von Sicherheitslücken in Webbrowsern oder über Datendienste wie Dropbox.

Es kann passieren, dass Systeme blockiert werden und ein Arbeiten an dem betroffenen Rechner oder Netzwerk nicht mehr möglich ist. Ein weiterer Schaden kann entstehen, indem nur Dokumente verschlüsselt werden.

Spyware und Adware[2] spionieren den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller oder andere Quellen, um diese entweder zu verkaufen oder um gezielt Werbung zu platzieren. Diese Form von Malware wird häufig zusammen mit anderer, nützlicher Software installiert, ohne den Anwender zu fragen, und bleibt auch häufig nach deren Deinstallation weiter tätig.

Als **Spyware** werden Programme bezeichnet, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten.

Mit **Adware** wird Software klassifiziert, die –häufig zusammen mit gewünschten Installationen oder Webabrufen– ohne Nachfrage und ohne Nutzen für den Anwender Funktionen startet, die der Werbung oder auch Marktforschung dienen.

Scareware[3] ist darauf angelegt, den Benutzer zu verunsichern und ihn zu verleiten, schädliche Software zu installieren oder für ein unnützes Produkt zu bezahlen. Beispielsweise seien gefälschte Warnmeldungen über einen angeblichen Virenbefall des Computers genannt.

Grayware[4] wird teils als eigene Kategorie benutzt, um Software wie Spyware und Adware oder andere Varianten, die Systemfunktionen nicht direkt beeinträchtigen, von eindeutig schädlichen Formen abzugrenzen.

Rogueware[5] (auch Rogue-Software, Rogue-Sicherheitssoftware oder englisch „rogue security software") gaukelt dem Anwender vor, vermeintliche andere Schadprogramme zu entfernen. Manche Versionen werden kostenpflichtig angeboten, andere Versionen installieren weitere Schadprogramme während des Täuschungsvorgangs.

Die große Bedeutung von Malware belegt eine Sicherheitsstudie der Zeitschrift <kes> und Microsoft von 2014. Laut dieser ist die „Infektion durch Schadsoftware" auf den ersten Platz der Gefährdungen für die Unternehmens-IT vorgerückt und hat somit „Irrtum und Nachlässigkeit der Mitarbeiter" auf den zweiten Platz verdrängt.[6]

Wie schon im vorigen Abschnitt angedeutet, erfolgt eine Infektion bzw. Verbreitung eines Viruses, indem es sich selbst in noch nicht infizierte Dateien

kopiert und diese so anpasst, dass das Schadprogramm mitausgeführt wird, wenn das Wirtsprogramm gestartet wird.

Im Gegensatz zu Viren warten **Würmer**[7] nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versuchen, aktiv in neue Systeme einzudringen. Dafür nutzen sie Sicherheitsprobleme auf dem Zielsystem aus.

"*Malwareimpfung*"

Die größte Hürde für einen besseren Schutz gegenüber solchen Schadprogrammen ist es, das Thema den Mitarbeitern bewusst zu machen (72%). Gefolgt von dem fehlenden Einsatzwillen im Top Management oder auch im mittleren Management (55% und 52%) sowie fehlendem Geld (52%) und fehlenden kompetenten Mitarbeitern (50%). Dies belegt die Tatsache, dass der Hauptinfektionsweg immer noch die E-Mail ist.[8] Doch wie können effektive Maßnahmen grundsätzlich aussehen?

Als erste Maßnahme empfiehlt es sich, dass die Arbeitsrechner und Server, auf denen wichtige Daten liegen, immer die aktuellste Software verwenden sollten. Dabei sollte nicht nur das Betriebssystem, sondern auch Internet-Programme dazugezählt vor allem Plug-Ins wie Java Flash und Adobe Reader. Auch der Router sollte regelmäßig auf die aktuellste Firmware kontrolliert werden.

Des Weiteren sollten alle Sicherheitsprogramme auf dem neuesten Stand sein. Unter Sicherheitsprogrammen werden unter anderem Antivirenprogramm gezählt. Diese sollten in der Lage sein, im laufenden Betrieb Bedrohungen im System zu erkennen. Die neuesten Standards solcher Programme erkennen das Verhalten eines Programmes und prüfen dessen Reputation im Internet. Zusätzlich sollte ein Webschutz immer enthalten sein. Somit wird verhindert, dass auf unsicheren Seiten gesurft wird.

Auch die Gefahr durch "eingeschleppte Viren" wird oft unterschätzt. USB Geräte von Mitarbeitern bergen Gefahren und sollten standardmäßig überprüft werden. Weiterhin sollte immer ein Webschutz aktiviert sein, wozu eine heu-

ristische Erkennung (verhaltensbasierte Detektion) und eine Intrusion Prävention (Einbruchsprävention) zählen. All diese Einstellungen sollten durch regelmäßige Überprüfungen im System sichergestellt werden.

Neben einer guten Antivirus-Software sollte eine unterstützende Firewall eingesetzt werden. Laienhaft ausgedrückt, stellt eine Firewall eine Art Filter dar. Dieser filtert Inhalte aus dem Internet oder Netzwerk, um den angeschlossenen Rechner zu schützen. Folgende Schutzfunktion sollte eine Firewall beinhalten:

- Kontrolle der Zugriffe aus Internet und Netzwerk
- Absicherung des Datenverkehrs bei ein- und ausgehenden Verbindungen
- Aktive Kontrolle von Anwendungen
- Schutz der Privatsphäre
- Alarmierung bei verdächtigen Aktivitäten

Eine Evolution bei Firewalls stellen sogenannte Next-Generation-Firewalls dar, diese können zusätzlich Daten und Informationen liefern, um eine bessere Unterscheidung zwischen sicheren oder unsicheren Inhalten zu treffen.

Secure-Mobile-Access

Die Verschmelzung zwischen privaten und Geschäftsdaten-setzt sich weiter fort, woraus sich die Frage ergibt, welche Bring-Your-Own-Device (BYOD)-Strategie zum jeweiligen Unternehmen passt. Eine gute Firewall unterstützt an dieser Stelle ebenso bei der Datenverkehrsüberwachung und erkennt sowie blockiert Eindringlinge inkl. bekannter Malware. Zusätzlich werden erkannte Viren in einer Bedrohungsdatenbank gespeichert, um Folgeangriffe zu verhindern.

Eine effektive Verwaltung von Identitäten und die Durchleuchtung sämtlicher Datenpakete ist elementar. Ein mehrstufiger Ansatz zur Abwehr von Ransomware mit 3 Scan-Engines hat sich dafür bewährt. Anbieter wie die SonicWall Next-Generation Firewalls adressieren dieses Thema und verhindern somit effizient Schäden durch Ransomware. Die Dateien werden dafür in parallelen Engines analysiert und solange blockiert, bis ihre Sicherheit überprüft wurde.

Dabei werden Korrektursignaturen sofort bereitgestellt. Die Vorteile liegen in einer hoch effektiven Sicherheit, schnellen Reaktionszeiten und geringeren Gesamtbetriebskosten.

7.4 Fazit

Die Bedrohungslage durch Ransomware steigt immer weiter. Die größten Risiken stellen dabei die eigenen Mitarbeiter dar, da diese es Angreifern häufig sehr leicht machen, in das System einzudringen. Weitere Gefahren entstehen durch die Verschmelzung von privaten und geschäftlichen Daten. Eine Absicherungsstrategie und moderne Tools sind daher notwendig, um diesen Bedrohungen zu begegnen. Verlässliche Sicherheitspartner und die Betrachtung des Gesamtsystems sind dafür Voraussetzung.

Moderne Firewall-Lösungen wie die von SonicWall sind unerlässlich, um auf der technischen Seite gewappnet zu sein.

Jedoch können auch hochqualifizierte Unternehmen wie die Netz-Werker AG oder SonicWall es alleine nicht schaffen, dass die Bedeutung von IT-Sicherheitsthemen bei den Mitarbeitern fest im Bewusstsein verankert wird. An dieser Stelle ist das Management der Unternehmen gefordert, gezielt auf die Mitarbeiter einzuwirken.

Lessons Learned

- Jedem muss die tagtägliche Bedrohung bewusst sein.
- Ohne Firewall ist es heutzutage unmöglich, seine Daten effektiv zu schützen.
- Der beste Schutz funktioniert nur, wenn er aktuell ist.
- Bewusstsein für IT-Sicherheit muss bei Mitarbeiter aktiv verankert werden.

[1] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zum Thema Spyware.

[2] Bachfeld, D. (2008). Zweifelhafte Antiviren-Produkte. Aufgerufen am 16.10.2017. Verfügbar unter: https://www.heise.de/security/artikel/Zweifelhafte-Antiviren-Produkte-270094.html.

[3] Ehrmann, E. (2016). Lexikon für das IT-Recht 2016/2017: Die 150 wichtigsten Praxisthemen. Heidelberg: Verlagsgruppe Hüthig Jehle Rehm.

[4] Ehrmann, E. (2016).

[5] Ehrmann, E. (2016).

[6] Scheidemann, V. (2014). IT-Landschaften 2014: Lagebericht zur Sicherheit. Sonderdruck aus <kes> – Die Zeitschrift für Informations-Sicherheit Nr. 2014#4, 2014#5 und 2014#6. Aufgerufen am 16.10.2017. Verfügbar unter: https://www.teletrust.de/fileadmin/_migrated/content_uploads/KES-Studie_IT-Sicherheit_2014.pdf.

[7] Pichler, T, (2008). Malware-Jubiläum: 20 Jahre Internet-Würmer. Aufgerufen am 16.10.2017, Verfügbar unter: https://www.pressetext.com/news/20081101001. i. V. m. o. A. (2008). US-Militär: Wegen Wurm-Attacke werden USB-Sticks verboten. Aufgerufen am 16.10.2017. Verfügbar unter: http://www.gulli.com/news/4174-us-militaer-wegen-wurm-attacke-werden-usb-sticks-verboten-2008-11-21. i.V.m. Scherschel, F. A. (2016). DDoS-Rekord-Botnetz Mirai ließe sich bekämpfen – allerdings illegal. Aufgerufen am 16.12.2017. Verfügbar unter: https://www.heise.de/security/meldung/DDoS-Rekord-Botnetz-Mirai-liesse-sich-bekaempfen-allerdings-illegal-3453658.html. i. V. m. Bleich, H. (2016). DDoS-Attacke legt Twitter, Netflix, Paypal, Spotify und andere Dienste lahm. Aufgerufen am 16.10.2017. Verfügbar unter: https://www.heise.de/newsticker/meldung/DDoS-Attacke-legt-Twitter-Netflix-Paypal-Spotify-und-andere-Dienste-lahm-3357289.html.

[8] Scheidemann, V. (2014).

Teil 3: Regelungen, Checklisten und Empfehlungen

8. Pragmatische IT-Sicherheit für Kleine und Mittlere Unternehmen (KMU)

Matthias Hartmann, Ralf Waubke; HTW Berlin

Abstract

Kleine und mittlere Unternehmen haben besondere Anforderungen an die Absicherung ihrer IT. Insbesondere der permanente Zeit- und Ressourcenmangel zwingt zu pragmatischen Lösungen bei der IT-Sicherheit. Um dennoch eine gute Absicherung der IT zu erreichen, empfehlen die Verfasser aus fünf Alternativen die Anwendung der Checkliste nach SANS mit 20 priorisierten Handlungsfeldern auszuwählen. Die Absicherung der Maschinen, Anlagen und Werkzeuge im Zeitalter des Internets der Dinge kann analog erfolgen.

8.1 Besonderheiten Kleiner und Mittlerer Unternehmen (KMU)

Große mittelständische Unternehmen oder Konzerne dominieren die Wahrnehmung in der Öffentlichkeit und der Presse. Das betrifft insbesondere auch auf Meldungen über Verletzungen der IT-Sicherheit zu. Kleine und mittlere Unternehmen (KMU) sind dagegen oftmals unterrepräsentiert, obwohl sie für das Wachstum, den Strukturwandel und die Beschäftigung der deutschen Volkswirtschaft eine wichtige Rolle spielen. Über 99% aller Unternehmen in Deutschland sind den KMU zuzuordnen, die zusammen 47,5% der deutschen Bruttowertschöpfung erzielen.[1]

Die IT kleiner Unternehmen und Handwerksbetriebe basiert oftmals auf wenigen PCs oder Laptops, Routern und Mobiltelefonen. Nicht zu unterschätzen sind jedoch Fragen, wo die Kunden- und Firmendaten gespeichert und gesichert werden, wer intern und extern Zugriff auf Anwendungen hat und wie

der Zugang zu eigenen Systemen über USB-Sticks oder WLAN erfolgt. Im Zeitalter der Digitalisierung stellt sich zudem die Frage, wie Maschinen, Anlagen, Werkzeuge o.ä. abgesichert werden können, die mittlerweile vernetzt sind (Internet der Dinge). Dies betrifft z.B. die (Fern-)Wartung von Systemen bei Kunden und den Einsatz von Drohnen oder Werkzeugen mit Sensoren und Funkverbindung.

8.2 Vorgaben für die IT-Sicherheit

Das theoretische Instrumentarium für IT-Sicherheit ist vielfältig. Besonders bekannt ist die Normenreihe ISO 27000 ff.[2] sowie der BSI-Grundschutz[3]. Speziell für KMU wurden die Prüfkriterien der VdS Schadenverhütung[4] entwickelt. Immer bekannter werden in Europa und Deutschland die Prüfkriterien nach NIST[5] und SANS[6].

8.2.1 Normenreihe ISO 27000ff.

Die Normenreihe ISO 27000 ff. behandelt die Informationssicherheit in Unternehmen und ist sehr umfassend angelegt. Die Norm ist nicht auf Informationstechnologie beschränkt, sondern berücksichtigt auch Anforderungen an die Organisation der Informationssicherheit, die Identifikation von wertvollen Informationen und den verantwortungsvollen Umgang mit Informationen durch die Mitarbeiter oder Zugangskontrollen.

Ein Handwerksbetrieb oder ein kleines Unternehmen wird sich eher selten mit der Normenreihe ISO 27000ff. befassen, denn zum einen ist das Werk sehr umfangreich und die Prioritäten sind nicht auf den ersten Blick erkennbar. Zum anderen ist das Werk auch nicht gerade günstig in der Anschaffung.

8.2.2 BSI-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet ebenfalls einen sehr umfassenden Überblick zur Informationssicherheit unter dem Begriff des IT-Grundschutzes an.[7] Für größere Unternehmen stellt sich die Frage, ob nach der ISO 27000ff. oder nach dem BSI-Grundschutz vorgegangen werden soll.

Aktuell (2017) wird eine neue Version des Katalogs erarbeitet (Konzeptstatus), in der es Bausteine für eine neue Schicht „Industrielle IT" geben wird.[8] Dies wird ein wesentlicher Fortschritt sein, denn ebenso wie die ISO 27000ff. geht der BSI-Grundschutz bislang zu wenig auf Sicherheitsthemen in der Betriebsinformatik[9] ein wie Supervisory Control and Data Acquisition Systemen (SCADA), Manufacturing Execution Systems (MES), Industrial Ethernet oder Programmable Logic Controller (PLC).[10] Ebenso wie bei der ISO 27000ff. fehlt eine vorgegebene Priorisierung der Handlungsempfehlungen.

An der Hochschule für Technik und Wirtschaft (HTW) Berlin wird der BSI-Grundschutz verwendet. Entsprechend hat der Fachbereich Wirtschafts- und Rechtswissenschaften den Fragenkatalog beantwortet. Der Fachbereich hat 64 ProfessorInnen, 15 Verwaltungsangestellte und ca. 3.500 Studierende mit einer entsprechenden IT-Infrastruktur. Die Beantwortung des umfangreichen Fragenkatalogs war sehr zeitintensiv und wurde durch einen eigens damit beauftragten Laboringenieur vorgenommen. Positiv kann vermerkt werden, dass der IT-Grundschutz sehr umfassend angelegt ist. Kritisch anzumerken ist der Zeitaufwand, die notwendige IT-Expertise und die Komplexität des Ansatzes. Für die Anwendung ist ebenfalls das Fehlen einer ex-ante-Priorisierung (wie bei SANS, siehe unten) und die Schwierigkeit der Erstellung einer Management-Zusammenfassung problematisch. Für den Verfasser in seiner Rolle als Dekan des Fachbereichs war es nur sehr schwer möglich, ein klares und einfaches Handlungsprogramm ableiten zu können. Mithin ist der IT-Grundschutz in eine Reihe mit der ISO 27000ff. zu stellen.

8.2.3 VdS Quick-Check

Die VdS Schadenverhütung GmbH ist ein Unternehmen des Gesamtverbandes der deutschen Versicherungswirtschaft (GDV)[11]. Die VdS hat für die Cyber-Security von KMU einen 39 Fragen umfassenden webbasierten Quick-Check entwickelt. Dieser umfasst die vier Hauptbereiche: Organisation, Technik, Prävention und Management. Zur Organisation beinhaltet der Quick-Check Fragestellungen zu Verantwortlichkeiten, Richtlinien, Zugängen und zum Personal. Der Bereich Technik beinhaltet Themen zu IT-Systemen, Netzwerken, mobilen Geräten und mobilen Datenträgern sowie der Bereich Prävention die Kategorien: Umgebung, Datensicherung, Ausfälle und Sicherheitsvorfälle. Der

letztgenannte Bereich Management umfasst das IT-Outsourcing und Cloud-Computing. Nachdem der Quick-Check durchgeführt wurde, erhalten Teilnehmer eine direkte Auswertung in Form einer Matrix. In dieser wird in Bezug zu den Kategorien ein Erfüllungsgrad in% angegeben, der durch eine Ampellogik unterstützt wird (Grün über 90%, Gelb zwischen 60% und 90% sowie Rot unter 60%).[12] Der Quick-Check enthält jedoch keine Fragestellungen zur produktionsnahen IT. Aus diesem Grund offeriert die VdS GmbH die Möglichkeit einen ICS (Industrial Control Systems) -Quick-Check durchzuführen, der 48 Fragen enthält. Am Ende wird wiederum eine Matrix mit den Ergebnissen ausgegeben[13]. Positiv zu vermerken ist die Handlungsorientierung des Ansatzes.

8.2.4 NIST Rahmenkonzept für Cyber Security

Das US-amerikanische National Institute of Standards and Technology (NIST) entwickelte ein Rahmenkonzept für eine systematische Verbesserung der Cyber-Security. Das Konzept mit dem Namen „Framework for Improving Critical Infrastructure Cybersecurity" wurde 2014 veröffentlicht (Version 1.0).[14] Eine neuere Variante (Version 1.1) ist zurzeit in der Konzeptionsphase und wurde zur Diskussion im Januar 2017 veröffentlicht[15]. Bei beiden Versionen liegt der Schwerpunkt auf der kritischen Infrastruktur (KRITIS) von Organisationen. Das Rahmenkonzept leitet von den fünf Funktionen „Identifizieren (Identify)", „Schützen (Protect)", „Erkennen (Detect)", „Antworten (Respond)" und „Wiederherstellen (Recover)" Kategorien ab, von denen wiederum Unterkategorien gebildet werden. Von diesen können Maßnahmen und Aktivitäten zur Verbesserung der Cyber-Security abgeleitet werden.[16]

8.2.5 Prüfkriterien nach SANS

Besondere Erwähnung sollen an dieser Stelle die 20 Prüfkriterien (Critical Security Controls for Effective Cyber Defense) des Center for Internet Security (CIS) bekommen, die in der Praxis teilweise auch unter dem Begriff SANS bekannt sind.[17] Die sogenannten 20 Critical Security Controls (aktuell in der Version 6.1)[18] sind theoriegeleitet und gleichzeitig praxisorientiert und damit im positiven Sinne ein sehr pragmatischer Ansatz für Unternehmen, insbesondere auch für Kleine und Mittlere Unternehmen. Die Logik ist gerade auch für Nicht-Experten nachvollziehbar. Die Pragmatik liegt in der Priorisierung

der IT-Security-Themen und der sofortigen Anwendbarkeit. Die Darstellung der Critical Security Controls zeigt, dass mit erster Priorität eine Inventarisierung aller Geräte stattfinden soll. Denn es hilft z.B. nicht, Maßnahmen des Datenschutzes zu propagieren, wenn nicht einmal klar ist, auf welchen Geräten Daten gespeichert sind bzw. aufgerufen werden können. Mit zweiter Priorität sollen alle Software-Programme inventarisiert werden. Sogenannte Penetration Tests und Red Team Excercises (Nr. 20) sollten erst nach Abarbeiten aller anderen Maßnahmen durchgeführt werden. Denn ohne die Absicherung der ersten 19 Critical Security Controls wird ein Red Team beliebig viele Sicherheitslücken finden.

Die folgende Auflistung zeigt die 20 Critical Security Controls:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and appropriate training to fill the gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Excercises

Ebenso wie bei der ISO 27000ff., der bisherigen Version des BSI-Grundschutzes und dem Rahmenkonzept von NIST werden auch bei den SANS-Controls keine Empfehlungen für die Absicherung der Betriebsinformatik gegeben. Die analoge Anwendung der SANS-Controls ist jedoch einfach. So müssen z.B. nur die Critical Controls Nr. 1 und Nr. 2 auch auf Maschinen, Anlagen, Werkzeuge u.a. angewendet werden. Personenbezogene und organisatorische Sicherheitsfragen stehen bei SANS allerdings im Hintergrund.

8.3 Sicherheitsbedarf im Internet der Dinge

Im Internet der Dinge erhalten immer mehr physische Gegenstände Sensoren und Funktechnologien. Diese Dinge werden zunehmend über das Internet miteinander vernetzt und bilden somit das Internet der Dinge (englisch: Internet of Things, kurz IoT), d.h. auch ein Bohrer, Hammer oder Vermessungswerkzeuge werden zukünftig Informationen erfassen und senden. Der Hammer wird mithin „cyberized". Überspitzt formuliert: IT betrifft nicht mehr nur die IT. Wirtschaftsinformatik und Betriebsinformatik wachsen zusammen. Und damit wird IT-Sicherheit zu Cyber-Sicherheit. Dies hat auch Auswirkungen auf die in der folgenden Abbildung dargestellte Automatisierungspyramide. Diese hierarchisch gestaltete Pyramide besteht aus sechs Ebenen, von denen die beiden oberen Ebenen (ERP und MES) der Büro IT (Office IT) zugeordnet werden (Betriebswirtschaft) und die unteren vier Ebenen der produktionsnahen IT (Technik). Aus traditioneller Perspektive gibt es zwischen diesen Ebenen relativ wenig Schnittstellen, weshalb die Steuerung und Betrachtungsweise häufig noch isoliert erfolgt[19]. Die vertikale und horizontale Vernetzung steigt jedoch zunehmend, weshalb eine isolierte Betrachtung gefährlich sein kann – insbesondere bei Fragen der IT-Security-. Zur Verdeutlichung dieses Phänomens werden zunächst typische Angriffe auf die Büro-IT und dann typische Angriffe auf die Betriebstechnik und Alltagsgegenstände aufgezeigt.

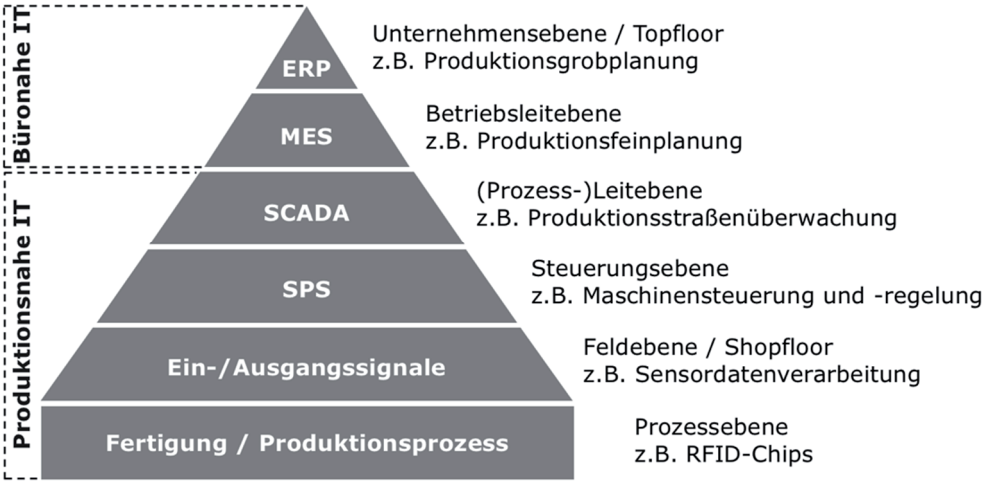

Abbildung 15: Trennung von büronaher IT und produktionsnaher IT anhand der Automatisierungspyramide, Abbildung angelehnt an Siepmann.[20]

8.3.1 Angriffe auf die büronahe IT

Equifax ist ein bedeutender US-amerikanischer Finanzdienstleister, der vor allem Bonitätsauskünfte erteilt. Durch eine Sicherheitslücke in der Webanwendung Apache Struts konnten Hacker in das Netzwerk eindringen und zwischen Mai und dem 29. Juli 2017 auf Datenbanken zugreifen. Die Sicherheitslücke war bereits seit Anfang März 2017 bekannt und konnte seitdem durch einen Patch geschlossen werden, was Equifax verpasste[21]. In Summe konnten Daten von 143 Mio. US-Bürgern erlangt werden. Diese Daten beinhalten u.a. Sozialversicherungs-, Führerschein- und Kreditkartennummern.[22]

Wannacry ist ein sogenannter Kryptotrojaner, der Festplatten verschlüsselt, um nachfolgend Lösegeld (Ransomware) zu fordern. Die Schadsoftware wurde via E-Mails verteilt und über einen in der Mail integrierten Link aktiv. Die sich ab dem 12. Mai 2017 ausbreitende Schadsoftware nutzte eine Sicherheitslücke in älteren Windowsversionen aus, die jedoch seit März 2017 gepatcht werden konnten, was vielfach versäumt wurde. In Summe wurden 230.000 Computer in 150 Ländern infiziert. Dabei wurde auch die Deutsche Bahn getroffen. So fielen z.B. Anzeigetafeln und Kameras aus.[23]

Petya ist wie Wannacry ein Verschlüsselungstrojaner, der Lösegeld fordert. Auch hier erfolgte der Angriff über einen Link in einer E-Mail, um darauf aufbauend eine Windowssicherheitslücke zu nutzen. Die im Juni 2017 aufgetauchte Variante nutzte darüber hinaus ein gängiges Administrationswerkzeug aus, um andere Geräte im Netzwerk zu infizieren. Somit war auch die Infektion von Windows 10 Geräten möglich. Einige Experten bezeichnen den Trojaner deswegen auch als NotPetya. Betroffen waren unter anderem die Unternehmen Beiersdorf, Rosneft, Merck Sharp & Drohne sowie Maersk. Dabei wird der angerichtete Schaden alleine bei Maersk auf 200-300 Mio. € taxiert.[24]

8.3.2 Angriffe auf die produktionsnahe IT

Stuxnet ist ein Wurm zur Maschinensteuerung und hatte das Ziel, die iranischen Zentrifugen zu zerstören. Es wird zwischen zwei Stuxnet-Varianten unterschieden. Die erste Version versuchte über die Drucksteuerung in den Zentrifugen diese zu zerstören, wohingegen die zweite Variante die Rotationsgeschwindigkeit manipulierte. Die zweite Variante wurde 2009 eingesetzt und über USB-Schnittstellen eingeschleust. Zur Manipulation der Rotationsgeschwindigkeit hat Stuxnet die Siemenssteuerung S-7-315 unter Kontrolle gebracht.[25]

Bei einem deutschen Stahlhersteller wurde ein **Hochofen** manipuliert. Das BSI berichtete 2014, dass über Spear-Phishing Mails in das Büronetzwerk eingedrungen wurde und die Hacker sich dann sukzessive in das Produktionsnetzwerk vorgearbeitet haben. Dort hatten sie Zugriff auf die Steuerung eines Hochofens und haben ein Runterfahren des Hochofens verhindert, was zu erheblichen Schäden in der Anlage geführt hat.[26]

Black-Energy ist ein Schadprogramm, das zur Manipulation eines ukrainischen Umspannwerkes führte. Auch hier sorgten Anhänge in E-Mails für die Installation der Schadsoftware. In der Folge zog sich das Programm weitere Schadkomponenten aus dem Internet. Dadurch war es möglich, Dateien zu löschen, die für Rechenprozesse der industriellen Anlagen genutzt werden. Dies führte zu einem Blackout in der Westukraine, von dem 700.000 Haushalte betroffen waren.[27]

8.3.3 Angriffe auf unser tägliches Leben

Die Puppe **My Friend Cayla** ist ein sogenanntes Smart Toy, das sich mit dem Internet verbinden lässt. Der britische Spielzeughersteller Genesis stattete Cayla mit einem Lautsprecher und einem Mikrofon aus. Sofern die Puppe mit dem Internet verbunden ist, kann sie Fragen beantworten, wodurch die Puppe zum Gesprächspartner von Kindern wird. Cayla wird via Bluetooth mit einem Smartphone oder Tablet PC verbunden, dabei bedarf es bei der Verbindung keines Passwortes, wodurch sich jeder im Umkreis direkt mit Cayla verbinden kann. Einmal mit Cayla verbunden, kann das Mikrofon und der Lautsprecher benutzt werden. Damit kann alles Gesagte im Raum mitgehört oder sogar mit Kindern gesprochen werden.[28]

8.4 Pragmatische IT-Sicherheit für KMU und Handwerksbetriebe

Kleine Unternehmen und insbesondere Handwerksbetriebe haben oft nicht die zeitlichen und finanziellen Mittel, um eine Zertifizierung nach ISO oder dem BSI-Grundschutz durchzuführen. Daher stellt sich die Frage, wie IT-Sicherheit in kleinen Unternehmen und Handwerksbetrieben beachtet werden sollte. Mittlere Unternehmen müssen sich pragmatisch definieren, welche Anforderungen erfüllt werden müssen und welche Vorgehensweise sinnvoll ist.

Unseres Erachtens sind die 20 Prüfkriterien nach SANS gut verständlich und einfach in der Anwendung. Man muss nicht IT-Spezialist sein, um die Inhalte und die Prioritäten zu verstehen. Unsere Meinung basiert auf den Erkenntnissen eines Projektes, dass an der HTW Berlin für Berliner KMU durchgeführt wird. Thema des Projektes ist die Digitalisierung von Prozessen in den Unternehmen. Das Projekt wird durch den Europäischen Fonds für regionale Entwicklung (EFRE) gefördert und hat eine Laufzeit vom 01.07.2016 bis zum 30.06.2019.[29] Aktuell (September 2017) haben 60 Unternehmen aus Berlin um Unterstützung im Rahmen des Projektes angefragt und erhalten.

Lessons Learned

- IT-Sicherheit betrifft nicht nur klassische IT-Geräte, sondern alle Geräte, die mit dem Internet (der Dinge) verbunden sind.
- Mithilfe der 20 Prüfkriterien nach SANS kann der IT-Sicherheitsstatus eines kleinen oder mittleren Unternehmens sehr gut eingeschätzt werden.
- Die 20 Kriterien nach SANS sind zugleich Handlungsempfehlung.
- Cyber-Angriffe suchen sich ihre Wege über Bürorechner, Maschinen und Werkzeuge sowie über mit dem Internet verbundenen Alltagsgegenständen.
- Die HTW Berlin bietet Unterstützung im Bereich IT-Security an.

---

[1] Söllner, R. (2014). Die wirtschaftliche Bedeutung kleiner und mittlerer Unternehmen in Deutschland. In Wirtschaft und Statistik (S. 40-51), Hrsg. Statistisches Bundesamt, Wiesbaden.

[2] International Organization for Standardization (o. J.). Aufgerufen am 12.08.2017. Verfügbar unter: https://www.iso.org/isoiec-27001-information-security.html.

[3] Bundesamt für Sicherheit in der Informationssicherheit (o. J.). Aufgerufen am 17.08.2017. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

[4] VdS Schadenverhütung GmbH (o. J.). VdS Quick-Check. Aufgerufen am 14.08.2017. Verfügbar unter: https://vds.de/de/cyber/quick-check/.

[5] National Institute of Standards and Technology (o. J.). Aufgerufen am 20.08.2017. Verfügbar unter: https://www.nist.gov/cyberframework/.

[6] Center for Internet Security (2017). CIS Controls. Aufgerufen am 06.08.2017. Verfügbar unter: https://www.cisecurity.org/controls/.

[7] Bundesamt für Sicherheit in der Informationssicherheit (2016). IT-Grundschutz Basis für Informationssicherheit. Aufgerufen am 12.08.2017. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Allgemeines/Einstiegskapitel/einstiegskapitel_node.html.

[8] Bundesamt für Sicherheit in der Informationssicherheit (2017). Die Modernisierung des IT-Grundschutzes. Aufgerufen am 12.08.2017. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/itgrundschutz_modernisierung_node.html.

[9] Die Betriebsinformatik, auch Shop-Floor-IT genannt, (z.B. IT für die Produktionssteuerung etc.) ist von der Büro IT, auch Office IT genannt, (z.B. kfm. Bereich) abzugrenzen und ist produktionsnahe verortet.

[10] Lass, S. & Fuhr, D. (2014). IT-Sicherheit in der Fabrik. In Productivity Management 19 (S. 13-16), Hrsg. Gronau, N. & Scholz-Reiter. Berlin: Gito.

[11] VdS Schadenverhütung GmbH (o. J.). VdS Quick-Check. Aufgerufen am 14.08.2017. Verfügbar unter://vds.de/de/unternehmen/.

[12] VdS Schadenverhütung GmbH (o. J.). VdS Quick-Check. Aufgerufen am 14.08.2017. Verfügbar unter: https://vds.de/de/cyber/quick-check/.

[13] VdS Schadenverhütung GmbH (o. J.) VdS Quick-Check für ICS. Aufgerufen am 17.12.2017. Verfügbar unter: https://www.vds-quick-check.de/der-vds-quick-check-fuer-ics-im-detail/.

[14] National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. Verfügbar unter: https://www.nist.gov/cyber-framework/draft-version-11.

[15] National Institute of Standards and Technology (2017). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Verfügbar unter: https://www.nist.gov/cyber-framework/draft-version-11.

[16] National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. Verfügbar unter: https://www.nist.gov/cyber-framework/.

[17] Vgl. Hartmann, M. und Halecker, B. (2017). Pragmatische Cyber Security in Kriti-schen Infrastrukturen – zwei Fallbeispiele. In: Safety und Security - Mit Sicherheit gut vernetzt - Branchentreff der Berliner und Brandenburger Wissenschaft und Industrie. Hrsg. Pinnow, C. und Schäfer, S., Beuth Verlag Berlin, Wien, Zürich.

[18] Center for Internet Security (2017). CIS Controls. Aufgerufen am 06.08.2017. Verfügbar unter: https://www.cisecurity.org/controls/.

[19] Vogel-Heuser, B. (2017): Herausforderungen und Anforderungen aus Sicht der IT und der Automatisierungstechnik. In Bauernhansl, T.; Hompel, M. und Vogel-Heuser, B. (Hrsg.), Industrie 4.0 in Produktion, Automatisierung und Logistik (S. 37-48). Wiesbaden: Springer.

[20] Siepmann, D. (2016). Industrie 4.0 - Technologische Komponenten. In Roth, A. (Hrsg.), Einführung und Umsetzung von Industrie 4.0 (S. 47-72). Berlin Heidelberg: Springer Gabler Verlag.

[21] Sokolov, D. (2017). Equifax soll früheren Hack verheimlicht haben. Aufgerufen am 19.09.2017. Verfügbar unter: https://www.heise.de/newsticker/meldung/Equifax-soll-frueheren-Hack-verheimlicht-haben-3835052.html.

[22] Equifax (2017). Aufgerufen am 10.09.2017. Verfügbar unter: https://www.equifaxsecurity2017.com.

[23] Staun, H. (2017). Das Rätsel der Shadow Brokers. Aufgerufen am 07.08.2017. Verfügbar unter: http://www.faz.net/-gsb-8y1w3.

[24] O. A. (2017). „Virus fräst sich durch große Netzwerke und nimmt alles mit". Aufgerufen am 03.08.2017. Verfügbar unter: http://www.faz.net/-gqm-8z8o8.

[25] Langner, R. (2013). To Kill a Centrifuge. Verfügbar unter: https://www.langner.com/resources/.

[26] Scherschel, F. A. (2014) BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk. Aufgerufen am 27.08.2017. Verfügbar unter: https://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html.

[27] Heller, P. (2016). Die Hackerdämmerung. Aufgerufen am 16.08.2017. Verfügbar unter: http://www.faz.net/-gx7-8c6ow.

[28] Kühl, E. (2017) Vernichten Sie diese Puppe. Aufgerufen am 05.09.2017. Verfügbar unter: http://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur.

[29] Details zum Projekt finden sich in diesem Buch im Beitrag „EFRE Projekt Digital Value für Berliner Unternehmen".

9. Sichere Verwaltung digitaler Daten

Gerd M. Fuchs, Rechtsanwaltskanzlei FOXLAW®

Abstract

Die gesetzlichen Anforderungen an die Verarbeitung personenbezogener Daten sind hoch – die ab Mai 2018 geltende EU-Datenschutzgrundverordnung wird diese noch erweitern. Dieser Artikel stellt dar, worauf Unternehmen bereits bei der Erhebung personenbezogener Daten achten müssen, welche Pflichten zur Sicherung dieser Daten im Unternehmen bestehen und welche Sanktionen bei Datenschutzverstößen drohen.

9.1 Einleitung

Die Bedeutung von Daten, ihre Erhebung, Speicherung und Nutzung – kurz „Verarbeitung" – für Unternehmen nimmt stetig zu. Nicht nur in Zeiten von „Big Data"[1] spielen Daten für eine gezielte und erfolgreiche Wertschöpfung eine ganz erhebliche Rolle. Und damit auch der Datenschutz, der stets dann auf den Plan tritt, wenn personenbezogene Daten[2] verarbeitet werden: Mitarbeiterdaten, Kundendaten, Unternehmensdaten, Nutzungsdaten sowie auch sensible Daten wie etwa Bankdaten.

Dieser Beitrag soll einen Überblick über die wesentlichen Pflichten des Unternehmens bei der Verarbeitung personenbezogener Daten vermitteln und Unternehmen dadurch in die Lage versetzen, rechtskonform und wirtschaftlich erfolgreich mit personenbezogenen Daten umzugehen.

9.2 Die rechtskonforme Erhebung und Verarbeitung von personenbezogenen Daten

Erste ganz wesentliche Voraussetzung für die Zulässigkeit der Verarbeitung personenbezogener Daten ist eine rechtskonforme Erhebung dieser Daten. Gesetzlich gilt ein striktes Verbot der Verarbeitung personenbezogener Daten.[3] Dieses wird nur durch eine im Gesetz definierte Erlaubnis, eine „Ermäch-

tigungsgrundlage“[4] oder aber durch eine ausdrückliche Einwilligung[5] des Betroffenen, also desjenigen, zu dessen Person diese Daten gehören, aufgehoben.

9.2.1 Gesetzliche Ermächtigungsgrundlagen

Die Regelungen zum Datenschutz sind in einer Vielzahl an Gesetzen geregelt. Hier handelt es sich um eine spezielle Rechtsmaterie, die ständig durch nationale und/oder europäische Regulierung verändert bzw. harmonisiert wird.

Neben der zum 18.05.2018 in Kraft tretenden EU-Datenschutzgrundverordnung (DS-GVO) sind vor allem das Bundesdatenschutzgesetz (BDSG), landesrechtliche Datenschutzgesetzte wie etwa das Berliner Datenschutzgesetz (BlnDSG) sowie weitere Spezial- bzw. Bereichsgesetze für Bund und Länder wie etwa das Telemediengesetz (TMG) oder das Telekommunikationsgesetz (TKG) zu nennen.

Diese sehen Regelungen für die Erhebung und Verarbeitung personenbezogener Daten vor. Bekannte Beispiele wären etwa die Strafprozessordnung (StPO) für die Erhebung von Daten im Zuge von staatsanwaltschaftlichen Ermittlungen oder aber das Einwohnermeldegesetz.

Meist aber betreffen diese Regelungen die Erhebung personenbezogener Daten durch staatliche Stellen. Für Unternehmen sind so gut wie keine gesetzlichen Ermächtigungsgrundlagen für die Erhebung dieser Daten vorhanden, jedenfalls nicht im Zusammenhang mit wirtschaftlicher Tätigkeit.

9.2.2 Einwilligung des Betroffenen

Den Regelfall für die rechtlich zulässige Erhebung von personenbezogenen Daten durch Unternehmen stellt daher die Einwilligung des Betroffenen dar.[6] An die Wirksamkeit dieser Einwilligung stellt das Gesetz sehr hohe Anforderungen, vgl. § 4a, § 28 Abs. 3b BDSG. So muss das Unternehmen sicherstellen, dass die Einwilligung des Betroffenen rechtskonform und wirksam eingeholt wird. So sieht § 4a BDSG u.a. vor, dass die Einwilligung nur wirksam ist, wenn sie auf der freien Entscheidung des Betroffenen beruht. Der Betroffene ist zudem auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf

Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Für auf elektronischem Wege eingeholte Einwilligungen, etwa die online erteilte Einwilligung zum Erhalt von Email-Werbung, ist das zum BDSG speziellere Telemediengesetz (TMG) zu beachten. Hier sieht § 13 Abs. 2 TMG vor, dass die Einwilligung elektronisch erklärt werden kann, wenn der Dienstanbieter sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Zudem sieht das TMG eine Vielzahl an Hinweisen zum Umgang des Unternehmens mit personenbezogenen Daten des Nutzers vor.[7] Diese werden üblicherweise in Datenschutzhinweisen oder Datenschutzbestimmungen aufgeführt, die auf der Internetseite des Unternehmens leicht auffindbar und jederzeit abrufbar sind.

Erschwerend kommt hinzu, dass etwa das Gebot der Datenvermeidung bzw. Datensparsamkeit nach § 3a BDSG zu beachten ist: Daten sind zu pseudonymisieren oder zu anonymisieren, soweit es möglich und verhältnismäßig ist.

Beachtet das Unternehmen all diese strengen und vielerorts gesetzlich verankerten Vorgaben und erhebt damit rechtskonform die Einwilligung des Nutzers, so ist damit die Grundvoraussetzung für die Verarbeitung von personenbezogenen Daten des Nutzers geschaffen.

Wichtig ist dann vor allem, dass diese Einwilligung – ganz gleich ob online oder offline erhoben - dauerhaft gespeichert bzw. dokumentiert ist. Denn im Streitfall muss das Unternehmen nachweisen, dass eine wirksame Einwilligung in die Datenverarbeitung vorliegt.

Hat das Unternehmen Daten beim Betroffenen rechtskonform erhoben, gilt es aber gleichwohl, dass diese Daten nur in rechtlich zulässiger Weise verarbeitet und genutzt werden dürfen. Sie sind gegen Verlust und Diebstahl zu sichern. Entfällt der Zweck, zu dem die Daten ursprünglich erhoben wurden, so sind diese zu Löschen. Und nicht zu vergessen: der Betroffene hat stets das Recht,

vom verarbeitenden Unternehmen zu erfahren, welche persönlichen Daten von ihm gespeichert und zu welchem Zweck sie genutzt werden.[8]

9.3 Sichere Verarbeitung personenbezogener Daten

Mit der Einwilligung des Betroffenen zur Verarbeitung personenbezogener Daten ist das Unternehmen berechtigt, diese dem Zweck entsprechend zu nutzen. Damit einher geht die Pflicht, diese Daten, die Informationen über eine Person sowie auch weitere Informationen, die sich mit ihr in Verbindung bringen lassen – etwa eine IP-Adresse - zu schützen.

Die Schutzanforderungen ergeben sich ebenfalls aus den gesetzlichen Regelungen – unter Beachtung der Qualität der betroffenen Daten. So wurden im Zuge der Datenschutz-Grundverordnung auch die Bestimmungen zur Datensicherheit und damit zu den technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten überarbeitet. Gleiches gilt für die Novelle des BDSG, die zeitgleich mit der DS-GVO in Kraft treten.

Die neue DS-GVO definiert eine Reihe an Vorgaben für die „Sicherheit der Verarbeitung"[9]. Und Art. 5 Abs. 2 DSGVO schreibt vor, dass das Unternehmen die Einhaltung der Datensicherheit gewährleisten und auf Anforderung auch nachweisen muss.

9.3.1 Technische und organisatorische Maßnahmen

Die DS-GVO – wie auch zuvor und weiterhin das BDSG – definiert eine Reihe an technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.

Das deutsche Datenschutzrecht sah bislang in § 9 BDSG nebst Anlage einen Katalog von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten vor. § 9 BDSG inklusive Anlage wird nun durch die ranghöhere DS-GVO, hier Art. 32, ersetzt. Darin geregt sind: abstrakte[10] Maßnahmen zur Umsetzung technischer und organisatorischer Maßnahmen und damit der Datensicherheit, anders als noch zuvor in § 9 BDSG.

Abzustellen ist nach dieser Vorschrift hinsichtlich der erforderlichen Maßnahmen u.a. auf den Stand der Technik, die Implementierungskosten und die Art

des Umfangs sowie die Umstände und den Zweck der Datenverarbeitung. Diese Maßnahmen sollen zudem das drohende Risiko der Beeinträchtigung von Persönlichkeits- und Freiheitsrechten – so etwa Datenverlust oder „Datenklau" – und dessen Eintrittswahrscheinlichkeit berücksichtigen.

Das Unternehmen muss also Maßnahmen zum ausreichenden Schutz der Daten ergreifen, die aktuell zur Verfügung stehen und die sich bereits in der Praxis bewährt haben. Das impliziert regelmäßige Überprüfungen und Anpassungen dieser Maßnahmen.

Zudem legt Art. 32 Abs. 1 c) DS-GVO fest, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können müssen.

So muss das Unternehmen zunächst eine sog. „Schutzbedarfsfeststellung" hinsichtlich der unterschiedlichen personenbezogenen Daten durchführen. Bei dieser sind zunächst die möglichen Bedrohungen und ihre Eintrittswahrscheinlichkeit als auch der potenzielle Schaden für die Rechte und Freiheiten natürlicher Personen[11] zu identifizieren, um daraus die entsprechenden Maßnahmen ableiten und etablieren zu können.

9.3.2 Einzelne Maßnahmen

Dem Wortlaut des Art. 32 Abs. 1 a) DS-GVO lässt sich etwa die Pseudonymisierung sowie die Verschlüsselung von Daten als mögliche Maßnahme entnehmen. Anonymisierung wird hingegen nicht erwähnt. Weiter geht hingegen § 58 Abs. 3 des Referentenentwurfs für das deutsche Ausführungsgesetz zur Datenschutz-Grundverordnung. Darin werden als mögliche Maßnahmen etwa Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, Übertragungskontrolle, Eingabekontrolle, Transportkontrolle, Wiederherstellung, Datenintegrität, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle sowie ein Verschlüsselungsverfahren genannt.

Welche Maßnahme das Unternehmen für die jeweiligen Daten bzw. Datenkategorien ergreift, bleibt ihm überlassen, jedenfalls solange, wie die vier in Art. 32 Abs. 1 b) der DS-GVO genannten Schutzziele erreicht sind. Diese sind Vertraulichkeit (die Daten sind für unberechtigte Dritte nicht zugänglich), Integrität (die Daten können nicht verfälscht werden), Verfügbarkeit (die Daten

stehen bei Bedarf zur Verfügung) sowie die Belastbarkeit der Systeme und Dienste (Systeme halten einer gewissen Beanspruchung stand). In der Praxis erfordert dies nicht nur ein wirksames Notfallmanagement, sondern auch eine regelmäßige Überprüfung der Maßnahmen auf Wirksamkeit und angemessene (aktuelle) Sicherheit der Daten. Art. 32 Abs. 1 d) DS-GVO schreibt hierzu sogar regelmäßige Test der Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen vor.

Erweitert werden diese gesetzlichen Vorgaben durch Art. 25 DS-GVO. Danach sollen Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden. Dies meint u.a. die Etablierung von Möglichkeiten wie Deaktivierung von Funktionalitäten, Anonymisierung oder Pseudonymisierung von Daten, gleichwohl aber auch Authentisierungs- und Authentifizierungprozesse sowie die Verschlüsselung von Daten.

Damit nicht genug: In Anlehnung an das Gebot der Datenvermeidung und Datensparsamkeit nach § 3a BDSG sollen IT-Systeme datenschutzfreundlich voreingestellt sein[12] - es sollen nur diejenigen personenbezogenen Daten verarbeitet werden, die für den beabsichtigten Zweck unbedingt erforderlich sind.

9.3.3 Bestellung eines Datenschutzbeauftragten

Empfehlenswert – und je nach Umfang der Verarbeitung personenbezogener Daten im Unternehmen auch gesetzliche Vorschrift – ist die Bestellung eines betrieblichen oder externen Datenschutzbeauftragten. Wie bereits in § 4f. BDSG definiert, sieht auch die DS-GVO die Bestellung eines Datenschutzbeauftragten vor, vgl. Art. 37 DS-GVO. Dieser wird mit der Planung, Umsetzung und Wirksamkeitskontrolle der getroffenen Maßnahmen betraut. Er ist gemäß Art. 38 Abs. 1 DSGVO ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden.

9.3.4 Sanktionen

Kommt das Unternehmen seinen Pflichten hinsichtlich einer ausreichenden Datensicherheit nicht nach, so droht – anders als bei Verstößen gegen § 9 BDSG, die nicht sanktioniert waren – ein Bußgeld in Höhe von bis zu 10 Millionen Euro oder bis 2% des weltweit erzielten Jahresumsatzes. Nicht zuletzt

diese erheblichen Bußgelder sollten jedes Unternehmen dazu bewegen, Datenschutz und Datensicherheit ernst zu nehmen.

9.4 Fazit

Die Sicherheit von personenbezogenen Daten ist eine Angelegenheit, die für jedes Unternehmen eine sehr hohe Priorität haben sollte – nicht nur wegen dem sonst drohenden erheblichen Bußgeld. Daher sollte – aus Sicht der Experten[13] – jedes Unternehmen, das personenbezogene Daten verarbeitet, a) ein Management für Daten- bzw. Informationssicherheit etablieren, b) den Schutzbedarf dieser Daten feststellen, c) die Risiken bewerten, d) entsprechende Maßnahmen zu deren Schutz planen, etablieren und regelmäßig testen und e) sämtliche Schritte dokumentieren bzw. verschriftlichen.

Lessons Learned

- Bereits bei der Erhebung von personenbezogenen Daten ist strikt darauf zu achten, dass die Einwilligung des Betroffenen wirksam und unter Beachtung der erforderlichen Hinweis- und Protokollierungspflichten eingeholt wird. Geschieht dies nicht, sind sämtliche darauf aufbauende Datenverarbeitungsprozesse unzulässig
- Erhobene Daten sind zweckgebunden zu verarbeiten und gegen unberechtigten Zugriff Dritter sowie weitere Risiken zu sichern. Dazu bedarf es geeigneter, wirksamer und dem Stand der Technik entsprechender Maßnahmen. Diese sind regelmäßig auf ihre Wirksamkeit zu Überprüfen.
- Ggf. ist ein Datenschutzbeauftragter zu bestellen, der in die Planung und Umsetzung der Datenschutz- und Datensicherheitsprozesse involviert ist und entsprechende Maßnahmen etablieren und überwachen kann

[1] „Big Data" wird häufig als Sammelbegriff für digitale Technologien verwendet, die in technischer Hinsicht für eine neue Ära digitaler Kommunikation und Verarbeitung und in sozialer Hinsicht für einen gesellschaftlichen Umbruch verantwortlich gemacht werden, vgl. R. Reichert: Big Data: Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie, S. 9. Mit ihm wird oft auch der Komplex der Technologien beschrieben, die zum Sammeln und Auswerten dieser Datenmengen verwendet werden, vgl. Edd Dumbill: What is big data? An introduction to the big data landscape, 11. Januar 2012.

[2] Personenbezogene Daten: Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), Vgl. § 3 Abs. 1 BDSG (Bundesdatenschutzgesetz).

[3] Vgl. § 4 Abs. 1 BDSG.

[4] Vgl. § 4 Abs. 1 und 2 BDSG.

[5] Vgl. § 4a BDSG.

[6] So geregelt in § 4a BDSG sowie § 12 TMG.

[7] Siehe etwa §§ 4, 28 BDSG, § 13 TMG.

[8] Auskunftsanspruch des Betroffenen nach §§ 34 BDSG, 13 UKlaG.

[9] Hauptsächlich geregelt in Art. 5 Abs. 1 f) DS-GVO sowie in Art. 32 DS-GVO. Daneben in weiteren Bestimmungen wie z.B. Art. 24, 25, 36 DS-GVO die Datensicherheit.

[10] Konkretisiert werden diese Maßnahmen etwa durch die Aufzählung von Maßnahmen in § 58 Abs. 3 des Referentenentwurfes für das deutsche Ausführungsgesetz zur Datenschutz-Grundverordnung. Diese fußen auf der Anlage zu § 9 BDSG und erweitern diese.

[11] Siehe etwa Folgenabschätzung nach Art. 35 DS-GVO.

[12] „Data protection by default".

[13] Vgl. Informationsblatt des Bayerischen Landesamtes für Datenschutzaufsicht zu Artikel 32 DS-GVO.

10. IT-Sicherheit durch Mitarbeiterschulung

Sascha Wilms, Deutschland sicher im Netz e.V.

Abstract

Die Schwachstelle Mitarbeiter ist ein bevorzugtes Angriffsziel für Cyberkriminelle, denn regelmäßige Mitarbeiterschulungen zur Erhöhung des IT-Sicherheitsniveaus werden von Unternehmensleitungen weiterhin vernachlässigt. Sensibilisierungsmaßnahmen für Mitarbeiter für einen intakten Wirtschaftsschutz sind insbesondere auch für Kleine und Mittlere Unternehmen von großer Bedeutung. Einen vielsprechenden Ansatz bietet hier das Bildungsangebot *Bottom-Up: Berufsschüler für IT-Sicherheit* von Deutschland sicher im Netz.

10.1 Der Faktor Mensch und IT-Sicherheit

Mit der zunehmenden Digitalisierung der Arbeitswelt steigen auch die Anforderungen an den Schutz von Daten und die Sicherheit der IT-Infrastruktur. Unabhängig von politischen Forderungen auch nach einem „Security by Design", ist der Faktor Mensch als Schutzmaßnahme aber auch als Sicherheitsrisiko nicht zu vernachlässigen. Häufig ermöglichen wir als Anwender durch Unaufmerksamkeit und auch Unwissenheit erst IT-Angriffe.

Unter Umständen kann ein Datendiebstahl oder ein durch einen erfolgreichen Angriff provozierter Systemausfall ernstzunehmende finanzielle Folgen für betroffene Betriebe haben. Trotz der hohen Bedeutung für die Unternehmen und Ausbildungsbetriebe bilden die derzeitigen Ausbildungsordnungen der Länder die Vermittlung von IT-Sicherheitskompetenzen in Berufsschulen noch unzureichend ab.

Die neue Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt"[1] formuliert für berufsbildende Schulen vor dem Hintergrund des Ziels beruflicher Bildung – dem Erwerb einer umfassenden Handlungskompetenz –

Anforderungen an den Erwerb digitaler Kompetenzen lediglich auf einem höheren Abstraktionsgrad.

Ausbildung spielt heute und in Zukunft allerdings eine zentrale Rolle, wenn es um die IT-Sicherheit im Unternehmen geht: IT-Sicherheit ist ein eigenständiger Prozess und schließt in der Regel alle Geschäftsprozesse, die für die Bereitstellung von Produkten und Dienstleistungen in Betrieben nötig sind, ein. Deutschland sicher im Netz e.V. (DsiN) hat mit dem Ansatz *Bottom-Up* ein kostenfreies Bildungsangebot entwickelt, um dem bestehenden Aufklärungsdefizit auf Seiten der Mitarbeiter von heute und morgen entgegenzuwirken. Berufsschüler erfahren durch das Angebot bereits in ihrer Ausbildung praxisnahes IT-Sicherheitswissen und werden auf die Notwendigkeiten und Herausforderungen der digitalen Sicherheit im betrieblichen Alltag vorbereitet.

10.2 Passgenaue Schulungsangebote für den Mittelstand

Der Mittelstand schult (noch) zu wenig. Wie die Bundesdruckerei in einer aktuellen Studie *Digitalisierung und IT-Sicherheit in deutschen Unternehmen*[2] aufzeigt, werden Mitarbeiterschulungen in Unternehmen weiterhin vernachlässigt. Weniger als die Hälfte der befragten Unternehmen (46%) haben regelmäßige Mitarbeiterschulungen durchgeführt. Deutschland sicher im Netz kommt in einer eigenen Studie zu einem eindeutigeren Ergebnis: der Sicherheitsmonitor Mittelstand 2016[3] ergab, dass noch nicht einmal 25% der befragten Unternehmen regelmäßige Mitarbeiterschulungen durchführen.

10.3 Hoher Bedarf in Betrieben für IT-Sicherheitswissen

Gleichzeitig ist der Bedarf an digitalen Kompetenzen der Mitarbeiter in Unternehmen groß. Der Entwicklung des Bildungsangebots *Bottom-Up* ging eine Bedarfsermittlung[4] voraus: Rund 400 Unternehmensvertreter, Berufsschullehrkräfte und Auszubildende beteiligten sich an der Bedarfsanalyse. Deutlich wurde, dass die Mehrheit der Befragten bewertet die Vermittlung digitaler Kompetenzen als bedeutsam. 97% und somit fast jedes Unternehmen hält die Vermittlung entsprechender Kompetenzen für wichtig bzw. sehr wichtig. Bei Berufsschullehrkräften sind es 91% und bei den Berufsschülern 78%. Dies wird vor allem vor dem Hintergrund beachtenswert, dass IT-Sicherheit und

Datenschutz feste Bestandteile des Alltags in Unternehmen sind: 88% der Unternehmensvertreter geben an, dass ihnen diese Themen häufig bzw. sehr häufig in ihrem Arbeitsalltag begegnen.

Auf Basis der weiteren Ergebnisse der Bedarfsermittlung wurden die Schulungsmaterialien von *Bottom-Up* entwickelt. Da die Grenzen zwischen betrieblicher und privater Nutzung immer fließender werden, wurde die Themenabdeckung im Hinblick auf die Motivation der Schüler so gewählt, dass sie das angeeignete Wissen auch privat anwenden können. Dies ist vor dem Hintergrund der verschwimmenden Grenzen zwischen Berufsalltag und Privatem insbesondere für junge Auszubildende ein vielversprechender Ansatz.

10.4 Auszubildende bewähren sich als Multiplikatoren

Der Einsatz der Schulungsmaterialien an Berufsschulen ist wirksam: Lehrkräfte und Berufsschüler unterschiedlicher Ausbildungsgänge – von Schreiner- über Metallbaulehrlingen bis hin zu Auszubildenden im Bereich Büromanagement – setzen verschiedene Formate und Methoden zur Wissensvermittlung und dessen Anwendung im Betrieb ein.

Der Transfer der erworbenen Sicherheitskompetenzen durch die Berufsschüler erfolgt über Transfermaterialen für den Einsatz im Betrieb. Dazu gehören Quiz, Checklisten sowie weitere Handreichungen. Um die Auszubildenden bei der Anwendung des erlernten Sicherheitswissens zu unterstützen, werden Arbeitsaufträge mit Berufsschulen formuliert. Durch diese Maßnahme wird sichergestellt, dass das neue Wissen tatsächlich in den Betrieben ankommt.

Das Ergebnis des Ansatzes: Auszubildende können das neue Wissen unmittelbar im Betriebsalltag anwenden und sogar auch Kollegen und Chefs hilfreiche Hinweise geben.

10.5 IT-Sicherheit im Mittelstand verankern

Aufbauend auf der Vermittlung und dem Transfer von IT-Sicherheitswissen werden mit *Bottom-Up* Strukturen geschaffen, die Auszubildende als Multiplikatoren für gelebte IT-Sicherheit in den Ausbildungsbetrieben unterstützen. Ferner wurde hierzu eine gesonderte Lerneinheit für Auszubildende entwickelt, die das Ziel einer eigenen Betriebsgründung oder die Übernahme von

Führungsposition verfolgen. Gleichzeitig lernen sie dadurch die heutigen Anforderungen an die Betriebsleitung und Geschäftsführung kennen und werden für die Anforderungen im eigenen Ausbildungsbetrieb frühestmöglich sensibilisiert.

10.6 Verstärkte Aufklärung gegen Social Engineering und Phishing

Im Zuge der weiteren bundesweiten Verbreitung von *Bottom-Up* wird in den Schulungsmaterialien verstärkt auf den Schutz gegen Social Engineering und Phishing hingewirkt. Phishing nimmt weiterhin zu: laut der Analysen der Anti-Phishing Working Group, einer internationalen Allianz gegen Cybercrime, nahmen Phishing-Angriffe in 2016 im Vergleich zu 2015 um 65% zu[5] und erstreckten sich dabei über fast alle Kommunikationskanäle wie E-Mail, Post, Fax, Messenger, soziale Medien wie Facebook oder über ein direktes Gespräch. Beim CEO-Fraud beispielsweise geben sich Kriminelle in der Buchhaltung eines Unternehmens als Geschäftsführung aus und drängen auf eine schnelle Geldtransaktion auf ein von ihnen kontrolliertes Konto – und das oftmals mit Erfolg.

Abhilfe leistet hier nur eine gezielte Mitarbeitersensibilisierung. Dabei greift *Bottom-Up* auf bewährte und innovative Schulungsmaterialien und Formate zurück. Die Forschungsgruppe SECUSO (Security, Usability and Society) der Technischen Universität (TU) Darmstadt hat im Rahmen des Projekts KMU AWARE eigens Schulungsmaterialien zur Sensibilisierung für Phishing entwickelt.[6]

Weiterhin baut *Bottom-Up* auf die Integration von „Serious Game – Sicher im Internet" vom Verein Sichere Identität Berlin-Brandenburg.[7] Der Gamification-Ansatz bereitet Auszubildende und Mitarbeiter anhand eines Onlinespiels darauf vor, mögliche Angriffe und Schwachstellen im Berufsalltag frühzeitig zu erkennen und abzuwehren.

10.7 Fazit: Chancen für Ausbildungsbetriebe

Fest steht: Auszubildende werden durch das Schulungsangebot von *Bottom-Up* für die Sicherheitsherausforderungen des digitalen Geschäftsalltags sensibilisiert[8]. Der Transfer in die Ausbildungsbetriebe stellt sicher, dass das neu

erlernte Wissen auch dort ankommt, wo es benötigt wird. Ausbildungsbetriebe können die Schulungsunterlagen zudem zu Selbstlernzwecken sowie zu Mitarbeiterschulungen nutzen.

Damit bieten Auszubildende eine Chance für jeden Betrieb, das eigene Sicherheitsniveau zu erhöhen. Für einen maximalen Nutzen sind die Auszubildenden als Multiplikatoren für mehr IT-Sicherheit dabei auf die Unterstützung der Ausbildungsbetriebe und die Betriebsleiter angewiesen – IT-Sicherheit ist und bleibt eben auch Chefsache!

Lessons Learned

- Mitarbeiter sind häufig die größte Schwachstelle für die IT-Sicherheit.
- Nötige Sensibilisierungsmaßnahmen in den Unternehmen bleiben oftmals aus.
- Das Bildungsangebot *Bottom-Up* schult die Auszubildenden von heute und Betriebsleiter von morgen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
IT-Sicherheit IN DER WIRTSCHAFT

[1] Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (2016). Bildung in der digitalen Welt Strategie der Kultusministerkonferenz. Aufgerufen am 23.08.2017, Verfügbar unter: https://www.kmk.org/fileadmin/Dateien/pdf/Presse-UndAktuelles/2016/Bildung_digitale_Welt_Webversion.pdf.

[2] Bundesdruckerei (2017), Digitalisierung und IT-Sicherheit in deutschen Unternehmen. Aufgerufen am 23.08.2017. Verfügbar unter: https://www.bundesdruckerei.de/de/system/files/dokumente/pdf/Studie-Digitalisierung_und_IT-Sicherheit.pdf.

[3] Deutschland sicher im Netz, DsiN-Sicherheitsmonitor Mittelstand 2016. Aufgerufen am 23.08.2017. Verfügbar unter: https://www.sicher-im-netz.de/downloads/dsin-sicherheitsmonitor-2016.

[4] Deutschland sicher im Netz (2016), Bedarfsanalyse für die Vermittlung von IT-Sicherheitswissen an Berufsschulen. Aufgerufen am 23.08.2017. Verfügbar unter https://www.dsin-berufsschulen.de/bedarfsanalyse.

[5] Anti-Phishing Working Group (2016), APWG Phishing Activity Trends Report. Aufgerufen am 23.08.2017. Verfügbar unter https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf.

[6] www.awareness-im-mittelstand.de. Aufgerufen am 30.09.2017.

[7] www.sichere-identitaet-bb.de. Aufgerufen am 30.09.2017.

[8] www.dsin-berufsschulen.de. Aufgerufen am 30.09.2017.

11. Digitalisierung und Sicherheit müssen Hand in Hand gehen

Vanessa Grühser, IHK Berlin; Carsten Vossel, CCVOSSEL GmbH

Abstract

Die Digitalisierung wird ein immer stärkerer Wachstumstreiber für die Wirtschaft. Digitalisierung heißt gleichzeitig aber auch, an die IT- und Cybersicherheit im Unternehmen zu denken. Denn neben der Wirtschaft hat sich längst auch das Verbrechen digitalisiert. Für Unternehmen bedeutet das, eine Sicherheitsstrategie zu verfolgen, die neben der IT-Infrastruktur den Mitarbeiter in den Mittelpunkt stellt. Sicherheitsspezifische Weiterbildungen, Awareness-Kampagnen oder spezielle Software können dabei helfen.

11.1 Einleitung

Die Digitalisierung hat das Potential, (neue) digitale Geschäftsprozesse und -modelle über alle Branchen hinweg zu etablieren und das Wirtschaften auf digitale Füße zu stellen. Digitalisierung heißt gleichzeitig aber auch, an die IT- und Cybersicherheit im Unternehmen zu denken. Kleine und mittlere Unternehmen setzen sich dafür leider noch zu selten die „Sicherheitsbrille" auf – und das muss sich ändern. Denn die Digitalisierung des Verbrechens hat, wie in Abschnitt 11.2 Digitalisierung der Wirtschaft und Kriminalität deutlich wird, längst eingesetzt. Investitionen in die IT- und Cybersicherheit müssen in diesem Zusammenhang von Unternehmen als Investitionen in die Zukunfts- und Wettbewerbsfähigkeit verstanden werden. Die Verantwortung für die (digitale) Sicherheit liegt dabei – wie auch die Verantwortung für den wirtschaftlichen Erfolg und die Digitalisierungsstrategie – bei der Geschäftsführung. Davon ausgehend muss für eine erfolgreiche Sicherheitsstrategie der Mitarbeiter im Mittelpunkt stehen: Sicherheitsspezifische Weiterbildungen und Awareness-Kampagnen sind dafür, wie im Abschnitt 11.4 Sensibilisierung und Weiterbildung von Mitarbeitern gezeigt wird, geeignete Maßnahmen.

11.2 Digitalisierung der Wirtschaft und Kriminalität

Die Digitalisierung wird ein immer stärkerer Wachstumstreiber für die Wirtschaft. Dabei nehmen die Komplexität der Themen, der Prozesse und die Vernetzung in und zwischen Unternehmen zu. Gleichzeitig muss jedes Unternehmen sich in zunehmendem Maße mit (neuen digitalen) Bedrohungen – Spionage, Sabotage, Erpressung etc. – auseinandersetzen. Mit der Digitalisierung von Geschäftsprozessen und -modellen geht damit auch die Digitalisierung des Verbrechens einher. Diese Tendenz verschärft sich permanent und betrifft Unternehmen aller Größenklassen. Mit jeder technologischen Entwicklung wie zum Beispiel mobile Datennutzung, soziale Netzwerke, Cloud Computing, Smart grids oder Industrie 4.0, entstehen neue sicherheitsrelevante Fragestellungen im Unternehmen. Wie das IHK-Unternehmensbarometer zur Digitalisierung zeigt, sind sich Unternehmen dessen überwiegend bewusst – so nehmen 72% der Unternehmen in Deutschland wachsende Sicherheitsrisiken durch die Digitalisierung wahr (24% sehen keine Veränderung, nur 4% sogar weniger Risiken).[1] Deutlich wird auch, dass die gefühlte Bedrohung mit der Unternehmensgröße ansteigt. Ausschlaggebend für ein digitales Verbrechen ist jedoch primär die Tatsache, ob wirtschaftlich, politisch oder militärisch verwertbare Informationen vorliegen oder ob wertvolle immaterielle Vermögensgegenstände im Unternehmen existieren – und das ist oft auch in kleinen Unternehmen der Fall. Digitale und klassische Verbrechen stellen damit eine permanente unternehmerische Gefahr dar. Laut dem aktuellen Kriminalitätsbarometer sehen Berliner und Brandenburger Unternehmen in der Kriminalität das wichtigste gesellschaftliche Problem – noch vor dem Fachkräftemangel.[2] Die Zahl der von Hackerangriffen betroffenen Unternehmen hat sich von 2010 mit 11,9% bis 2016 auf 27,4% mehr als verdoppelt. Davon betroffen sind vor allem Dienstleister (34,6%) und Industriebetriebe (24,0%). Cyberdelikte verdrängen damit erstmalig klassische Deliktarten wie Betrug und Einbruchdiebstahl – das schlägt sich auch in der Schadenssumme nieder. Etwa ein Fünftel der Gesamtschäden durch Kriminalität sind auf Angriffe aus dem Internet zurückzuführen. Die Digitalisierung des Verbrechens hat damit die Unternehmen erreicht und verdeutlicht einmal mehr, dass die Digitalisierung der Wirtschaft nur mit einer IT-Sicherheitsstrategie erfolgreich sein kann.

11.3 Investition in IT-Sicherheit für Wettbewerbsfähigkeit

Das Thema Sicherheit, speziell IT- und Cybersicherheit, ist längst ein Querschnittsthema über alle Bereiche der Unternehmenstätigkeit hinweg. Kosten entstehen den Unternehmen dabei auf zwei Wegen: Zum einen müssen sie sich vor kriminellen Aktivitäten schützen und zum anderen tragen sie die Kosten zur Beseitigung von Schäden. Die IT- und Cybersicherheit muss daher bei der Umsetzung digitaler Strategien eine hohe Priorität erhalten. Die Digitalisierung im eigenen Unternehmen aktiv zu gestalten, heißt, die Sicherheit als eine strategische Aufgabe und Teil des Risikomanagements in der Geschäftsführung zu verstehen. Die Verantwortung für die Sicherheit liegt damit genauso wie die Verantwortung für den wirtschaftlichen Erfolg und die Digitalisierungsstrategie bei der Geschäftsführung. Die in diesem Zusammenhang getätigten Investitionen sind als Investitionen in die Zukunfts- und Wettbewerbsfähigkeit des eigenen Unternehmens zu bewerten. Am Anfang steht dabei in der Regel die Beauftragung eines externen IT-Dienstleisters mit anschließender Erstellung eines IT-Sicherheitskonzepts. Um kleineren Unternehmen ohne eigene Sicherheitsexpertise diesen ersten Schritt zu erleichtern, hat die IHK-Organisation dafür den Kriterienkatalog „IT-Dienstleistungen – aber sicher!" zusammengestellt, der bei der Auswahl eines vertrauenswürdigen IT-Dienstleistern behilflich sein kann.

Neben Investitionen in präventive Maßnahmen spielen für Unternehmen wie auch Sicherheitsbehörden die reaktiven Maßnahmen nach der Straftat eine besondere Rolle. Denn Unternehmen investieren, durch ihre Bereitschaft Straftaten im vollen Umfang anzuzeigen, unmittelbar in einen sicheren Wirtschaftsstandort. Eine (bewusste) Anzeigebereitschaft von Unternehmen ist damit Grundvoraussetzung, die die Politik und Sicherheitsbehörden in die Lage versetzt, Kriminalität wirkungsvoll zu bekämpfen. Nicht selten stellen sich betroffene Unternehmen erst im Schadensfall die Frage, welche Berliner Sicherheitsbehörde der richtige Ansprechpartner ist und wie dieser schnell und unkompliziert erreicht werden kann. Als ein erster Wegweiser kann dabei die IHK Broschüre „Unternehmen im Visier von Kriminellen" dienen.

Die zwei größten Hemmnisse für die Digitalisierung sehen Unternehmen in Deutschland im Datenschutz (58%) und der IT-Sicherheit (57%).[3] Triebfe-

dern dieser Unsicherheiten sind auch in den jeweiligen (aktuellen) gesetzlichen Regelungen zu finden. Fragen des Dateneigentums oder des Ortes der Datenspeicherung sorgen in vielen Unternehmen für Verunsicherung. Ein zukunftsfestes Datenschutzrecht muss dabei einen Spagat zwischen den grundrechtlich geschützten Interessen des Betroffenen und den legitimen Interessen von Unternehmen an der Nutzung von Daten schaffen. Die EU-Datenschutzgrundverordnung (EU-DSGVO) bemüht sich zwar um diesen Ausgleich. Die Praxis muss jedoch zeigen, ob die Regelung der Zweckbindung für die Datennutzung Unternehmen mit digitalen Geschäftsmodellen genügend Spielraum bietet. Mit Blick auf das IT-Sicherheitsgesetz könnten Vorbehalte von Unternehmen abgebaut werden, wenn z.B. Verpflichtungen für Anbieter von geschäftsmäßig betriebenen Webseiten durch handhabbare Empfehlungen ergänzt werden. Ziel bei allen staatlichen und wirtschaftlichen Aktivitäten muss es daher sein, Sicherheit entlang der Wertschöpfungskette nachhaltig zu gewährleisten. Sowohl der Staat als auch die Wirtschaft können auf diesem Wege dafür sorgen, Cybersicherheit als deutschen Wettbewerbsvorteil in der Digitalisierung zu etablieren. Der Staat muss dabei zukunftsfeste rechtliche Rahmenbedingungen sicherstellen, die rechtliche Verfolgung von IT-Kriminalität gewährleisten und durch eine gezielte Cybersicherheitsforschung Investitionsanreize in die IT- und Cybersicherheit schaffen. Auf Unternehmensebene muss dagegen für sichere digitale Produkte und Lösungen (Security-by-Design) gesorgt werden. Neben der Berücksichtigung von Sicherheitsaspekten in der Konzeptionsphase gilt es für Unternehmen, Sicherheit im Unternehmen als Ganzes zu leben. Im Mittelpunkt steht dabei der Mitarbeiter. Dieser soll nicht als Risikofaktor, sondern vielmehr als Sicherheitsfaktor agieren können. Um dieses Ziel zu erreichen, bedarf es sowohl einer Mitarbeitersensibilisierung für das Thema IT-Sicherheit als auch geeigneter Weiterbildungsmaßnahmen. Unternehmerische Maßnahmen und Vorgehensweisen werden im folgenden Abschnitt genauer betrachtet.

11.4 Sensibilisierung und Weiterbildung von Mitarbeitern

Die Befähigung von Mitarbeitern für die sichere Nutzung von IT-Systemen, die Einhaltung von Datenschutz und Datensicherheit und die Wachsamkeit, nicht Opfer von *Social Engineering*[4] zu werden, muss im Unternehmen aktiv

gelebt werden. Nur so können Digitalisierung und Sicherheit Hand in Hand gehen. Die erste und entscheidende Handreichung muss dabei von der Geschäftsführung kommen. Im besten Fall werden sicherheitsspezifische Weiterbildungen als ein dauerhafter Prozess etabliert, und ein interner Sicherheitsbeauftragter bzw. externer Dienstleister übernimmt in der Folge die aktive Umsetzung. Die Ergebnisse des DsiN-Sicherheitsmonitors Mittelstand verdeutlichen, dass unzureichende Kenntnisse der Mitarbeiter zu den größten Schwachstellen der IT-Sicherheit zählen.[5] Lediglich 27% der kleinen und mittelständischen Unternehmen bieten regelmäßige Schulungen und Informationen zur IT-Sicherheit für ihre Mitarbeiter an. In den letzten Jahren zeigte sich hierbei eine Stagnation, die besonders vor dem Hintergrund der Zunahme von Angriffen, die auf die „Schwachstelle Mitarbeiter" ausgerichtet sind, Gefahren für das Unternehmen mit sich bringen.

Diese Stagnation überrascht auch deshalb, weil der Großteil der Unternehmen den aus der Digitalisierung resultierenden Weiterbildungsbedarf durchaus erkennt: Eine aktuelle TNS-Infratest-Studie ergab, dass 88% der befragten Unternehmen den sicheren Umgang ihrer Mitarbeiter mit dem Thema IT-Sicherheit als wichtig oder äußert wichtig bewerten.[6] Einen Überblick über effektive und schnell umsetzbare Maßnahmen können oft schon kompakte Seminarformate liefern. Unter der URL *www.ihk-berlin.de/seminaritsicherheit* bietet die IHK Berlin ein Tagesseminar zum Thema IT-Sicherheit an, das speziell auf die Bedarfe kleiner und mittlerer Unternehmen ausgerichtet ist.

Carsten Vossel, Geschäftsführer der CCVOSSEL GmbH Berlin, wird in Abschnitt 11.5 in Form eines Gastbeitrags einen Einblick in die digitalen Gefahren im Unternehmen geben und ausgewählte Möglichkeiten aufzeigen, mit denen die Geschäftsführung mit ihren Mitarbeitern gemeinsam zur Unternehmenssicherheit beitragen kann.

11.5 Horrorszenario „Angriff auf die Unternehmens-IT"

Die Anforderungen an Unternehmen steigen derzeit aus unterschiedlichen Gründen. Zum einen steigen die Cyber-Angriffe exponentiell und ebenso die Abhängigkeit von der IT. Zum anderen werden vom Gesetzgeber neue Regeln definiert wie z.B. KRITIS und EU-Datenschutzgrundverordnung. Zusätzlich

steigt der Druck, durch Kunden, Finanzinstitute und Versicherer beim Thema Informationssicherheit gut aufgestellt zu sein und dies gegebenenfalls auch nachweisen zu können.

IT-Verantwortliche verkünden deshalb oft „Wir sind gut geschützt, unser Netzwerk ist sicher" und wähnen sich in Sicherheit. Durch Firewall, Virenschutz und weiterer Systeme sind die Daten vor einem Hackerangriff von außen geschützt. Doch erfolgt der Angriff von innen, schützen diese Systeme nur zum Teil. Doch wie kann solch ein Angriff erfolgen? Hier einige Beispiele, die auch so im „echten Leben" passieren:

Cyber-Kriminelle verschaffen sich Zugang auf Ihre Systeme und verschlüsseln Ihre Unternehmensdaten. Kurze Zeit danach bekommen Sie von den Hackern eine Aufforderung zur Zahlung von Lösegeld, um wieder Zugriff auf diese zu bekommen und weiterarbeiten zu können. Man kann sagen, in diesem Fall haben Kriminelle ein für sich „erfolgreiches Phishing" durchgeführt – Sie oder einer Ihrer Mitarbeiter hat vermutlich unwissentlich und völlig unbekümmert auf eine gefälschte E-Mail reagiert oder einen Link angeklickt. Schäden (Zahlungen von z.B. Lösegeldern) belaufen sich hier schnell auf viele Tausend Euro. Oder erinnern Sie sich an den Fall, bei dem Hacker in Großbritannien die Computersysteme vieler Krankenhäuser und Arztpraxen lahmlegten? Die Ärzte mussten Ihre Arbeit niederlegen, Operationen verschoben werden, Kranke wurden nach Hause geschickt oder in andere Kliniken verlegt. Für ein Krankenhaus der schlimmste anzunehmende Vorfall. Auch die Deutsche Bahn wurde kürzlich Opfer eines Angriffs – auf vielen Bahnhöfen zeigten die digitalen Informationstafeln die An- und Abfahrtzeiten nicht mehr an, was bei vielen Reisenden zu Ärger führte und dem Image der Bahn schadete. Der französische Autobauer Renault stoppte nach einem Angriff in einigen Werken sogar seine Produktion – als Schutzmaßnahme, um eine Ausbreitung einer Schadsoftware zu verhindern. Allen Betroffenen war eines gemeinsam: Sie wurden Opfer Cyber-Krimineller durch Ransomware bzw. Verschlüsselungstrojaner wie WannaCry, Locky oder Petya. Und noch eines vereinte alle Opfer: Die Schwachstelle war nicht das System, sondern das fehlende Bewusstsein der Mitarbeiter für Cyber-Gefahren.

11.5.1 Schulungen zur IT-Sicherheit und die interne Akzeptanz

Sie müssen täglich Ihre Kunden zufriedenstellen, Wirtschaftspläne erfüllen und innovative Lösungen präsentieren – damit sind Sie und Ihre Mitarbeiter voll ausgelastet und es bleibt wenig Zeit für weitere Schulungen. Diese Mehrbelastung könnte zu wenig Akzeptanz und Unterstützung für das zusätzliche Thema Security Awareness bzw. IT-Sicherheit führen und als reine Zeitverschwendung gesehen werden. Denn:

1. Für die Zeit des Besuchs von solchen Maßnahmen in Form von Schulungen gerät Ihre eigentliche Tätigkeit in den Hintergrund – und kostet im Regelfall viel Geld.
2. Nicht für jeden Teilnehmer ist der vermittelte Inhalt passend, oft wird eher nach dem Gießkannenprinzip informiert (Jeder Teilnehmer erhält ungeachtet seiner Tätigkeit die gleichen Informationen.).
3. Unter „Zwang" besuchte Security Awareness Schulungen führen häufig zur generellen Ablehnung des Themas Security.
4. Die Teilnehmer fühlen sich nicht angesprochen, denn so etwas könne ihnen doch nicht passieren, da sie in ihren Augen mit keinen wichtigen Daten arbeiten.

11.5.2 Möglichkeiten der Mitarbeiter-Schulung

Awareness-Kampagnen können Ihnen helfen, das Verhalten im Umgang mit der Cyber-Sicherheit nachhaltig zu ändern. Sachverhalte wie schnell z.B. Cyber-Kriminelle an Daten gelangen oder welche Trojaner gerade im Umlauf sind, helfen bei der Einschätzung der Gefahr. Dafür müssen Sie sich täglich umfassend informieren, um diese Informationen zeitnah weitergeben zu können. Zusätzlich hätten Sie aber auch die Möglichkeit, Ihre IT-Sicherheit durch einen IT-Dienstleister messen zu lassen. Äußerst wirkungsvoll ist der sogenannte Awareness Check. Dieser beinhaltet unter anderem eine Phishing-Kampagne und die daraus resultierende Reaktion Ihrer Mitarbeiter. Dabei werden durch einen IT-Dienstleister Fake-E-Mails an Ihre Mitarbeiter verschickt und später anonym ausgewertet. Wie häufig wurden diese E-Mails geöffnet, der angebotene Link in der E-Mail angeklickt und angehängte Dateien

geöffnet. Eine anschließende Konfrontation der Mitarbeiter mit den erzielten Ergebnissen schärft deren und Ihre Sinne für zukünftige Bedrohungen.

Eine einfache Möglichkeit regelmäßig in den Blick zu bekommen, was in Bezug auf IT-Sicherheit wichtig ist, bietet sogenannte Awareness-Software. CCAWARE zum Beispiel ersetzt den Anmeldebildschirm durch regelmäßig wechselnde Motive, die in Text und Bild das Thema IT-Sicherheit unterhaltsam aufgreifen. So gelingt mit geringen Aufwand und Kosten eine kontinuierliche Sensibilisierung der Belegschaft und somit eine Steigerung der Awareness gegenüber von Hackern gestellten Fallen.

11.6 Fazit

Der Mensch ist und bleibt die größte Sicherheitslücke im IT-System jedes Unternehmens. Eine Lücke die sich nicht schließen, sondern nur verkleinern lässt und trotzdem größer wird, wenn man Sie aus dem Blick verliert. Dieser Herausforderung gilt es auf Unternehmensebene mit einer Sicherheitsstrategie, die neben der IT-Infrastruktur den Mitarbeiter in den Mittelpunkt stellt, zu begegnen. Maßnahmen wie sicherheitsspezifische Weiterbildungen und Awareness-Kampagnen oder spezielle Software können zu einem größeren Sicherheitsbewusstsein im ganzen Unternehmen beitragen. Um mehr IT- und Cybersicherheit zu erreichen, ist es wichtig, dass die Geschäftsführung Sicherheit als eine strategische Aufgabe und als Teil des Risikomanagements versteht und gleichzeitig den Mitarbeiter zu einem sicheren Verhalten befähigt. Ausschlaggebend ist neben der Qualität der Maßnahmen natürlich auch ihre Anwendungshäufigkeit. Die Digitalisierung des eigenen Unternehmens und die damit verbundene Sicherheit müssen Hand in Hand gehen. Aktuelle Entwicklungen bei Cyberangriffen verdeutlichen, dass das Verbrechen nicht mehr nur analog seine Opfer sucht, sondern schon längst digital unterwegs ist und sich immer neue Angriffswege erschließt. Eine kontinuierliche sicherheitsbezogene Aufmerksamkeit und Anpassungsfähigkeit muss damit zum unternehmerischen Grundwerkzeug gehören.

Lessons Learned

- Investitionen in die IT- und Cybersicherheit sind Investitionen in die Zukunfts- und Wettbewerbsfähigkeit des Unternehmens.
- Die größte Sicherheitslücke in der IT ist immer noch der Mensch.
- Sicherheitsspezifische Weiterbildungen und Awareness-Kampagnen sind unerlässlich.

---

[1] Liecke, M., Sobania, K. & van Renssen, L. (2016). Wirtschaft digital: Perspektiven erkannt, erste Schritte getan. Das IHK-Unternehmensbarometer zur Digitalisierung. Berlin: Deutscher Industrie- und Handelskammertag.

[2] Herrschelmann, T. & Kuß, A. (2017). Kriminalitätsbarometer Berlin-Brandenburg 2017. Eine vergleichende Studie zur Belastung der Wirtschaft mit Kriminalität. Frankfurt (Oder): Industrie- und Handelskammer Ostbrandenburg.

[3] Liecke, M., Sobania, K. & van Renssen, L. (2016). Wirtschaft digital: Perspektiven erkannt, erste Schritte getan. Das IHK-Unternehmensbarometer zur Digitalisierung. Berlin: Deutscher Industrie- und Handelskammertag.

[4] Unter Social Engineering oder auch soziale Manipulation versteht sich die zwischenmenschliche Beeinflussung mit dem Ziel, bei Personen bestimmte Verhaltenswei-sen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.

[5] Brandl, S., Engler, N., Grau, N., Wilms, S. & Zimmermann, M. (2016). DsiN-Sicherheitsmonitor Mittelstand 2016. Berlin: Deutschland sicher im Netz e.V. und DATEV eG.

[6] TNS Infratest / Studiengemeinschaft Darmstadt Studie (2017). Weiterbildungstrends in Deutschland 2017. Aufgerufen am 16.08.2017 unter: http://www.digitalbusiness-cloud.de/aktuelle-tns-infratest-studie-2017-digitalisierung-erhoeht-weiterbildungsbedarf.

12. Usable Security – Mit Benutzerfreundlichkeit zu mehr IT-Sicherheit

Hartmut Schmitt, HK Business Solutions GmbH; Luigi Lo Iacono, TH Köln

Abstract

Software, Apps und vernetzte Technikprodukte müssen mit Sicherheitsfeatures ausgestattet sein, die einen wirksamen Schutz vor Cyberangriffen bieten. Auf Anwenderebene präsentieren sich diese Sicherheitsfeatures jedoch oft mit einer schlechten Usability, weshalb sie von den Nutzern falsch bedient, ignoriert oder gar umgangen werden. Hierdurch eröffnen sich mögliche Angriffsflächen für Cyberkriminelle – mit weitreichenden Folgen für die IT-Sicherheit der Nutzer bzw. Unternehmen.

12.1 Digitale Transformation erfordert adäquaten Schutz

Informationstechnische Systeme durchdringen alle Bereiche unseres beruflichen Alltags. Auch kleinere Firmen, Dienstleister und Handwerker sind immer stärker mit ihren Kunden, Partnern und Lieferanten vernetzt. Der Mittelstand hat längst erkannt, welche Chancen sich durch die digitale Transformation von Unternehmen eröffnen. Diese reichen von der effizienteren Ausgestaltung von Geschäftsprozessen bis hin zu nicht dagewesenen Möglichkeiten der Wertschöpfung durch neuartige Geschäftsmodelle. Der digitale Wandel ist jedoch auch mit neuen Risiken verbunden. Es fallen kaum noch zu überschauende Datenmengen an, die großteils in Clouds abgelegt bzw. verarbeitet werden und für deren Schutz geeignete Sicherheitskonzepte und Schutzmechanismen benötigt werden. Die Folge: Zu dem enormen Funktionsangebot von Software, technischen Produkten, Apps und Onlineservices, aus dem Firmen heute wählen können, gesellt sich eine ebenso große Anzahl von Technologien für die Daten-, Informations- und Kommunikationssicherheit, z.B. Virenscanner, Firewalls und Werkzeuge für die Kommunikations- und Datenverschlüsselung.[1]

Trotzdem ist der Mangel an IT-Sicherheit noch eines der größten Hemmnisse der Digitalisierung[2]. In den vergangenen zwei Jahren wurden mehr als zwei Drittel der deutschen Industrieunternehmen (69%) Opfer von Cyberangriffen wie Datendiebstahl, Wirtschaftsspionage oder digitaler Sabotage, wodurch allein der deutschen Industrie pro Jahr ein Schaden von 22,4 Milliarden Euro entsteht[3]. Mit der fortschreitenden Digitalisierung und der zunehmenden Vernetzung einhergehend, vergrößert sich die Angreifbarkeit der verwendeten IT-Systeme; es wird daher erwartet, dass die Cyber-Attacken und der dadurch verursachte Schaden noch massiv ansteigen werden[4].

Dass die Anzahl der erfolgreichen Angriffe trotz jahrelanger Forschung und Entwicklung an sicheren IT-Systemen zunimmt, hat vielfältige Ursachen. Eines der zentralen Probleme ist, dass Sicherheitsmechanismen nicht auf allen Ebenen der Wertschöpfungskette so ausgestaltet sind, dass sie für die betreffenden Personenkreise auch effizient, effektiv und zufriedenstellend anwendbar sind.[2] Vor welche großen Probleme die Verwendung von Sicherheitskomponenten viele Nutzer stellt, macht beispielsweise der IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik (BSI)[5] deutlich: er unterscheidet allein über 100 menschliche Fehlhandlungen. Viele davon rühren daher, dass die festgelegten Sicherheitsvorschriften und implementierten Sicherheitsmechanismen den Nutzer überfordern. Empfindet ein Nutzer die Schutzmechanismen und Sicherheitsfunktionen seiner betrieblichen Software jedoch als Barriere oder als leistungsverringernd, so besteht die Gefahr, dass er diese unbewusst falsch verwendet oder bewusst umgeht; dies kann dazu führen, dass der Schutz sensibler Daten versagt und unter Umständen das gesamte Sicherheitskonzept des Unternehmens zu Fall gebracht wird[1].

12.2 Nutzerzentriertes Security Engineering

Der Nutzer wurde lange Zeit zu Unrecht als schwächstes Glied in der „Sicherheitskette" betrachtet[6] bzw. dazu gemacht. Er wurde als Sicherheitsrisiko behandelt, das kontrolliert werden muss,[7] und daher in der Regel nicht in die Konzeption und Entwicklung von Sicherheitskonzepten einbezogen. Das Ergebnis dieser traditionellen Sichtweise sind Sicherheitstechnologien, deren

Anforderungen von durchschnittlichen Nutzern nur schwer gänzlich erfüllt werden können. Digitale Schutzmechanismen bieten jedoch nur dann einen effektiven Schutz, wenn sie von allen relevanten Nutzergruppen grundlegend verstanden werden und keine Barriere in der Nutzung der IT-Systeme darstellen.[8] Letzteres heißt aber nicht, dass Sicherheitsmechanismen nur dann gebrauchstauglich sind, wenn sie ihre Funktion autark und unsichtbar für den Nutzer im Hintergrund erbringen. In vielen Fällen ist eine aussagekräftige Visualisierung des Sicherheitszustandes sogar explizit gewünscht. Während der Bearbeitung der Primäraufgaben dürfen die Sicherheitsfunktionen jedoch keine ständige Interaktion erfordern, da dies zur Belastung wird.

Um die Basis für eine systematische Entwicklung sicherer und benutzbarer interaktiver Produkte zu schaffen, müssen daher die Konzepte, Methoden und Werkzeuge des Security Engineerings mit denen des Usability Engineerings zusammengeführt werden, also den Planungs- und Entwicklungsarbeiten, die die spätere Gebrauchstauglichkeit der Systeme gewährleisten sollen. Hierbei sind Modelle aus der Psychologie ebenso zu berücksichtigen wie Ergebnisse der Designforschung. Durch diesen interdisziplinären Ansatz, der seit einigen Jahren unter dem Schlagwort *Usable Security* oder *gebrauchstaugliche Informationssicherheit* diskutiert wird, sollen auch Laien und technikferne Anwender in die Lage versetzt werden, Sicherheitselemente und deren Notwendigkeit besser zu verstehen und diese in der dafür vorgesehenen Weise zu verwenden.

Ob und wie erfolgreich ein Nutzer Sicherheitsfunktionen von Software anwendet, ist von einer Vielzahl von Faktoren abhängig,[9] z.B. von seinem Vorwissen und seinen Erfahrungen, aber auch von seiner Motivation die Sicherheitsfunktionen zu nutzen. Ein Beispiel macht dies deutlich: Für die Anmeldung der Nutzer an einem IT-System werden meist Passwörter eingesetzt. In Passwortregelwerken ist festgelegt, wie lang diese sein müssen, ob sie Sonderzeichen enthalten müssen und wie oft sie geändert werden müssen. Da viele Nutzer durch die Anzahl und Komplexität der von ihnen verwendeten Passwörter überfordert sind, kommt es beim Umgang mit Passwörtern immer wieder zu Fehlverhalten, z.B. werden zu einfache Passwörter gewählt oder die Passwörter werden für andere sichtbar notiert. Es existieren zwar vielversprechende

Lösungsansätze, bei denen die Nutzer keine Passwörter mehr eingeben müssen, sondern vom System anhand biometrischer Merkmale oder ihrer Nutzungsprofile erkannt werden. Trotzdem werden heute immer noch meist Passwörter zur Authentifizierung verwendet – selbst bei Geräten mit Touchscreens, bei denen das Eintippen von Sonderzeichen dreimal länger dauert als mit Tastaturen.[10]

Ein weiteres Beispiel, das den Bedarf an gebrauchstauglichen und benutzerfreundlichen Lösungen aufzeigt, ist die vertrauliche E-Mail-Kommunikation: Obwohl seit etwa 20 Jahren an gebrauchstauglichen Lösungen für die E-Mail-Verschlüsselung geforscht wird,[11] sehen auch bei einer aktuellen Studie[12] noch 70% der Teilnehmer Verbesserungsbedarf. Es besteht also ein großes Interesse nach verwertbaren Erkenntnissen aus der Forschung, aber auch nach praktischen Empfehlungen für deren Umsetzung – in IT-Sicherheitsfeatures und -lösungen, die auch für Laien und Gelegenheitsnutzer verständlich und benutzbar sind.

12.3 Lösungen für mittelständische Unternehmen

Eine wichtige Grundlage für die Entwicklung benutzerfreundlicher und gleichzeitig sicherer IT-Systeme kann ein ganzheitliches Qualitätsverständnis bilden, in dem die Merkmale Usability und Security nicht mehr primär als konkurrierende oder gar unvereinbare Qualitätsmerkmale wahrgenommen werden. Einen Beitrag hierzu leistet das Qualitätsmodell, das im Forschungsprojekt USecureD[13] entwickelt wurde (siehe Abbildung 16). Es umfasst die drei relevanten Teilbereiche *Gebrauchstauglichkeit*, *Sicherheit* und *Nutzungsqualität*. Ziel bei der Entwicklung des Modells war es, sowohl Softwareentwicklern als auch Nutzern in mittelständischen Betrieben eine möglichst einfache, nachvollziehbare und vergleichbare Bewertung der Qualität ihrer Produkte zu ermöglichen.

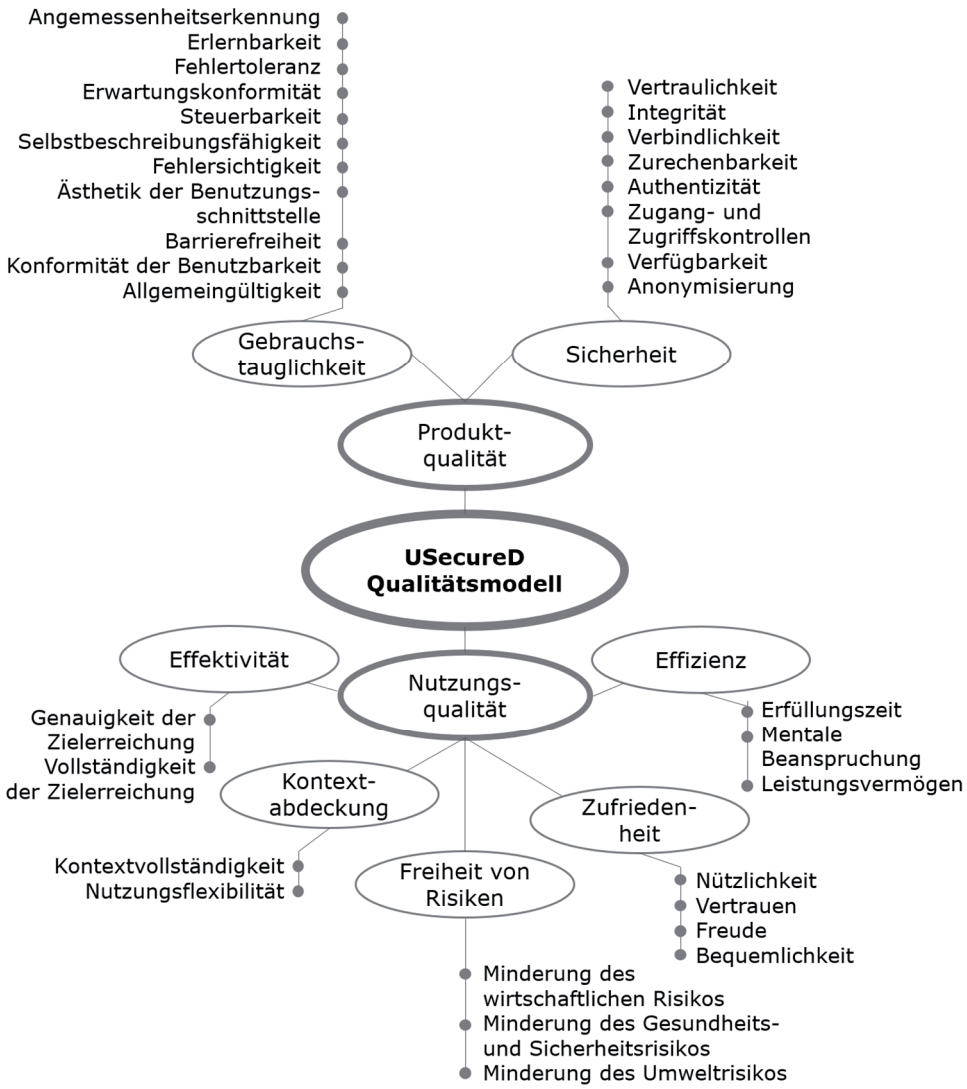

Abbildung 16: Qualitätsmodell des USecureD-Projekts. © TH Köln.

Es bedarf allerdings noch vieler weiterer Arbeitshilfen für Softwareentwickler, die dabei helfen, ein gutes Verständnis für gebrauchstaugliche IT-Sicherheit aufzubauen, und eine effiziente Unterstützung bei der Umsetzung bieten. Auch an dieser Stelle setzt das USecureD-Projekt an: Es stellt Methoden und

Werkzeuge zur Verfügung, die bereits in frühen Phasen der Produktentwicklung genutzt werden können, z.B. bei der Konzeption von IT-Systemen, beim Treffen grundlegender Architekturentscheidungen und bei der Anfertigung erster Oberflächenentwürfe. Diese Entwurfs- und Gestaltungswerkzeuge wurden auf unterschiedlichen Abstraktionsebenen dokumentiert als *Prinzipien*, *Richtlinien* und sogenannte *Patterns* (siehe Abbildung 17).

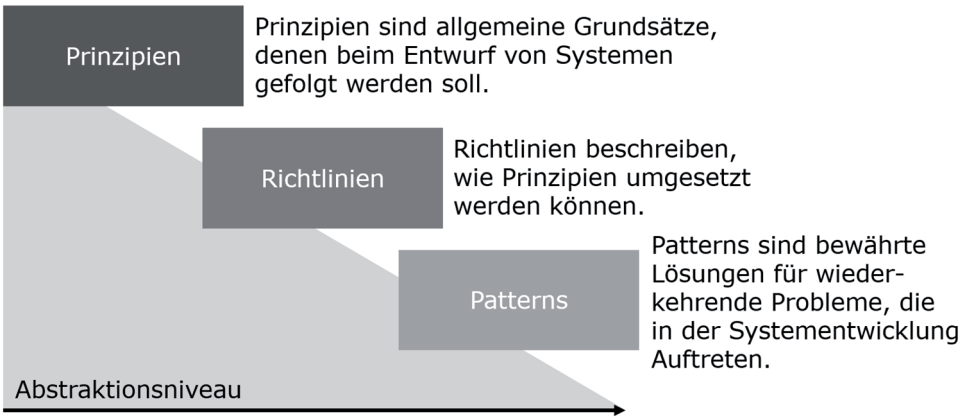

Abbildung 17: Entwurfs- und Gestaltungswerkzeuge des USecureD-Projekts. © TH Köln.

Durch den Einsatz dieser Werkzeuge kann erreicht werden, dass viele Probleme, die die Gebrauchstauglichkeit betreffen, gar nicht erst zustande kommen, weil sowohl das Sicherheitsfeature als auch der zugrundeliegende Entwicklungsprozess von vornherein bestimmte Eigenschaften und Qualitätsattribute besitzen. Neben solchen Entwurfs- und Gestaltungswerkzeugen wurden im Rahmen des Projekts auch Evaluationsmethoden und -werkzeuge entwickelt, mit denen im Anschluss an die Produktentwicklung überprüft werden kann, ob das Qualitätsmerkmal Usable Security erfolgreich umgesetzt wurde. Außerdem wurden Checklisten und ähnliche Werkzeuge erarbeitet, die Anwenderunternehmen bei einer Auswahl von E-Business-Anwendungen mit dem Qualitätsmerkmal Usable Security unterstützen. Die beschriebenen Ergebnisse stehen auf der Projektwebsite[13] sowie einer Werkzeug-Plattform[14] kostenlos als Downloads und zur Anwendung zur Verfügung.

Lessons Learned

- Viele der heutigen Sicherheitsfeatures werden von den Nutzern ignoriert, umgangen oder falsch angewendet.
- Um bessere Lösungen zu erreichen, muss die interdisziplinäre Zusammenarbeit zwischen IT-Security-Spezialisten, Usability-Spezialisten, Designern und Psychologen intensiviert werden.
- Im Forschungsprojekt USecureD wurden Werkzeuge entwickelt, die Mittelständler bei der Entwicklung und der Auswahl von Produkten mit dem Qualitätsmerkmal *Usable Security* unterstützen.

---

[1] Gorski, P. L., Lo Iacono, L. & Schmitt, H. (2015). Usable Security und Privacy by Design – Teil 1: Benutzerzentrierte Entwicklung von Sicherheitsfunktionen. Entwickler Magazin, Ausgabe 2015(6), S. 62–68.

[2] Holz, T., Pohlmann, N., Bodden, E., Smith, M. & Hoffmann, J. (2016). Strategiepapier IT-Sicherheit. Aufgerufen am 12.07.2017. Verfügbar unter: https://www.ptj.de/lw_resource/datapool/_items/item_7794/strategiepapier_it-sicherheit.pdf.

[3] Shahd, M. & Kopke, C. (2016). Industrie im Visier von Cyberkriminellen und Nachrichtendiensten. Aufgerufen am 12.07.2017. Verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Industrie-im-Visier-von-Cyberkriminellen-und-Nachrichtendiensten.html.

[4] TÜV TRUST IT GmbH (2015). Unternehmen werden 2015 ihre Sicherheitsstrategien stärker gewichten. Aufgerufen am 12.07.2017. Verfügbar unter: https://it-tuv.com/unternehmen-werden-2015-ihre-sicherheitsstrategien-staerker-gewichten/.

[5] Bundesamt für Sicherheit in der Informationstechnik (2016). IT-Grundschutz-Kataloge - G 3 Menschliche Fehlhandlungen. Aufgerufen am 12.07.2017. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03.html.

[6] Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. New York, NY: John Wiley & Sons.

[7] Adams, A. & Sasse, M. A. (1999). Users Are Not the Enemy. Communications of the ACM, Ausgabe 42(12), S. 40–46.

[8] Schmitt, H., Gorski, P. L. & Lo Iacono, L. (2016). Usable Security – Benutzerfreundliche Sicherheitsfunktionen für Software und interaktive Produkte. Wissenschaft trifft Praxis, Ausgabe 6, S. 5-13.

[9] Cranor, L. F. (2008). A Framework for Reasoning About the Human in the Loop. In E. Churchill & R. Dhamija (Hrsg.), Proceedings of the 1st Conference on usability, Psychology, and Security 2008 (1. Artikel). Berkeley, CA: USENIX Association.

[10] Sasse, M. A. (2013). „Technology Should Be Smarter Than This!": A Vision for Overcoming the Great Authentication Fatigue. In W. Jonker & M. Petković (Hrsg.), Secure Data Management (S. 33–36). Berlin: Springer.

[11] Whitten, A. & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium (S. 169–184). Berkeley, CA: USENIX Association.

[12] Nguyen, H. V. & Lo Iacono, L. (2016). USecureD – Auswertung der Online-Studie. Aufgerufen am 12.07.2017. Verfügbar unter: https://www.usecured.de/UseWP/wp-content/uploads/2015/04/USecureD-Anforderungsanalyse-Online-Studienergebnisse-V.1.pdf.

[13] USecureD-Konsortium (2017). USecureD – Usable Security by Design. Aufgerufen am 12.07.2017. Verfügbar unter: https://www.usecured.de/. Das Projekt USecureD (Laufzeit: Mai 2015 – April 2017) wurde vom Bundesministerium für Wirtschaft und Energie im Rahmen der Förderinitiative „Einfach intuitiv – Usability für den Mittelstand" unter Förderkennzeichen 01MU14002 gefördert.

[14] Technische Hochschule Köln, Data and Application Security Group (2017). USecureD Tools. Aufgerufen am 12.07.2017. Verfügbar unter: https://das.th-koeln.de/usecured.

13. Bedrohungen und Maßnahmen zur IT Sicherheit für Kleine und Mittlere Unternehmen: Eine Checkliste

Michael Holzhüter
HTW Berlin / Fraunhofer-Institut für Offene Kommunikationssysteme

Abstract

Nicht nur die großen Unternehmen sind von IT-Sicherheitsvorfällen betroffen. Die Frage ist nicht wie das Unternehmen angegriffen wird, sondern wann. Die meisten Gegenmaßnahmen sind sehr trivial und benötigen nur einen organisatorischen Aufwand, ohne spezielles IT-Wissen. Mittels einer Checkliste können die Unternehmen prüfen, welche Themen sie noch angehen müssen.

13.1 Einleitung

Themen rund um die IT Sicherheit sind Top Themen in der IT für Unternehmen.[1] Gründe liegen dabei in der zunehmenden Vernetzung der Betriebe untereinander sowie dem zunehmenden Digitalisierungsgrad. Gerade aber kleine und mittelständische Unternehmen haben nicht die eigenen Kapazitäten oder das Wissen, diese Themen zielgerichtet anzugehen.

Die Hochschule für Technik und Wirtschaft Berlin hat sich diesem Thema angenommen und ein Sicherheitslabor für alle Themen rund um die IT-Sicherheit gegründet. In Zusammenarbeit mit dem Fraunhofer Institut für offene Kommunikationssysteme sowie der Fraunhofer Academy wird an der Hochschule ein Lernlabor Cybersicherheit geschaffen. In diesem werden zahlreiche Schulungen für Sicherheitsthemen angeboten.[2]

13.2 Unternehmensgröße

Nicht nur großen Unternehmen sind Ziele für Cyberattacken, sondern ebenso kleine und mittlere Unternehmen sowie Privatpersonen. Das Ziel ist es dabei oft nicht, die Person dahinter zu schädigen, sondern eine weitere Verbreitung

der Schadsoftware. Auch die Bildung von Netzwerken, um eine großangelegte Aktion gegen Dritte zu fahren, ist eines der Szenarien. Ziel sind hierbei gerade die kleinen Unternehmen, die nicht die Möglichkeiten haben, sich in einem Umfang wie ein Konzern gegen solche Bedrohungen zu schützen, auch bemerken kleinere und mittlere Unternehmen häufig einen Sicherheitsvorfall erst spät oder gar nicht.

13.3 Bedrohungen und Maßnahmen

Welche Bedrohungen sind überhaupt relevant? Die Antwort darauf lautet: alle, jedoch muss danach unterschieden werden, wie hoch die Wahrscheinlichkeit ist, dass diese Bedrohung eintritt. Gerade diese Fragen sind ohne Erfahrung in der IT häufig nicht zu beantworten. Ebenso relevant ist die Frage, wie diesen Gefahren gegenübergetreten wird und was gemacht werden muss, wenn das Unternehmen selbst Opfer eine Cyber-Attacke geworden ist.

Hinter den Maßnahmen stehen im Verhältnis wenig technische Maßnahmen, sondern mehr organisatorische Maßnahmen. Die technischen Maßnahmen kann ein IT Dienstleitungsunternehmen erledigen, die organisatorischen Maßnahmen hingegen müssen selbst im Unternehmen angetrieben werden. Mitarbeiter müssen zu den Themen sensibilisiert werden und Arbeitsabläufe oder technische Voraussetzungen angepasst werden, damit Sicherheitsvorfälle vermieden werden können. Sämtliche IT Systeme müssen dokumentiert werden, damit IT Dienstleister oder Mitarbeiter angewiesen werden können.

Dazu sollen folgende Punkte Aufschluss über Bedrohung in den verschiedenen Sektoren sowie Maßnahmen geben, um diese zu unterbinden. Diese sind nicht getrennt voneinander zu betrachten, sondern bieten den Unternehmen in ihrer Gesamtheit einen Basisschutz für IT Sicherheit im Unternehmen. Auch wenn diese Maßnahmen Aufwand bedeuten, ist dieser in den meisten Fällen sinnhaft investiert. Der Mehrwert daraus wird bei Eintritt der Bedrohung bzw. bereits davor für die Verhinderung einer Bedrohung ersichtlich.

1. *Mitarbeiter*

   Gerade die Bedrohung von innen wird immer wieder unterschätzt. Gekündigte Mitarbeiter, die weiterhin Zugang zu den IT Systemen oder Räumen haben, sind eine große Bedrohung. Aber auch Mitarbeiter mit erweiterten Rechten (Geschäftsführung, IT Administratoren, Assistenz der Geschäftsleitung) sind beliebte Ziele für Hacker.[3]

   Dazu sind ungeklärte Zuständigkeiten oder nicht vorhandene Vertreter häufige Probleme. Um diesen Problemen vorsorglich entgegen zu wirken, sollten folgenden Maßnahmen ergriffen werden:

   - Das Erstellen von Checklisten für den Eintritt und den Austritt von Mitarbeitern erinnert daran, welche Dinge Mitarbeitern gegeben wurden, beispielsweise Passwörter für IT Systeme, Schlüssel, IT wie Notebooks, Mobilfunkgeräte und die dazugehörigen PINs, Code für die Alarmanlage, etc.
   - Eine Übersicht über die Rechte und Profile in ihrem IT-System bietet außerdem eine schnelle und effiziente Übersicht. Hier sollte nach dem Motto „Weniger ist Mehr" gearbeitet werden. Auch wenn es mit Aufwand verbunden ist, immer mal wieder das Berechtigungskonzept anzupassen, ist es besser, von Anfang an, so wenig Rechte wie möglich einzuräumen. Werden diese später wieder entzogen, sind Konflikte vorprogrammiert.
   - Aber auch der Zugang zu Räumen sollte dokumentiert werden. Eine Zutrittsregelung bzw. -berechtigung hilft ihren Checklisten für den Eintritt und Austritt von Mitarbeitern.
   - Arbeiten die Mitarbeiter mit personenbezogenen Daten sollten diese darauf gehend geschult werden, um das Risikobewusstsein zu schärfen. Dazu sollten klare Zuständigkeiten und Verantwortlichkeiten geklärt werden (z.B. Wer schaltet am Abend die Alarmanlage an? Wer führt die Datensicherung durch?) Daraus abgeleitet sollte auch eine Vertreterregelung geschaffen werden, damit beispielsweise eine Datensicherung durchgeführt werden kann, wenn der Zuständige im Urlaub oder krank ist.

2. *Gebäudesicherung und Zutrittsregelung*
   Die IT-Systeme müssen nicht nur vor elementaren Bedrohungen (z.B. Feuer, Wasser, Hitze) geschützt werden sondern auch vor Einbruch und Diebstahl. Gerade elementare Bedrohungen werden immer wieder unterschätzt. Im Juli 2017 kam es in Berlin und Umgebung immer wieder zu Starkregen. Wasser lief in Keller oder tieferliegende Gebäudeteile und hinterließ oft nicht nur Schäden am Gebäude, sondern auch an den IT Systemen (Serverraum) oder an der Verkabelung.[4] Dementsprechend sollten die IT Systeme vor äußeren Einflüssen geschützt werden. Vor Einbruch oder Diebstahl muss mit technischen und organisatorischen Maßnahmen geschützt werden.

3. *Sicherung der Daten, Sichere Nutzung der IT-Geräte und des IT-Systems*
   Die neue EU-Datenschutzgrundverordnung und die damit begleitenden vorbeugenden Maßnahmen stellen Unternehmen vor eine besondere Herausforderung. Mit der neuen europäischen Grundverordnung müssen Unternehmen mehr Maßnahmen zum Thema Datenschutz ergreifen und sind bis zum 25.05.2018 gefordert, die erforderlichen Maßnahmen umzusetzen. Verstöße oder die Nichteinhaltung der Meldefristen können mitunter zu hohen Strafen führen.
   Nach einer Studie von Veritas sind gerade einmal 2% der Unternehmen auf die neue Verordnung vorbereitet.[5] Dabei sind Unternehmen dazu verpflichtet, die Daten Dritter zu sichern und zu schützen. Eigene sensible und vertrauliche Daten sind zu schützen und die Datenweitergabe (Stichwort: Auftragsdatenverarbeitung) ist zu regeln. Ist eine Sicherheitslücke im Unternehmen bekannt geworden oder wurden beispielsweise personenbezogene Daten ihrer Kunden und Mitarbeiter gestohlen, sind Unternehmen einer gesetzlichen Meldepflicht unterworfen. Dazu benötigt es kurze und effektive Reaktionen auf Vorfälle. Mit Hilfe von Inventarlisten für Hard- und Software können weitere Maßnahmen ergriffen werden. Dazu sollten IT-Systeme regelmäßig auf ihren ordnungsgemäßen Zustand überprüft werden. Defekte Geräte oder defekte Datenträger sollten gründlich gelöscht bzw. entsorgt

werden. Ein besonderes Augenmerk sollte vor allem auf die IT Systeme gelegt werden, die einen besonderen Schutz benötigen (Personaldaten, Kundendaten, Zahlungssysteme, Buchhaltungssystem etc.). Verhaltensregeln gehören ebenfalls zu den vorbeugenden Maßnahmen. Verlässt beispielsweise ein Mitarbeiter den Computerarbeitsplatz, sollte dieser vor unberechtigten Zugriff gesichert werden.

4. *Sicherung von IT-Netzen, IT-Systemen und Anwendungen*
   Schutz vor äußeren Cyberbedrohungen bieten nur gepatchte und aktuell gehaltene Systeme. In diesem Sektor helfen besonders technische Systeme zur Sicherung. Mit Hilfe einer Installations- und Systemdokumentation können zielgerichtet Wartungen an den Systemen durchführt werden. Informationen dazu bietet das Bundesamt für Sicherheit in der Informationstechnik. Ein Informationsdienst informiert Bürger und vor allem kleine Unternehmen vor Sicherheitslücken und aktuellen Bedrohungen.[6] Diese Aufgaben werden von Unternehmen meist an IT-Dienstleistungsunternehmen übertragen. Jedoch sollten Wartungsvorgänge nur bei Bedarf erfolgen, da diese meist über Fernwartungssysteme erfolgen. Auch wenn es komfortabler und einfacher ist, stellt dies keine sichere Lösung dar. Mit Hilfe von Virenschutzprogrammen, Firewalls, getrennten Netzwerkbereichen (auch WLAN-Bereiche in internes und Gäste-Netz trennen), regelmäßigen Updates, Deaktivieren von nicht benötigten Programmteilen oder Funktionen, Änderung von vordefinierten Passwörtern sind die meisten technischen Basismaßnahmen abgedeckt.

5. *Sicherheitsmanagement*
   Ist ein Sicherheitsproblem erst einmal eingetreten, ist der Weiterbetrieb gefährdet und birgt daher auch ein hohes finanzielles Risiko. Sämtliche Fixkosten fallen weiterhin an. Ggf. hat ein Ausfall von bestimmten IT-Systemen Auswirkungen auf die Zusammenarbeit mit Partnern. Auch könnten Kunden nicht mehr bedient werden. Dazu sollten IT-Sicherheitsziele für alle Bereiche festgelegt werden sowie die Umsetzung der Maßnahmen fest eingeplant werden. Jedoch sind IT-

Systeme nicht zu 100% sicher, egal wie gut die Maßnahmen sind. Dazu kann ein Notfallplan Abhilfe schaffen. Das Deutsche Handwerksblatt berichtet in einem Beitrag zur Vorsorge für den Notfall. Wenn der Betriebsleiter einmal ausfällt, müssen viele Dinge von anderen Personen im Unternehmen geregelt werden, damit der Betrieb weiterläuft.[7] Dieser Plan identifiziert kritische Geschäftsprozesse, gibt Aufschluss darüber, welche Maßnahmen ergriffen werden müssen, wer der richtige Ansprechpartner ist und informiert darüber wie schnell der Normalbetrieb wiederaufgenommen werden könnte.
Die Daten eines Unternehmens in papierreiner oder digitaler Form sind das wichtigste Gut für das Bestehen eines Unternehmens. Die Daten entsprechend zu sichern und die Sicherungen auf ihre Funktionstüchtigkeit zu prüfen, ist daher unabdingbar. Ein entsprechendes Datensicherungskonzept enthält zudem in welchem Rhythmus die Sicherung durchgeführt und verschlüsselt werden muss und wo und wie lange diese aufzubewahren ist. Dazu ist ein Unternehmen gesetzlich verpflichtet.[8]

6. *Weitere Dienste*
Fast jedes Unternehmen unterhält zudem eine Website oder einen Social-Media-Kanal. Diese Bereiche sind ebenso beliebte Ziele für Angriffe. Nichts ist schädlicher, als wenn der Ruf eines Unternehmens oder die der geschäftsführenden Personen geschädigt wird. Diese Bereiche sind nicht nur gegen äußeren Einfluss zu schützen, sondern auch rechtlich abzusichern. Neben dem Urheberrecht, gehören Nutzungsbedingungen, Haftungsausschlüsse sowie Löschstrategien für unerwünschten Inhalt zu den Maßnahmen. Dazu gehören auch die privaten Kanäle der geschäftsführenden Personen. Identitätsdiebstahl ist aber nicht nur für das Geschäft schädigend, sondern auch für das private Umfeld. Nach einer Studie von PWC war 2016 bereits jeder Dritte davon betroffen.[9]

13.4 Wahl eines IT-Dienstleisters

Den richtigen IT-Dienstleister zu wählen, gestaltet sich schwierig. Zu einem benötigt es keine besonderen Anforderungen sich als IT-Dienstleister selbstständig zu machen. Jedoch können einige Aspekte Aufschluss über die Kompetenz des IT-Dienstleisters bieten.

Neben der Ausbildung des IT-Dienstleisters zählen auch Zertifikate und Weiterbildungsmaßnahmen zu den Auswahlkriterien. Unerlässlich ist zudem der Ruf eines IT-Dienstleisters über Referenzen oder Empfehlungen von Bekannten. Ebenso sollte auf den Kundenkreis des Dienstleisters geachtet werden, bzw. auf Transparenz geachtet werden, welche weiteren Kunden und Branchen dieser bedient. Die Industrie und Handelskammer unterhält zudem eine Webseite mit einem Kriterienkatalog,[10] der für die Auswahl eines vertrauenswürdigen Dienstleisters geeignet ist. IT-Dienstleister können den Katalog ebenfalls nutzen um Aufschlüsse über die Bedürfnisse und bevorstehenden Aufgaben bekommen zu können.

13.5 Fazit

Mit einigen Maßnahmen kann ein Basis-Schutz für Unternehmen hergestellt werden. Dazu können Unternehmen mit einem Notfallhandbuch im Schadensfall besser und effektiver reagieren. Neben den organisatorischen Maßnahmen, die innerbetrieblich umzusetzen sind, benötigen Kleine und Mittlere Unternehmen die Unterstützung von Dienstleistungsunternehmen, welche die technischen Maßnahmen im Unternehmen umsetzen. Viele Maßnahmen erzeugen am Anfang zwar einen hohen Aufwand, müssen aber in Folge nur noch mit geringem Aufwand gepflegt werden. Die Einsparpotentiale liegen zum einen bei der erfolgreichen Angriffsabwehr oder zum anderen darin, dass ein Unternehmen erst gar nicht von Viren und Malware befallen werden kann.

Lessons Learned

- Ein Notfallkonzept bedeutet zunächst Aufwand, kann aber viele Kosten bei Eintritt eines Notfalls (z.B. Ausfall Mitarbeiter, Hackerangriff, Feuer, Diebstahl) sparen oder gar den Fortbestand des Unternehmens retten.
- Mit wenigen Maßnahmen kann ein Basis-Schutz hergestellt werden.
- Die Auswahl des richtigen IT-Dienstleisters ist essentiell.

---

[1] Capgemini. (2017). Die Top-Technologien des Jahres. Aufgerufen am 21. 08 2017. Verfügbar unter: http://mc.capgemini.de/magazin/it-trends/it-top-themen.

[2] Fraunhofer Academy (2017). Lernlabor Cybersicherheit. Aufgerufen am 16.10.2017. Verfügbar unter: https://www.academy.fraunhofer.de/de/weiterbildung/informationkommunikation/cybersicherheit.html.

[3] Maier, F. (2017). Diese Mitarbeiter gefährden Ihre Sicherheit. Aufgerufen am 21.08.2017. Verfügbar unter: von https://www.computerwoche.de/a/diese-mitarbeitergefaehrden-ihre-sicherheit,3330382,3.

[4] MAZ-Online. (2017). Kreisbehörde steht unter Wasser. Aufgerufen am 21. 08 2017. Verfügbar unter: http://www.maz-online.de/Lokales/Oberhavel/Kreisbehoerde-steht-unter-Wasser.

[5] Diedrich, O. (2017). Studie: Unternehmen glauben nur, auf neuen Datenschutz vorbereitet zu sein. Aufgerufen am 21. 08 2017. Verfügbar unter: https://www.heise.de/ix/meldung/Studie-Unternehmen-glauben-nur-auf-neuen-Datenschutz-vorbereitet-zu-sein-3784634.html.

[6] Bundesamt für Sicherheit in der Informationstechnik (2017). Bürger-CERT (Computer Emergency Response Team). Aufgerufen am 16.10.2017. Verfügbar unter: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Buerger-CERT/Buerger-CERT_node.html.

[7] Freund, K. (2017). Vorsorgen für den Notfall. Deutsches Handwerksblatt, S. 44-45.

[8] Vgl. § 254 Bürgerliches Gesetzbuch.

[9] PwC. (2016). Identitätsklau - die Gefahr aus dem Netz. Aufgerufen am 21. 08 2017. Verfügbar unter: https://www.pwc.de/de/handel-und-konsumguter/assets/cybersecurity-identitaetsdiebstahl-2016.pdf.

[10] Industrie- und Handelskammer (2017). Mit Sicherheit die richtige Wahl. Aufgerufen am 16.10.2017. Verfügbar unter: https://www.ihk.de/unternehmen.

14. Schutzbedarfsanalyse für nachhaltiges Unternehmertum

Matthias Hartmann, Leonhard Gebhardt; HTW Berlin

Abstract

In diesem Artikel werden die drei Dimensionen der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) als Voraussetzung für nachhaltiges Unternehmertum vorgestellt. Die Schutzbedarfsanalyse ist Grundlage für die Feststellung des Ist-Zustands, die durch Maßnahmen und Reaktionsleitfäden komplementiert werden muss.

14.1 Nachhaltigkeit bedarf der IT-Sicherheit

Im Englischen wird nachhaltiges Unternehmertum als Sustainable Entrepreneurship bezeichnet und ist unter dieser Bezeichnung auch im deutschsprachigen Raum bekannt geworden. Der Gedanke der Nachhaltigkeit stammt grundsätzlich aus der Forstwirtschaft.[1] Letztlich ist dieser Gedanke auch auf den Fortbestand eines Unternehmens erweiterbar. In diesem Sinne ist Nachhaltigkeit aus systemtheoretischer Perspektive das effiziente Wirtschaften über ein Zeitkontinuum bei gleichzeitiger Vermeidung eines nicht-zielkonformen Inputs bzw. eines nicht-zielfonformen Outputs. Auf IT-Sicherheit bezogen bedeutet dies z.B., dass keine Malware in die IT-Infrastruktur eines Unternehmens gelangen darf.

Die Schutzziele der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) sind somit wesentliche Bedingungen eines nachhaltigen Unternehmertums bzw. Managements. Die Verletzung der Schutzziele kann bis zur Liquidation eines Unternehmens führen: Die Handelskette Target Canada Co. (133 Geschäfte, 17.600 Mitarbeiter) wurde von Hackern angegriffen, in dessen Verlauf Datensätze (Kredit- und Bankkarten) von mehreren Millionen Kunden erbeutet wurden. Der Vertrauensverlust endete in einem Umsatzsturz, der das Unternehmen 2015 letztlich in die Insolvenz führte.[2]

14.2 Verfügbarkeit, Integrität und Vertraulichkeit

Grundsätzlich gibt es drei Schutzziele der IT-Sicherheit:[3]

Verfügbarkeit bezieht sich sowohl auf funktionierende Systeme als auch den legitimen (digitalen) Zugriff auf Informationen oder Daten.

Integrität bedeutet Vollständigkeit und Unveränderlichkeit von Daten. Letzteres beinhaltet auch, dass Informationen nicht nachträglich manipuliert werden.

Vertraulichkeit beschreibt den Schutz vor unzulässiger Weitergabe oder Veröffentlichung von Informationen. Dritte dürfen ohne Autorisierung keinen Zugang zu vertraulichen Daten haben.

14.3 Schutzbedarfsanalyse

Insbesondere die Führungskräfte aber auch die Mitarbeiter der Unternehmen sind herausgefordert, die drei oben genannten Schutzziele zu gewährleisten. Zu diesem Zweck werden mögliche Risiken betrachtet. Konkret sollten Führungskräfte und Mitarbeiter alle Eventualitäten aufschreiben, die für das Unternehmen in Betracht kommen könnten, um diese dann zu bewerten und letztlich mögliche Antworten zu entwickeln. Hierzu gibt es auch Standards mit Empfehlungen wie z.B. vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

Im Prinzip ist die Vorgehensweise sehr einfach:

Im ersten Schritt werden die Schadenspotenziale aufgeschrieben, die die IT des Unternehmens beeinflussen könnten. Hier wird es eine hohe Vielfalt an unterschiedlichsten Themen geben: Krankheit des einzigen Administrators, Wassereinbruch bei Dauerregen im Serverraum, Verlust eines Laptops des Firmenchefs, Befall mit Schadsoftware usw.

Im zweiten Schritt wird die Eintrittswahrscheinlichkeit der Schadenspotenziale eingeschätzt. Das kann vereinfachend auch in fünf Wahrscheinlichkeitsstufen erfolgen.

1 = Das Ereignis wird nie eintreten
2 = Das Ereignis wird selten eintreten

3 = Das Ereignis wird manchmal eintreten
4 = Das Ereignis wird oft, aber unregelmäßig eintreten
5 = Das Ereignis wird regelmäßig eintreten

Wirtschaftsprüfer und größere Unternehmen versuchen sich zeitweise an einer vordergründig exakten Ermittlung der Eintrittswahrscheinlichkeiten in Prozentzahlen, was regelmäßig zu intensiven, aber nutzlosen Diskussionen in der Geschäftsführung oder dem Vorstand führt.[4] Eine komparative (vergleichende) Messung ist in diesem Fall einer metrisierenden (vordergründig exakten) Messung vorzuziehen. Beispiele können sein:

- Es ist als sicher (Stufe 3) anzunehmen, dass der einzige Administrator manchmal krank werden wird und nicht zur Verfügung steht.
- Es wird angenommen, dass der Serverraum durch Dauerregen wahrscheinlich nicht überflutet wird (Stufe 2). Anmerkung: Bitte darauf achten, dass gegebenenfalls Wasserleitungen in der Wand des Serverraums verlegt sind oder sich der Serverraum neben der Toilette oder einem Waschraum befindet.
- Es wird angenommen, dass der Verlust des Laptops des Firmenchefs selten eintreten wird (Stufe 2)
- Es wird angenommen, dass der Befall mit Schadsoftware sicher eintreten wird (Stufe 5).

Im dritten Schritt wird der mögliche Schadensumfang beschrieben:

- In diesem Sinne kann es sein, dass bei Krankheit des einzigen Administrators der Betrieb stillsteht. Je nach Art des Unternehmens kann dies nun lebensbedrohlich für das Unternehmen sein (z.B. als Steuerberater) oder als Nebeneffekt gewertet werden (z.B. bei einem Bauunternehmen mit 5 Mitarbeitern).
- Der Wassereinbruch in einem Serverraum kann im gleichen Sinne lebensbedrohlich oder ein Nebeneffekt sein.
- Der Verlust des Laptops des Firmenchefs kann bedeuten, dass Erpressungsgeld gezahlt werden muss oder ein Konkurrent nun über die firmeninternen Daten und Geheimnisse verfügt. Damit kann das Geschäft bedroht sein, muss es aber nicht.

- Beim Befall der IT-Infrastruktur mit Schadsoftware kann das Ereignis ebenfalls unterschiedliche Auswirkungen haben (Datenverlust, Erpressung, …)

14.4 (Sofort-)Maßnahmen und Reaktionsleitfäden

Im Anschluss an die Schutzbedarfsanalyse werden Handlungsstrategien entwickelt. Hier lassen sich (Sofort-)Maßnahmen von Reaktionsplänen unterscheiden. Maßnahmen könnten sein:

- Im Falle des einzigen Administrators wird mittelfristig entweder ein zweiter Mitarbeiter geschult oder die Aufgabe an einen externen Dienstleister vergeben.
- Beim möglichen Wassereinbruch wird ab sofort regelmäßig ein Backup gezogen bzw. in kürzeren Abständen gezogen. Das Backup wird nicht im gleichen Raum aufgehoben.
- Die Festplatte des Laptops wird sofort verschlüsselt und auch davon regelmäßig ein Backup gezogen
- Gegen die Schadsoftware wird mit einem IT-Dienstleister untersucht, inwieweit die bis dato eingesetzte Antivirensoftware bzw. die Firewall ausreichend ist.

Die Erstellung von Reaktionsleitfäden erfolgt anhand von „Wenn – dann"-Sätzen:

- Wenn der Administrator ausfällt, dann übernimmt der ebenfalls geschulte Mitarbeiter diese Arbeit.
- Wenn es zu einem Wassereinbruch in einem Serverraum kommt, dann wird der Serverraum vorsichtig getrocknet (Dazu gibt es Empfehlungen). Nach Trocknung wird die Funktionsfähigkeit geprüft. Wenn die Hardware beschädigt ist, wird neu beschafft und das Backup eingespielt.
- Wenn der Laptop verloren geht, dann wird eine Verlustmeldung und/oder eine Anzeige erstattet und der Laptop ersetzt und das Backup eingespielt.
- Bei Befall der Rechner mit Schadsoftware wird die Arbeit mit den Rechnern sofort eingestellt und ein Experte hinzugezogen.

Die genannten Beispiele sind vereinfachend dargestellt und sollten eine Hilfestellung zum Nachdenken über den eigenen Betrieb bieten.

Lessons Learned

- Für nachhaltig orientierte Unternehmen ist die Beachtung der IT-Sicherheit existenzsichernd.
- Vertraulichkeit, Integrität und Verfügbarkeit sind die Schutzziele der IT-Sicherheit.
- Es empfiehlt sich die Durchführung einer Schutzbedarfsanalyse sowie die Umsetzung von Sofortmaßnahmen und die Erstellung von Reaktionsleitfäden.

---

[1] Vgl. Fischer, Klaus (2017). Corporate Sustainability Governance. Nachhaltigkeitsbezogene Steuerung von Unternehmen in einer globalisierten Welt. Springer Fachmedien Wiesbaden GmbH, S. 70ff.

[2] Sokolov, D. AJ (2015). Ein Jahr nach Datenleck: Target Kanada ist Pleite. Heise Online-Artikel, zu finden unter: https://www.heise.de/tp/features/Ein-Jahr-nach-Datenleck-Target-Kanada-ist-Pleite-3370093.html, aufgerufen am 17.10.2017.

[3] Für manche Autoren, wie z.B. Gadatsch und Mangiapane (2017) gehören neben den drei etablierten Dimensionen (siehe BSI-Standard 200-2) auch die „Datenexistenz" und die „Verbindlichkeit" von Kommunikation bzw. von ausgetauschten Informationen (S. 22) dazu. Die Autoren weisen insbesondere auf die Bedeutung für den E-Commerce Bereich hin. Nach Ansicht der Autoren ist die Dimension der Datenexistenz bereits eingeschlossen in den beiden Dimension „Verfügbarkeit" und „Integrität". Die Dimensionen werden erklärt nach Gadatsch und Mangiapane (2017). IT-Sicherheit. Digitalisierung der Geschäftsprozesse und Informationssicherheit. Wiesbaden: Springer Vieweg, S. 17–21.

[4] Vgl. Hartmann, M. und Halecker, B. (2017). Pragmatische Cyber Security in Kritischen Infrastrukturen – zwei Fallbeispiele. In: Safety und Security - Mit Sicherheit gut vernetzt - Branchentreff der Berliner und Brandenburger Wissenschaft und Industrie. Hrsg. Pinnow, C. und Schäfer, S., Beuth Verlag Berlin, Wien, Zürich.

Teil 4: Unterstützungsangebote für KMU und Handwerksbetriebe

15. EFRE Projekt „Digital Value" für Berliner Unternehmen

Matthias Hartmann, Stefan Wittenberg, Madlen Böer; HTW Berlin

Abstract

Die Herausforderungen der Digitalisierung sind besonders für kleine und mittelständische Unternehmen ohne eigene Entwicklungsabteilung oder Business Development schwieriger zu meistern. Die Hochschule für Technik und Wirtschaft unterschützt im Projekt Digital Value kleine und mittelständische Unternehmen im Berliner Raum und setzt konkrete Maßnahmen zur Digitalisierung um.

15.1 Die Hochschule für Technik und Wirtschaft Berlin (HTW Berlin)

Die Hochschule für Technik und Wirtschaft in Berlin wurde 1994 gegründet und ist mit beinahe 14.000 Studierenden die größte Hochschule für angewandte Wissenschaften im Osten Deutschlands, damit liegt die Hochschule im Vergleich der Fachhochschulen bundesweit auf Rang 12.[1] Das Angebot für Studierende ist mit 70 Studiengängen umfangreich und vielfältig. Studierende schätzen besonders die praxisorientierte Ausrichtung in den Lehrveranstaltungen. ProfessorenInnen und Lehrbeauftragte weisen an der HTW Berlin mindestens fünf Jahre Praxiserfahrung auf. Kontinuierliche Projekte mit Unternehmen sind ein Teil der Lehrveranstaltungen.

15.1.1 Top Rankings für die Lehre

Bundesweite Hochschulrankings bewerten die Studiengänge mit Platz 3-5 für Betriebswirtschaftslehre, Platz 2-6 Informatik, Platz 2-5 Wirtschaftsinformatik und Platz 2-5 Wirtschaftsingenieurwesen.[2] Die französische Personalberatung

Emerging und die trendence Institut GmbH haben für das University Employability Ranking weltweit Arbeitgeber befragt, wie gut Absolventen auf den Arbeitsmarkt vorbereitet sind. Hier konnte die HTW Berlin den 11. Platz von allen Universitäten und Fachhochschulen in Deutschland 2016 erreichen.[3] Diese Top-Platzierung ist aufgrund des Praxisbezugs besonders wertvoll und kennzeichnet die Absolventen mit einer herausragenden Vorbereitung auf den Berufseinstieg nach Abschluss des Studiums. Das Centrum für Hochschulentwicklung bewertet mehr als 300 Hochschulen im CHE Ranking für Studienbedingungen. Für den Fachbereich „Wirtschafts- und Rechtswissenschaften" an der HTW Berlin gab es Top-Platzierungen in der Spitzengruppe für die Qualität der Angebote zum Studieneinstieg und für das Studienergebnis in Bezug auf den Abschluss des Studiums in der Regelstudienzeit für die Bachelor und Masterstudiengänge.[4]

15.1.2 Hohe Forschungsintensität

Die HTW Berlin identifiziert die Forschung als wichtigen Erfolgsfaktor und kann mit Innovationen, Expertisen und wissenschaftlichen Netzwerken Entwicklungspotentiale nutzen und Projekte umsetzen. Bis zu jährlich 160 Drittmittelvorhaben bearbeiten Themen wie „Industrie von morgen", „Digitalisierung" und „Kreativwirtschaft". Der Wissenstransfer zwischen der Wissenschaft und der Praxis wird im HTW Berlin eigenen „Kooperationszentrum Wissenschaft-Praxis" gelebt. Im besonderen Maße profitieren kleine und mittelständische Unternehmen vom Zugang zu Wissensressourcen und von interdisziplinären Forschungsteams.

Neben Praxisbezug und Forschergeist hat die HTW Berlin eine ausgezeichnete internationale Beziehung zu über 140 Partnerunternehmen weltweit. Somit profitieren Studierende von einer umfassende Fremdsprachenausbildung, englischsprachiges Studienangebot und geförderten Auslandssemester.

15.2 Kooperationsforschungsprojekt „Digital Value"

Im Rahmen eines vom Europäischen Fonds für regionale Entwicklung (EFRE) geförderten Projektes mit der Bezeichnung „Digital Value" werden Unternehmen auf den Cyber- und Informationsraum trainiert und bei der Digitalisierung und der digitalen Absicherung unterstützt. Das Projekt mit dreijähriger

Laufzeit endet am 30.06.2019 und ist mit insgesamt 2 Millionen Euro von der EU und der HTW Berlin kofinanziert.

Im Projekt gilt es die Leitfrage zu klären, wie sich die Digitalisierung auf die bestehenden Wertschöpfungsketten auswirkt und wie die Digitalisierung zur Optimierung dieser genutzt werden kann. Das Ziel des Projektes besteht darin, eine Know-how Plattform zu etablieren sowie ein Diskussionsforum für die Berliner kleinen und mittelständischen Unternehmen und Start-ups zu schaffen. Das Projekt wird von der Hochschule für Technik und Wirtschaft Berlin durchgeführt. Projektleiter ist Prof. Dr. Matthias Hartmann.

Das Digital Value Anwendungszentrum strukturiert sich in drei Teilprojekte: (1) Digital Business Lab, (2) Lean Management und (3) Mobile Business Lab, die im Folgend kurz vorgestellt werden.

15.2.1 Digital Business Lab

Im Teilprojekt „Digital Business Lab" haben Unternehmen die Möglichkeit, in einem Informationsgespräch (Digital Welcome) das Geschäftsmodell ihres Unternehmens und digitale Handlungsbedarfe darzustellen und zu diskutieren. In einem zweiten Schritt (Digital Workshop) wird ein digitales Konzept für ein ausgewähltes Problem erarbeitet. Im dritten Schritt (Digital Pilot) wird eine digitale Referenzlösung geschaffen, um dem Unternehmen ein plastisches Lösungsbeispiel zu geben. Sollte das Unternehmen an einer Umsetzung interessiert sein, lassen sich weitere Forschungsprojekte aufsetzen.

15.2.2 Lean Factory Lab

Das Lean-Management-Labor ist dreigeteilt, bestehend aus drei Laborbereichen: Lean-Production-Management, Lean-Office-Management und Industrie 4.0. Es bildet zukünftige Arbeitswelten im Sinne einer Mini-Fabrik, eines Verwaltungsbereiches und eines Entwicklungs- und Prozessoptimierungsbereiches ab und ermöglicht die Durchführung von Projektarbeiten und realen Fallstudien mit dem Ziel Unternehmen und Studierende im sicheren Umgang mit digital vernetzten Menschen, Werkzeugen, Handlinggeräten und Maschinen zu trainieren. Alle drei Laborbereiche verwenden eine Vielzahl von IT-Anwen-

dungssystemen von Enterprise Ressource Planning (ERP), Manufacturing Execution System (MES) und Business Intelligence (BI)-Systemen, über Roboter, Fertigungs- und Automatisierungssteuerungen bis hin zu 3D-Visualisierungen und 3D-Druckern. Hierbei sind diverse IT-Sicherheitssysteme im Einsatz, um die Datensicherheit und den Datenschutz zu gewährleisten.

Der Bereich Lean-Production-Management-Training ist in zwei Teilbereiche aufgeteilt. Er besteht aus einer teilautomatisierten Fertigungsanlage des Unternehmens Festo Didactic mit Hochregallager, manueller Montagestation, automatischem Kameraprüfplatz, automatischer Montagestation und manueller Pressstation und ist angebunden an ein MES. Anhand der Anlage können automatisierte Produktionsprozesse und Lagerhaltung mittels einer MES Steuerung programmiert werden.

Der Bereich Lean-Office-Management dient zum Training von Verwaltungsprozessen, insbesondere unter dem Schwerpunkt Supply Chain Management. In diesem Bereich kommen ERP- und BI-IT-Systeme zum Einsatz, hier sind die Abläufe entlang der Wertschöpfungs- und Lieferkette unter realen Bedingungen erfahrbar.

Die Industrie 4.0-Lernfabrik demonstriert die Selbststeuerung von Objekten, Datenanalyse und Prozessoptimierungen. In dem Bereich kommt ein fahrerloses Transportsystem, ein kollaborativer Roboter, ein 3D- Drucker, sowie Augmented und Virtual Reality Technologie zum Einsatz. Es wird an einer Factory Cloud Lösung gearbeitet, die die einzelnen Internet of Things (IoT) Geräte mittels programmierter Schnittstellen in Echtzeit miteinander verknüpft. Parallel dazu entsteht eine digitale Fabrik inklusive einer passenden IT-Infrastruktur, die auf die realen Prozesse, Schnittstellen und Geräte übertragbar ist und so eine schnellere und risikoärmere Umsetzung der Arbeitsabläufe an den realen Geräten ermöglicht.

15.2.3 Mobile Business Lab

Das Mobile-Business-Lab befasst sich mit einer mobilen vor-Ort-Analyse digitaler Prozesse, deren Optimierung, sowie die Identifikation von digitalisierbaren Prozessen, die derzeit noch als gänzlich nicht-digitale, oder bereits in Tei-

len digitalisierte Prozesse im Unternehmen abgebildet sind. Neben den vielfältigen Aspekten der komplexen digitalen Wertschöpfung, finden Faktoren wie Sicherheit, Integrität und Konvergenz ihre Berücksichtigung. Zudem besitzen die Mitarbeiter im Mobile Business Lab eine große Expertise hinsichtlich der Nutzung von innovativen digitalen Technologien – wie z.B. Augmented Reality, Virtual Reality und Wearables – zur Abbildung und Digitalisierung von Geschäfts- und Produktionsprozessen. Das Mobile Business Lab berät auch in diesem Kontext KMU und Handwerksbetriebe zur Projekt- und FuE-Kooperationsentwicklung.

15.3 Vorgehensweise im Digital Business Lab

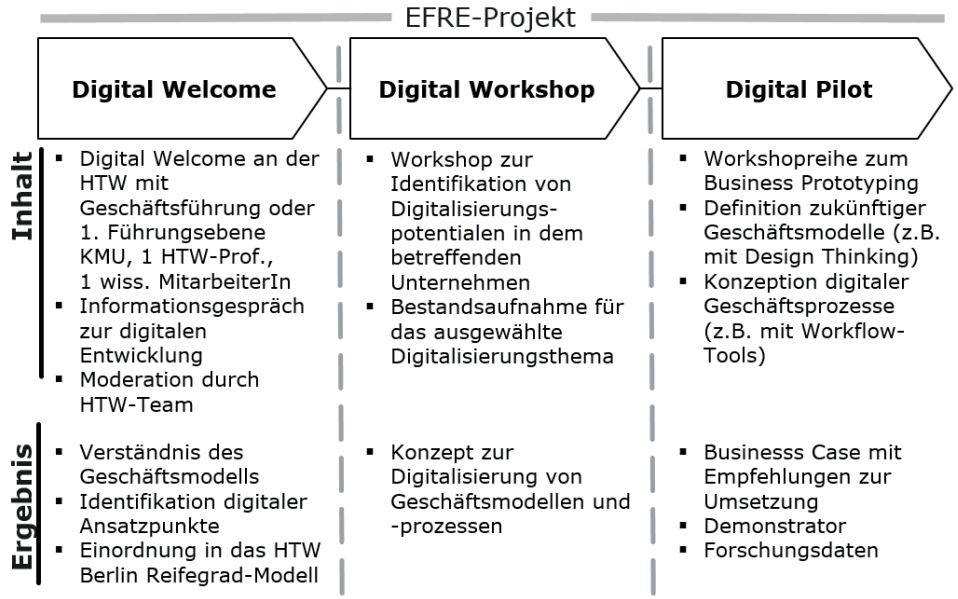

Abbildung 18: Phasen im Projekt Digital Value Anwendungszentrum, eigene Darstellung.

Das erste Gespräch zwischen der Geschäftsführung oder der ersten Führungsebene des Unternehmens nennt sich „Digital Welcome" und ist die erste Phase in diesem Teilprojekt. Daraus ergibt sich ein Verständnis des Geschäftsmodells in Form des Business Model Canvas, die Einschätzung des

digitalen Reifegrades nach dem HTW-Reifegradmodell sowie die Identifikation der digitalen Ansatzpunkte im Unternehmen.

Möchte das Unternehmen nach dem ersten Gespräch weiter an den digitalen Aufgabenstellungen arbeiten, folgt die Phase „Digital Workshop“. In dieser Phase arbeiten das HTW-Projektteam und Spezialisten aus dem Unternehmen an einer konkreten Aufgabenstellung und erstellen gemeinsam ein Konzept zur Digitalisierung des Geschäftsmodells.

Der „Digital Pilot“ als anschließende Phase ist individuell auf die digitalen Bedürfnisse des Unternehmens angepasst. Hier entstehen im Ergebnis konkrete Empfehlungen für Geschäftsmodell und Business Cases zur digitalen Transformation sowie Demonstratoren und Prototypen. Das weite Spektrum reicht von Apps für die Produktionsüberwachung bis zu Social Media Kampagnen. Das Projekt mit einem Unternehmen endet mit erfolgreicher Übergabe in einer Abschlusspräsentation.

15.4 Zwischenergebnisse des Projektes bis September 2017

15.4.1 Business Model Canvas für 50 Unternehmen

Bis September 2017 hat das Projektteam des Digital Business Anwendungszentrum mit 50 Unternehmen ein Informationsgespräch (Digital Welcome) geführt und umfassend über das Thema Digitalisierung diskutiert. Für diese Unternehmen ist das Geschäftsmodell nach dem Business Model Canvas (Abbildung 19) erfasst. Das Modell stellt das Leistungsversprechen des Unternehmens dem Kunden gegenüber in das Zentrum. Auf der rechten Seite der Darstellung sind Kundensegmente erfasst, sowie Kundenbeziehungen und Kommunikationskanäle für die Kundenansprache dargestellt. Die linke Seite des Modells fasst zusammen, wie das Leistungsversprechen dem Kunden gegenüber realisiert wird, mit welchen Partnern das Unternehmen kooperiert, welche Aktivitäten des Unternehmens für die Wertschöpfung relevant sind und auf welche Ressourcen das Unternehmen zurückgreift.[5]

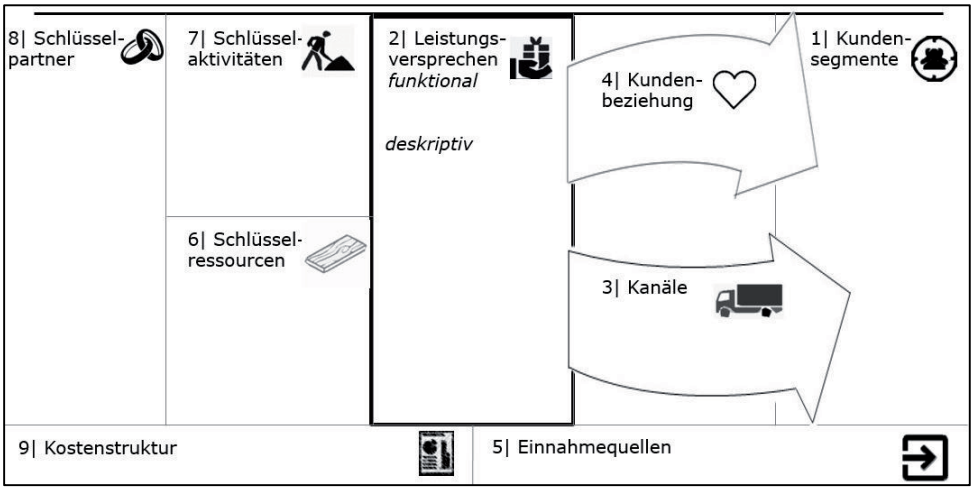

Abbildung 19: Business Model Canvas, in Anlehnung an Osterwalder, Pigneur (2010).

15.4.2 Feststellung des digitalen Reifegrades für 50 Unternehmen

Die am Projekt beteiligten KMU unterscheiden sich branchenspezifisch deutlich hinsichtlich des Fortschrittes der umgesetzten Digitalisierungsvorhaben: Zulieferer der Automobilindustrie tauschen bereits seit rund 40 Jahren über den Datenaustauschstandard EDI Geschäftsdokumente elektronisch mit Ihren Geschäftspartnern in der Supply Chain aus und haben Papierdokumente digitalisiert: Bei Unterschreiten eines Sicherheitsbeststandes bei einem Automobilhersteller wird automatisiert und ohne manuellen Eingriff ein Bestellabruf beim Zulieferer platziert. Der Zulieferer kann wiederum die Bestellabrufe automatisiert in einen Fertigungsauftrag im eigenen Enterprise-Resource-Planning-(ERP-)System umsetzen. In anderen Branchen – so etwa der Bauindustrie oder dem Handwerk wird in einer Vielzahl von Unternehmen die Auftragsabwicklung noch per Handzettel organisiert und der unternehmensübergreifende Datenaustausch ist noch in der Pilotierungsphase.[6]

Für den oben erwähnten Automobilzulieferer bietet sich auf Basis der bereits hochautomatisierten Prozesse zum Beispiel die Pilotierung eines cyber-physischen Systems an. Das Bauunternehmen ist mit einem derartigen Piloten vermutlich überfordert und zieht aus der Digitalisierung der Auftragsprozesse einen wesentlich größeren Nutzen.

Entscheidend für einen erfolgreichen Piloten im Rahmen des Projektes ist es daher, den digitalen Ist-Zustand zu erheben, um darauf aufbauend geeignete Maßnahmen zu entwickeln. Für die systematische Erfassung des digitalen Ist-Zustandes stehen in der Literatur eine Vielzahl von digitalen Reifegradmodellen bereit.

Die Modelle weisen in der Regel drei Bestandteile auf: Dimensionen mit Kriterien zur Digitalisierung, Reifegrade (Stufen) und Ausprägungen innerhalb der Dimensionen. Verschiedene Reifegrade ergeben sich dann aus dem Maß der Erfüllung der vorgegebenen Kriterien. Neben der Bewertung der technologischen Reife werden vielfach weitere Dimensionen wie Strategie, Führung, Produkte und Dienstleistungen, Organisation und Mitarbeiter herangezogen. Diese Modelle sind gut geeignet, um mit Unternehmensberatungen und Strategieabteilungen großer Konzerne eine umfassende Lagebeurteilung des eigenen Digitalisierungsfortschritts zu erstellen. Die Bewertung der Reifegrade sind oftmals schon eigene Projekte, in denen im Rahmen von Interviews mit Fach- und Führungskräften über mehrere Monate eine Analyse durchgeführt wird. Für die Diskussion mit den Vertretern der KMU sind die aufgeführten Modelle jedoch vielfach nicht praxistauglich, da im Unternehmen dafür keine Ressourcen bereitstehen. Weiterhin kennen die Inhaber der Unternehmen den Zustand Ihres Unternehmens oftmals bereits sehr gut und sind eher an einer Verbesserung des Status Quo interessiert.

Aus diesem Grund wurde ein KMU-taugliches Reifegradmodell entwickelt, das auf Basis von nur fünf Dimensionen eine einfache Selbsteinschätzung von Digital Basic bis hin zu Digital Disruption ermöglicht. Die ersten vier Reifegrade werden im Digital Welcome zur Bewertung der Reifegrade und Entwicklung von Maßnahmen der stufenweisen Verbesserung von einer Stufe zur nächsten genutzt. Der fünfte Reifegrad dient zur Diskussion möglicher disruptiver Auswirkungen von Technologien bzw. des Geschäftsmodells.

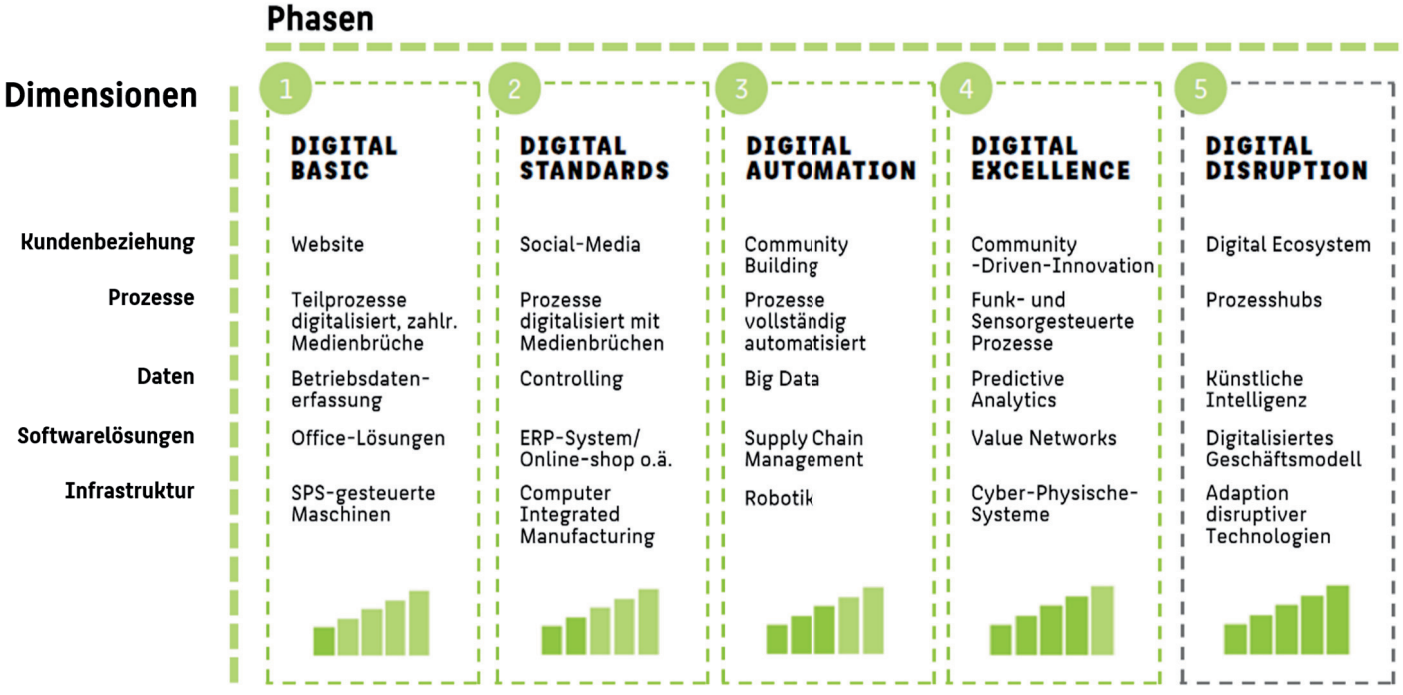

Abbildung 20: HTW Berlin Reifegrad-Modell, eigene Darstellung.

15.4.3 Identifikation digitaler Ansatzpunkte in den Unternehmen

Die Zusammenarbeit mit den Unternehmen zeigt, dass Digitalisierung für kleine und mittlere Unternehmen zum einen Teil die klassischen Themen der Informationstechnologie umfasst (z.B. ERP und DMS). Zum anderen Teil sind Projekte zur Mitarbeiter- und Kundengewinnung und -bindung nachgefragt (z.B. Social Media). Weniger nachgefragt werden die Erhebung, Auswertung und Nutzung komplexer Datenmengen über Big Data, Data Mining und Data Analytics. IT-Sicherheit bzw. Cyber-Sicherheit ist für viele Unternehmen kein Thema, das vordergründig auf der Agenda steht. Nach einer grundsätzlichen Sensibilisierung kann aber das Bewusstsein dafür geweckt werden.

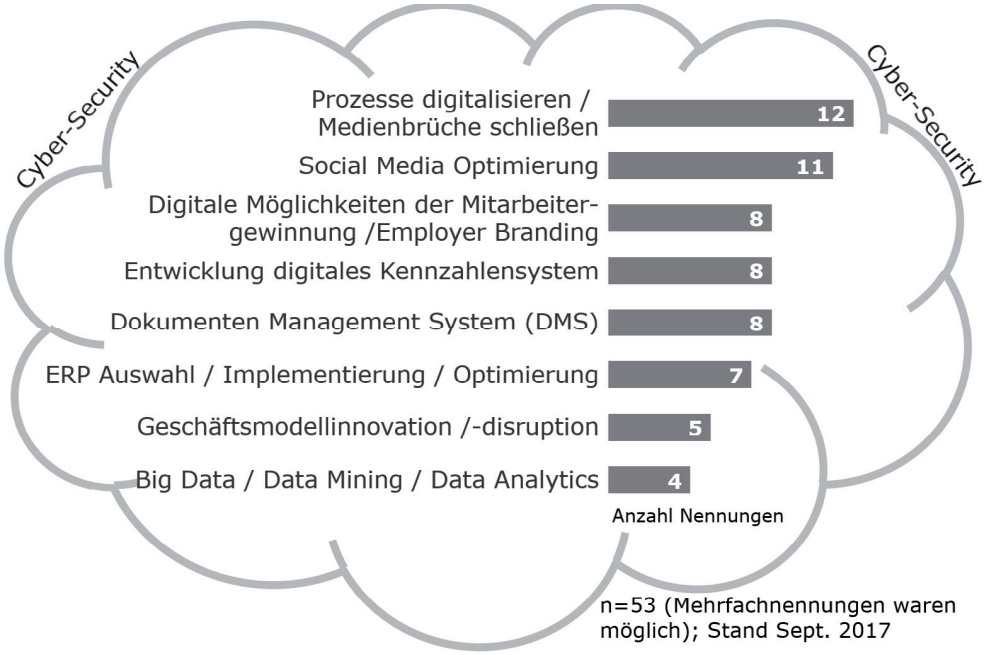

Abbildung 21: Identifikation digitaler Ansatzpunkte; eigene Darstellung.

15.5 Perspektive des Projektes „Digital Value"

Die Hälfte der Unternehmen will mit dem HTW-Team – Stand September 2017 – ein digitales Konzept oder einen digitalen Prototypen umsetzen. Die Umsetzung dieser Vorhaben hat mittelfristigen Charakter und geht über den Aufwand für Informationsgespräche zur Digitalisierung, die bei den Erstkontakten geführt werden, deutlich hinaus. So kann die Einführung von kompletten ERP- oder DMS-Systemen im Rahmen des Projektes nur qualitätssichernd begleitet werden, um in einem vertretbaren Ressourceneinsatz zu bleiben. Ziel des Digital Business Lab ist es, so vielen kleinen und mittleren Unternehmen wie möglich bei der Digitalisierung zu helfen.

Mithin wird das Jahr 2018 mit einer Reihe von neuen Informationsgesprächen zur Digitalisierung als auch mit einer Reihe mittelfristiger Umsetzungsprojekte zur Digitalisierung gefüllt sein. Daneben werden Präsentationen auf verschiedenen Unternehmerforen gehalten und ähnliche Tagungen wie zum Beispiel der 6. IT-Sicherheitstag Mittelstand 2017 veranstaltet, um eine möglichst große Breitenwirkung zu erzielen. Letztlich soll dadurch auch die Zusammenarbeit der anwendungsorientierten Hochschule für Technik und Wirtschaft (HTW) Berlin mit den Unternehmen beispielhaft gefördert werden. Es sind besonders die kleinen und mittleren Unternehmen, die durch die regionale Förderung noch wettbewerbsfähiger gemacht werden sollen.

Lessons Learned

- Mit dem Projekt „Digital Value" an der HTW Berlin existiert eine Plattform, die kleine und mittlere Unternehmen bei der Digitalisierung unterstützt.
- Die Zusammenarbeit mit den Unternehmen zeigt, dass Digitalisierung für kleine und mittlere Unternehmen zum einen Teil die klassischen Themen der Informationstechnologie umfasst (z.B. ERP und DMS). Zum anderen Teil sind Projekte zur Mitarbeiter- und Kundengewinnung und -bindung nachgefragt (z.B. Social Media).
- IT-Sicherheit ist für viele Unternehmen kein Thema, das vordergründig auf der Agenda steht. Nach einer grundsätzlichen Sensibilisierung kann aber das Bewusstsein dafür geweckt werden.

[1] Statistisches Bundesamt (2017). Bildung und Kultur. Studierende an Hochschulen –Vorbericht- Wintersemsester 2016/2017. Aufgerufen am 10.10.2017. Verfügbar unter: https://www.destatis.de/DE/Publikationen/Thematisch/BildungForschungKultur/Hochschulen/StudierendeHochschulenVorb2110410178004.pdf?__blob=publicationFile

[2] Jakob Blume (2016). Hochschulranking 2016. Das sind Deutschlands beste Unis. Aufgerufen am 10.10.2017. Verfügbar unter: http://www.wiwo.de/erfolg/campus-mba/hochschulranking-2016-das-sind-deutschlands-beste-unis/14719390-all.html.

[3] Emerging, trendence (2016). University Employability Ranking Deutschland 2016. Aufgerufen am 10.10.2017. Verfügbar unter: https://www.trendence.com/partner/hochschulen/university-employability-ranking.html.

[4] Centrum für Hochschulentwicklung (2017). CHE Ranking. Aufgerufen am 10.10.2017. Verfügbar unter: https://ranking.zeit.de/che/de/fachbereich/100018?ab=3.

[5] Osterwalder, Pigneur (2010).

[6] Vgl. Marcus Schreyer Beuth Pocket BIM - Einstieg kompakt für Bauunternehmer BIM-Methoden für die Bauausführung 1. Auflage 2016.

16. Digitales Handwerk in Ostbrandenburg

Henrik Klohs, Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg

Abstract

Im Zeitalter der Digitalisierung haben IT-Sicherheit, Datenschutz und -sicherheit eine hohe Bedeutung, auch der „Unsicherheitsfaktor MENSCH" ist in der IT-Hierarchie im Unternehmen nicht zu unterschätzen. Für Unternehmen im Handwerk muss ein stärkeres Bewusstsein für die Gefahren, die sich aus der täglichen Arbeit mit den neuen Informations- und Kommunikationstechnologien (IKT) und deren Vernetzung im Internet ergeben, geschaffen werden.

16.1 Einleitung

Die Vorteile der digitalen Informations- und Kommunikationstechnologien in Bezug auf eine erhöhte Arbeitseffizienz liegen auf der Hand. Gleichzeitig zeigen sich Handwerksunternehmen in Ostbrandenburg zunehmend besorgt über die erhöhte Anzahl von externen Angriffen auf die eigene IT-Infrastruktur. Beim Umgang mit den neuen Medien gilt es, strikte Regeln zu beachten, um sich gegenüber Cyberangriffen zu schützen, die eigenen Daten zu sichern, dem aktuellem Datenschutz zu entsprechen und die Sicherheit der eigenen IT-Infrastruktur zu gewährleisten.

16.2 Dienstleistungsangebot der Handwerkskammer

Die Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg bietet allen Handwerksunternehmen in der Region Ostbrandenburg einen umfassenden kostenfreien Service zum Thema „Digitales Handwerk". Eine besondere Zielstellung ist es, die Unternehmen dabei zu unterstützen, ihre Kompetenz auf dem Gebiet der IKT zu verbessern und ihre Geschäftsprozesse zu digitalisieren.

Von Informationsveranstaltungen und Workshops, über Weiterbildungsangebote bis hin zum individuellen Informationsgespräch unterstützt der BIT die

Mitgliedsbetriebe in Ostbrandenburg und beantwortet Fragen zur Digitalisierung von grundsätzlichem Verständnis bis hin zu Fördermöglichkeiten wie dem Brandenburgischen Innovationsgutschein Digital (BIG Digital).

Der BIT gibt folgende Unterstützung:

- beim Einsatz neuer Produktions- und Automatisierungstechnologien
- bei der Umsetzung der Digitalisierung interner Unternehmensprozesse
- bei der Organisation neuer digitaler Geschäftsmodellen und Prozesse
- bei der Umsetzung der Digitalisierung Ihrer IuK – Technik
- bei der Suche eines passenden IT-Dienstleisters

16.3 IT-Sicherheit im Handwerk

Der BIT der Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg wurde in mehreren Qualifizierungsmaßnahmen über das Projekt „IT-Sicherheit im Handwerk" (https://www.it-sicherheit-handwerk.de) auf dem Gebiet der IT-Sicherheit fit gemacht und ist als sogenannter IT-Sicherheitsbotschafter für das Handwerk ein wichtiger Ansprechpartner. Diese unterstützen u.a. bei

- dem Aufbau einer sicheren IT-Infrastruktur,
- Virenbefall,
- dem Schutz mobiler Geräte,
- der Datenverschlüsselung,
- dem Zugriff auf das Unternehmensnetz,
- Fragen rund um den Datenschutz,
- führen Sicherheitsanalysen durch,
- zeigen Sicherheitslücken auf,
- beraten und unterstützen beim Aufbau einer sicheren IT-Umgebung,
- vermitteln Security-Spezialisten,
- bilden die Brücke zu Spezialisten,
- helfen bei der Auswahl eines passenden Security-Spezialisten.[1]

16.4 Digitalisierung im Handwerk

Handwerkliche Produktionsverfahren, Dienstleistungen und innerbetriebliche Prozesse werden bzw. müssen mit Hilfe der Digitalisierung angepasst werden.

Innovative Problemlösungen sowie veränderte Arbeitskulturen sind nur darüber möglich, um auch in Zukunft weiter wettbewerbsfähig zu bleiben. Angebote und Partner aus der Industrie geben dazu den Input wie z.B.

- der Einsatz von Drohnen, mit denen u.a. der Dachdecker die Dächer auf mögliche Schäden untersuchen kann.
- der Einsatz von mobilen Laserscannern, um schnell und einfach eine digitale Aufmaß-Erstellung anzufertigen.
- die medienbruchfreie Datendurchgängigkeit die Fehlerquellen und den Zeitaufwand reduziert und zu einer Kostenersparnis führt.

Alle Arbeitsprozesse im Handwerksbetrieb und die damit verbundenen Qualifizierungen müssen schlüssig aufeinander angepasst werden.

Immer mehr und neue Technologien sind in kürzester Zeit verfügbar, die auch die Arbeitsweise im Handwerksbetrieb grundlegend verändert, so der Einsatz von 3D-Druckern

- in der Zahntechnik,
- in der Einzelteilfertigung,
- in der Ersatzteilherstellung und Prototyping.

Innovative sowie individuelle Produkte lassen sich aus den verschiedensten Materialien herstellen, die mit herkömmlichen Verfahren und Technologien nicht oder nur schwer umsetzbar wären. Auch sind Büro-, Verwaltungs- und Planungsarbeiten für viele Handwerksbetriebe sehr zeit- und kostenaufwendig. Durch den Einsatz von geeigneten Softwarelösungen wird die Organisation im Betrieb vereinfacht und effizienter gestaltet.

Lessons Learned

- Die Digitalisierung im Handwerk ist unabdingbar.
- Der Datenschutz und die Datensicherheit sind zu berücksichtigen.
- Die IT-Sicherheit im Handwerk ist zu gewährleisten.

---

[1] https://www.it-sicherheit-handwerk.de/fileadmin/downloads/Flyer/Flyer_2013.pdf, aufgerufen am 30.09.2017.

17. Beratung zu Innovation und Digitalisierung im Berliner Handwerk

Kerstin Wiktor, Handwerkskammer Berlin

Abstract

Die Berliner Handwerkskammer informiert ihre Mitgliedsunternehmen neutral und kostenfrei über Trends und Entwicklungen und berät zu konkreten Fragestellungen zur Zukunftssicherung. Für Innovation und Digitalisierung existieren explizite Angebote. Kooperationen unterstützen den Transfer von Wissen und Innovation aus dem und in das Handwerk.

17.1 Einleitung

Kammerstrukturen und Verbände fungieren als Schnittstelle des Handwerks zu Politik, Wissenschaft, Industrie und Gesellschaft. Die Berliner Handwerkskammer mit ihren Bildungszentren (BTZ und BiZWA) übernimmt neben hoheitlichen Aufgaben, wie der Pflege der Handwerksrolle, die Aus- und Weiterbildung im Handwerk und bietet ein umfangreiches Dienstleistungsspektrum. Ein wichtiger Baustein ist die neutrale Beratung für Gründer|innen und Betriebsinhaber|innen. Die Services der Handwerkskammer (HWK) decken ein weites Themenspektrum ab.

17.2 Struktur des Berliner Handwerks

Die Berliner Handwerkskammer wurde im Jahre 1900 gegründet. Seither sind ihre Mitarbeiter und Mitarbeiterinnen traditionell dem Handwerk verpflichtet. Ca. 30.000 Betriebe gehören zum Berliner Handwerk. Ca. 180.000 Menschen haben in Berlin ihren Arbeitsplatz im Handwerk und mehr als 13.000 Auszubildende finden hier ihre berufliche Perspektive. Die Handwerkskammer Berlin vertritt als Selbstverwaltung die Interessen des gesamten Berliner Handwerks aus zulassungspflichtigen und zulassungsfreien Handwerksberufen von A-Z: von Änderungsschneider|innen bis hin zu Zweiradmechaniker|innen. Insgesamt gehören mehr als 130 Berufe zum Handwerk[1]. Einen ganz wesentlichen

Anteil der Aufgaben nimmt die Aus- und Weiterbildung ein. Das Handwerk ist Ausbilder Nummer eins in Deutschland und glänzt mit seinem dualen Ausbildungssystem - dem Alleinstellungsmerkmal im globalen Maßstab. Praktisches Arbeiten und Lernen im Betrieb kombiniert mit der reflektierend theoretischen Ausbildung in der Berufsschule werden über die Grenzen Deutschlands hinaus hochgeschätzt.

Handwerksbetriebe sind in der Regel klein bis sehr klein (drei bis fünf Mitarbeiter). Diese Gruppe von Wirtschaftsteilnehmern kommt in der Betrachtung von Wirtschaft und in Statistiken selten für sich stehend, oft unter „Sonstige", vor. Um die Rolle des Handwerks sichtbar zu machen, ist Verbands- und Kammerarbeit wichtig. Bildet doch das Handwerk als „Wirtschaftsmacht von nebenan" eine stabile Stütze und zwar besonders in der regionalen Wirtschaft.

Mitgliedsbetriebe, die die kostenfreien Leistungen der Kammer in Anspruch nehmen, schätzen die professionelle Unterstützung.

17.3 Beratungsleistungen der Handwerkkammer

17.3.1 Dienstleistungen und neutrale Beratung

Neben den hoheitlichen Aufgaben spielt Dienstleistung und Beratung eine große Rolle im täglichen Tun von Handwerkskammern. Eingetragene Handwerksbetriebe erhalten zu nahezu allen betriebsrelevanten Themen Unterstützung:

- Betriebswirtschaftliche Beratung
- Bildungsberatung
- Existenzgründungsberatung
- Beratung zu Fragen der Handwerksausübung
- Innovationsberatung
- Rechtsberatung
- Technische Beratung
- Umwelt- und Energieberatung
- Weiterbildungsberatung
- Bestellung von Sachverständigen

Für Fragen zur Zukunftssicherung gibt es z.B. spezielle, durch das Bundesministerium für Wirtschaft und Energie (BMWi) geförderte Angebote. Die Beauftragten für Innovation und Technologie (BIT) übernehmen diese Aufgabe im Rahmen eines Innovationsclusters im Handwerk (Know-how-Transfer im Handwerk). Jede|r von ihnen ist damit sowohl Berater|in in der jeweiligen HWK als gleichzeitig auch Teil eines bundesweiten Netzwerkes – TTnet - mit derzeit ca. 100 Mitgliedern. Das Netzwerk mit seinem enormen Wissenspool kann umfassend zu handwerksrelevanten Themen beraten[2].

Die wesentlichen Aufgaben[3] der BIT sind:

- die systematische Steigerung der Innovationsbereitschaft und -fähigkeit von Handwerksunternehmen,
- die Verbesserung des Wissens- und Technologietransfers zwischen den Akteuren des Innovationssystems und den Handwerksunternehmen und
- der Transfer von Erfahrungen und Ergebnissen aus der Praxis in die handwerkliche Berufsbildung.

Eine gebündelte Expertise kommt letztlich allen Handwerksbetrieben, die Beratungsangebote in Anspruch nehmen möchten, zugute. BIT's sprechen die Sprache des Handwerks und verstehen die Sprachen von Politik, Wissenschaft, Industrie und Startups. Sie wirken als Mittler zwischen den Welten.

Mit kontinuierlicher Weiterbildung, Austausch oder Recherchen halten die Berater|innen ihr Wissen stets auf dem aktuellen Stand. Auf dieser Basis identifizieren sie aktuelle Themen, Technologien und Entwicklungen und transferieren sie ins Handwerk. Die Angebote werden dem tatsächlichen Bedarf der Mitgliedsbetriebe ständig angepasst.

17.3.2 Kooperationen und Netzwerke

Aus der Pflege von Netzwerken, der Vertretung in Gremien oder auch dem Besuch von Veranstaltungen ergeben sich für Handwerksbetriebe Kooperationsangebote, die nicht selten in nachhaltigen Geschäfts- oder F&E-Beziehungen zwischen den Beteiligten münden. Gewachsene Kooperationen bestehen zu Innungen und Fachverbänden, aber ebenso zu Instituten und Wissen-

schaftseinrichtungen. Leicht erklärt sich zum Beispiel eine Wissenschaftskooperation mit der Hochschule für Technik und Wirtschaft (HTW). Auf einer Konferenz kam ein Kontakt zum EFRE-Projekt Digital Value zustande. Aus diesem Kontakt entwickelte sich inzwischen eine für beide Seiten wertvolle Zusammenarbeit.

Klein- und mittelständische Unternehmen (KMU) aus dem Handwerk, die ihr Unternehmen digital aufstellen und dabei auf wissenschaftlich fundierte und praxisnahe Unterstützung zurückgreifen möchten, werden nach vorheriger Erstberatung durch die Beauftragte für Innovation und Technologie (BIT) von Professoren und HTW-Projektmitarbeitern entsprechend des EFRE-Projekts begleitet. Ausgangspunkt hierfür ist jeweils der derzeitige Digitalisierungsgrad des Unternehmens. Gemeinsam werden die individuellen Zielstellungen des Unternehmens erarbeitet und schließlich daraus ein Pilot bzw. Prototyp entwickelt. Begleitet durch einen BIT-Berater der Handwerkskammer, der die Ziele und Herausforderungen des Unternehmens auch unter dem Aspekt der Branchenzugehörigkeit betrachtet, kann die Beratung nach Abschluss des Pilotprojekts weitergehen. Der BIT begleitet den Betrieb als direkter Ansprechpartner über das EFRE-Projekt hinaus. So kann sich z.B. ein Projektantrag für die Weiterentwicklung des Piloten oder aber die Unterstützung bei der Suche nach weiteren Kooperationspartnern oder Finanzierungsmöglichkeiten anschließen. Mit dem Blick auf die Förderlandschaft und spezielle mittelstandsrelevante Programme wie sie z.B. mit ZIM (Zentrales Innovationsprogramm Mittelstand) oder auch Förderprogrammen der IBB – der Förderbank des Landes Berlin - insbesondere den kleinen Betrieben offenstehen, ergeben sich vielfältige Optionen für Handwerksbetriebe.

Dank der Förderung durch das Bundeswirtschaftsministerium ist die Beratungsleistung durch die Beauftragten für Innovation und Technologie (BIT) der Handwerkskammern für Handwerksbetriebe kostenfrei.

17.4 Innovationen im Handwerk

17.4.1 Innovationen prägen das Handwerk

Denkt man an den Fischer-Dübel oder den Adidas-Schraubstollenschuh, so führt die Spur zurück ins Handwerk.

Handwerker erfinden selten am Reißbrett. Meist entstehen Ideen und innovative Produkte aus der Unzufriedenheit mit einem bestimmten Umstand oder aus der Beobachtung des Alltags heraus. Praktische Anforderungen auf der Baustelle, in Betrieb, Atelier oder Werkstatt provozieren Erfindungen mit einfachen Fragestellungen:

- Wie kann man einen Arbeitsgang oder -Ablauf schneller, einfacher oder sicherer machen?
- Was stört einen Kunden und wie kann man das Problem mit einfachen bzw. mit Bordmitteln lösen?
- Wie kann man vorhandene Ressourcen sinnvoll kombinieren?

So entstanden zahlreiche praktische Erfindungen aus dem Handwerk heraus und praktisch nebenbei. Viele Tüftler und Erfinder haben einen handwerklichen Hintergrund.

17.4.2 Strukturiertes Erfinden ist im Handwerk selten

Der Innovationsprozess von der Idee bis zum Produkt und letztlich bis zur Vermarktung folgt im Handwerk selten prozessualen Strukturen. Intuition, gesunder Menschverstand und Try and Error leiten das Handwerk stärker als vordefinierte Prozesse.

Persönliches Herzblut für die Erfindung führt in vielen Fällen aber auch dazu, dass wenig erfolgreiche Projekte nicht rechtzeitig abgebrochen werden.

Nur relativ wenigen Patenten, die im Handwerk entstanden sind, gelang es schließlich, sich erfolgreich am Markt durchzusetzen. Fast gegen Null geht die Anzahl der Standards oder Normen, die vom Handwerk gesetzt wurden oder werden.

Die Innovationsberatung der Handwerkskammer soll diesen Widerspruch überwinden helfen und den Weg zur Umsetzung von Ideen ebnen. Ausgehend von einer grundsätzlichen Analyse der Machbarkeit, erhalten Erfinder aus dem Handwerk Anleitungen zum Umgang mit und Schutz von Ideen. Sie bekommen zusätzlich Hinweise zu Finanzierungsquellen und Unterstützung bei der Suche nach Kooperations- und Vermarktungspartnern.

17.5 Digitalisierung im Berliner Handwerk

Das Handwerk spürt in Zeiten der Digitalisierung wachsenden Druck durch den Markt einerseits und der Industrie andererseits. Es nimmt nicht selten eine „Sandwichposition" ein. Der Markt – über die unterschiedlichsten Kanäle mit Informationen versorgt – ist kritischer geworden, die Loyalität der Kunden schwindet. Die Industrie drängt mit individualisierten Produkten und Dienstleistungen auf den klassischen Handwerksmarkt. Unterstützt durch datengetriebene Geschäftsprozesse und -modelle, ist die Industrie in der Lage, Produkte in kurzer Zeit nahezu in Handwerksqualität zu liefern. Meist auch noch zu günstigeren Preisen als jeder Handwerker sie wirtschaftlich vertreten kann. Hinzu kommt, dass digitalisierte Maschinen- und Anlagen für kleine Handwerksunternehmen in der Beschaffung und kleine Losgrößen in der Produktion teuer sind, was deren Anschaffung erschwert. Hinzu kommen besonders in Berlin die Startups, die sich aufgrund ihrer Schnelligkeit und Wendigkeit als ernstzunehmende neue Mitspieler im Handwerksfeld etablieren.

Die Innovationsberatung der Handwerkskammer Berlin fokussiert sich auf geschäftsmodell- und prozessbezogene Digitalisierungsfragen sowie auf Kooperationen, in denen digitale Technologien ausprobiert und getestet werden können. Beispielhaft seien folgende Kooperationen, Initiativen und Netzwerke genannt:

- Die Handwerkskammer Berlin ist Transferpartner des Kompetenzzentrums digitales Handwerk. Die Kompetenzzentren und Agenturen 4.0 aus der Mittelstand 4.0-Initiative[4] des Bundeswirtschaftsministeriums (BMWi) liefern ein breites Informations- und Unterstützungsangebot.
- In Kooperation mit der HTW und dem EFRE-Projekt Digital Value bekommen Betriebe eine koordinierte Begleitung von der Bedarfsanalyse bis zur Umsetzungsbegleitung ihres individuellen Digitalisierungsvorhabens.
- Den Transfergedanken bedient z.B. die Berliner Kooperationsplattform „Marktreif"[5], über die sich Wirtschaftspartner aus Berlin finden, um Projektpartnerschaften zu schließen.

- Dem Austausch des Berliner Handwerks zum Thema digitale Transformation dient die kürzlich gegründete XING-Gruppe „Berliner Handwerk digital"[6].
- Im Anwendungszentrum creative Applied Interactive Technologies (cAPITs) der HTW geht es darum, gemeinsam herauszufinden, wie interaktive Technologien aus der Spielebranche z.B. auch im Handwerk nutzbringend angewendet werden können.
- Für den Methodentransfer pflegt die Handwerkskammer Kooperationen und Netzwerke. Unter anderem bildet die Mitarbeit der HWK in der Berliner Startup-Unit die Grundlage zur Zusammenarbeit mit Startups.
- In Punkto IT-Sicherheit sichern Kooperationen z.B. mit der Zentralen Ansprechstelle Cyber-Kriminalität (ZAC) der Berliner Polizei, der Initiative Deutschland sicher im Netz (DSiN) oder auch lokalen IT-Netzwerken, wie SIBB, den Zugang zu Wissen und Informationen.

Das Beratungs-Portfolio der Handwerkskammer besteht in Sachen Digitalisierung aus verschiedensten Informationen, Veranstaltungen und Workshops zu digitalen Entwicklungen und Anwendungen bzw. daraus resultierenden gesetzlichen Anforderungen. Ein konkreter Nutzen für den Handwerksalltag ist dabei Ausgangspunkt jeglicher Planungen.

17.6 Fazit

Das Handwerk ist konkret und mag es konkret. Aufgrund der betrieblichen Struktur von Handwerksbetrieben müssen Beratungs- und Unterstützungsangebote einen greifbaren und praktischen Bezug liefern. Unternehmer|innen im Handwerk brauchen keine umfangreichen theoretischen Abhandlungen, sondern konkrete Handlungsanleitungen und Umsetzungspartner. Erfolgreiche und nachhaltige Kooperationen entstehen, wenn sie von gegenseitigem Respekt getragen sind und Stolz und Eigenart des Handwerks berücksichtigen.

Lessons Learned

- Die Beauftragten für Innovation und Technologie (BIT) der Handwerkkammern beraten Handwerksunternehmen neutral und kostenfrei. Sie vermitteln Kooperationen und Netzwerke.
- Innovationsprozesse im Handwerk unterscheiden sich grundsätzlich von denen in Industrie, Wissenschaft und Startups.
- Für Digitalisierung im Handwerk braucht es jeweils einen konkreten praktischen Bezug.

---

[1] Vgl. Jahresbericht der Handwerkskammer Berlin. Berliner Handwerk (2017). Bilanz und Ausblick; S. 93 ff.

[2] Zentralverband des deutschen Handwerks (ZDH) (2017). Beauftragte für Innovation und Technologie. Aufgerufen am 14.08.2017. Verfügbar unter: https://www.zdh.de/themen/gewerbefoerderung/technik-innovation-und-normung/beauftragte-fuer-innovation-und-technologie/.

[3] Vgl. BAnz AT 16.01.2017 B1, Richtlinie zur Förderung eines Innovationsclusters im Handwerk durch ein Informations-, Beratungs- und Technologietransfernetzwerk (Know-how-Transfer im Handwerk) vom 10. Januar 2017, Abschn. 2.2.2.

[4] Bundesministerium für Wirtschaft und Energie (2017). Aufgerufen am 14.08.2017. Verfügbar unter: www.mittelstandigital.de/DE/Foerderinitiativen/mittelstand-4-0.

[5] Berlin Partner für Wirtschaft und Technologie GmbH, IHK Berlin, HWK Berlin (2017). Aufgerufen am 14.08.2017. Verfügbar unter: www.marktreif.berlin.

[6] XING AG (2017). Aufgerufen am 14.08.2017. Verfügbar unter: www.xing.com/communities/groups/berliner-handwerk-digital-314a-1098878.

18. Sicherung Kritischer Infrastrukturen

Joern Kinzel, Technologiezentrum Teltow

Abstract

Kritische Infrastrukturen schaffen die Voraussetzungen, um das Staatsgebilde und das Zusammenleben in einer Gemeinschaft zu ermöglichen. In diesem Beitrag wird die Definition von Kritischen Infrastrukturen erläutert, und die Position des Gesetzgebers dazu analysiert. Ferner werden die Vorteile von Kooperationsnetzwerken beschrieben, welche bei der Sicherung von kritischen Infrastrukturen helfen.

18.1 Kritische Infrastrukturen: Eine Definition

„Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."[1]

18.2 Darstellung Kritischer Infrastrukturen nach Branchen

In der BSI-Kritisverordnung (BSI-KritisV) werden folgende Branchen und Bereiche als Kritische Infrastrukturen aufgeführt:

1. Energie: Elektrizität, Gas, Mineralöl (§2 BSI-KritisV)
2. Wasser: Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung (§3 BSI-KritisV)
3. Ernährung: Ernährungswirtschaft, Lebensmittelhandel (§4 BSI-KritisV)
4. Informationstechnik und Telekommunikation (§5 BSI-KritisV)
5. Gesundheit: Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore (§6 BSI-KritisV)

6. Finanz- und Versicherungswesen: Banken, Börsen, Versicherungen, Finanzdienstleister (§7 BSI-KritisV)
7. Transport und Verkehr: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik (§8 BSI-KritisV)
8. Staat und Verwaltung: Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/ Rettungswesen einschließlich Katastrophenschutz
9. Medien und Kultur: Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke

18.3 Die Kritischen Infrastrukturen nach dem IT-Sicherheitsgesetz

Der Entwurf der Bundesregierung zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (kurz: IT-Sicherheitsgesetz oder IT-SiG) vom 25.02.2015 sieht unter anderem Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI-Gesetz oder BSIG) vor. Dadurch soll die IT-Sicherheit von Unternehmen verbessert und die Bürgerinnen und Bürger im Internet besser geschützt werden (BT-Drucks. 18/4096, S. 1). Dieser Gesetzesentwurf sorgte für viele Unsicherheiten. Insbesondere ist dem Entwurf nicht zweifelsfrei zu entnehmen, wer zu den sogenannten Kritischen Infrastrukturen gehört und somit zum Anwendungsbereich des Gesetzes gehört (siehe auch Kapitel 18.5). Weitere Informationen veröffentlicht auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seinen Informationsseiten[2].

Am 3. Mai 2016 ist der erste Teil der BSI-Kritisverordnung (§10 BSI-Gesetz) zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten. Betroffene Unternehmen (Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung) können hier eine Kontaktstelle gemäß §8b BSI-Gesetz benennen. Mit der ersten Verordnung zur Änderung der BSI-Kritisverordnung, die am 30.06.2017 in Kraft getreten ist, werden die Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr ergänzt.

Zu den wesentlichen Inhalten des IT-Sicherheitsgesetzes gehören die Einführung und Ausweitung von Meldungen über erhebliche Störungen sowie die

Einführung und der regelmäßige Nachweis branchenspezifischer Sicherheitsstandards. Das BSI-Gesetz wird u.a. durch §8b „Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen" ergänzt, der in Abschnitt 4 die Meldepflicht näher ausführt. Demnach sind Betreiber Kritischer Infrastrukturen dazu verpflichtet, „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden."

Weiterhin definiert Abschnitt 4, welche Angaben aus der Meldung hervorgehen müssen. Hierbei handelt es sich um:

- die technischen Rahmenbedingungen,
- die vermutete oder tatsächliche Ursache,
- die betroffene Informationstechnik und
- die Art der betroffenen Einrichtung oder Anlage sowie die Branche des Betreibers.

18.4 Kritikalität von Infrastrukturen

Infrastrukturen gelten als „kritisch", wenn sie für die Funktionsfähigkeit moderner Gesellschaften von wichtiger Bedeutung sind und ihr Ausfall oder ihre Beeinträchtigung nachhaltige Störungen im Gesamtsystem zur Folge hat. Ein wichtiges Kriterium dafür ist die Kritikalität als relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat.

Verschiedene Gefahren können Kritische Infrastrukturen bedrohen. Diese sind bei Risiko- und Gefährdungsanalysen sowie der Auswahl von Handlungsoptionen gleichermaßen zu berücksichtigen. Das BSI empfiehlt zur Abschätzung der Kritikalität, die IT-Infrastruktur und die dort betriebenen Systeme in verschiedene Schutzklassen einzuordnen. Danach muss der Betreiber einschätzen, wie groß das Risiko eines Angriffs auf das System ist. Wenn sowohl die

Schutzklasse als auch das Angriffsrisiko groß sind, sollte auch die Qualitätsklasse des ausgewählten Produktes hoch sein. Soweit möglich und anwendbar, werden hierzu technische Standards und Sicherheitsprofile festgelegt, insbesondere die sogenannten „Common Criteria Protection Profiles".

18.5 Im IT-Sicherheitsgesetz berücksichtigte Organisationen

Das IT-Sicherheitsgesetz will, dass Unternehmen ihre digitalen Informationen schützen. Unternehmen sind aufgefordert, Hacking und sonstige Schäden durch technische Fehler oder Fehlbedienungen der Mitarbeiter zu verhindern. Hierfür macht das Gesetz Vorgaben. Dazu gehört vor allem eine Dokumentation der Prozesse, Audits und Meldepflichten gegenüber der Aufsichtsbehörde.

Der Gesetzgeber will nicht allen Unternehmen diese erhöhten und kostenintensiven Pflichten auferlegen. Nur Unternehmen, die aus Bundessicht für die Versorgung der Bürger wichtig sind, unterfallen diesen Pflichten. Für die Sektoren Energie, Informationstechnik und Telekommunikation, Ernährung und Wasser sowie die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr wurde nunmehr mit einer Änderungsverordnung geregelt, welche Unternehmen aus diesen Sektoren unter das IT-Sicherheitsgesetz fallen. Zur Übersicht sei an dieser Stelle die BSI-KritisV – BSI-Kritisverordnung mit allen relevanten Schwellenwerten für alle Sektoren genannt[3].

Anlagenkategorie	***Bemessungskriterium***	***Schwellenwert***
Gewinnung		
Gewinnungsanlage	Gewonnene Wassermenge in Millionen m³/Jahr	22
Wasserwerk	Wasseraufkommen in Millionen m³/Jahr	22
Aufbereitung		
Aufbereitungsanlage	Aufbereitete Trinkwassermenge in Millionen m³/Jahr	22
Wasserwerk	Wasseraufkommen in Millionen m³/Jahr	22
Verteilung		

Wasserverteilungs-system	Verteilte Wassermenge in Millionen m³/ Jahr	22
Leitzentrale	Von den gesteuerten/überwachten Anlagen gewonnene, transportierte oder aufbereitete Menge Wasser in Millionen m³/Jahr	22

Tabelle 3: Schwellenwerte der Trinkwasserverordnung.

Tabelle 3 zeigt ein Beispiel von Schwellenwerten für die Trinkwasserverordnung. Als Faustregel kann man grob Unternehmen dazuzählen, von deren Leistung mindestens 500.000 Bürger betroffen sind. Laut Gesetzesbegründung sind hiervon wohl nur geschätzte 2.000 Unternehmen betroffen.

Jedes unter Kritis eingestufte Unternehmen ist angehalten, angemessene organisatorische und technische Datensicherheitsmaßnahmen nach dem Stand der Technik vorzusehen. Was dazu gehört, legt der Gesetz- und Verordnungsgeber nicht fest. Hier kommen Standards vom Bundesamt in der Informationstechnik (BSI) und ISO/DIN-Normen genauso zur Anwendung wie neue, bisher nicht ausdrücklich anerkannte Sicherheitsmaßnahmen. Dem Kostendruck stellt das IT-Sicherheitsgesetz bestimmte formelle Pflichten und eine Haftung über Bußgeldsanktionen (bis EUR 100.000,00) bei Pflichtverletzungen gegenüber.

Übrigens: Unabhängig von den vorgenannten Pflichten gilt ein kleiner Teil des IT-Sicherheitsgesetzes für alle Unternehmen, die eine Website betreiben. Fürdiese Unternehmen ist u.a. eine passende Verschlüsselung und Authentifizierung gerade bei Registrierungen vorgesehen, weiterhin eine regelmäßige Einspielung der Software inkl. Updates für die Beseitigung von Sicherheitslücken der sowie die Nutzer richtig zur IT-Sicherheit zu informieren.

18.6 Die Arbeit des Kooperationsnetzwerkes DiSiNet

Das DiSiNet ist ein ZIM-Kooperationsnetzwerk von zehn Unternehmen und vier Forschungseinrichtungen. Die Unternehmen sind klassische KMU mit drei bis maximal 50 Mitarbeitern. Ziel des Netzwerkes ist es, auf die Betriebsgrößen der kleinen Betreiber angepasste Sicherheitslösungen für Kritische Infrastrukturen zu entwickeln und den Unternehmen zugänglich zu machen. Ta-

belle 4 zeigt eine Übersicht aller Gefahren, die Kritische Infrastrukturen beeinträchtigen können (aus BMI, Kritis Strategie-) und Strukturen in ihrer Aufgabe schädigen können.

Naturereignisse	**Technisches / menschliches Versagen**	**Terrorismus, Kriminalität, Krieg**
Extremwetterereignisse u.a. Stürme, Starkniederschläge, Temperaturstürze, Hochwasser, Hitzewellen, Dürren	Systemversagen u.a. Unter- und Überkomplexität in der Planung, Hardware-, Softwarefehler	Terrorismus
Wald- und Heidebrände	Fahrlässigkeit	Sabotage
Seismische Ereignisse	Unfälle und Havarien	Sonstige Kriminalität
Epidemien und Pandemien bei Mensch, Tier und Pflanzen	Organisatorisches Versagen u.a. Defizite im Risiko- und Krisen-management, unzureichende Koordination und Kooperation	Bürgerkriege und Kriege
Kosmische Ereignisse u.a. kosmische Energiestürme, Meteoriten und Kometen	*N/A*	*N/A*

Tabelle 4: Gefahren, die Kritische Infrastrukturen beeinträchtigen können; Quelle: BMI, Kritis Strategie.

Das Netzwerk konzentriert sich dabei auf die grau hinterlegten Gefahren:

- Systemversagen durch Soft- und Hardwarefehler,
- organisatorisches Versagen durch inadäquate Unternehmensprozesse und
- durch kriminelle Energie verursachte Sabotageschäden.

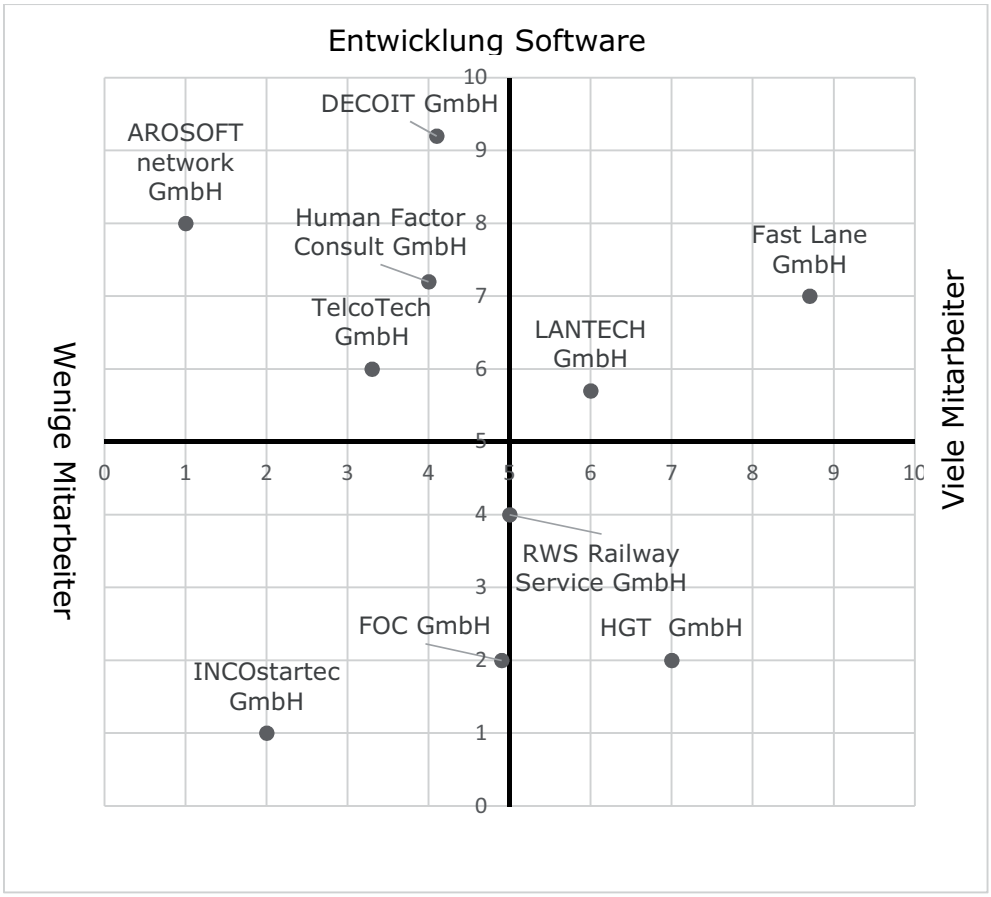

Abbildung 22: Charakterisierung der Unternehmen im Netzwerk DiSiNet; eigene Darstellung.

Da alle Unternehmen des Netzwerkes KMU sind, ist der Blickwinkel entsprechend fokussiert auf Anwendungen mit hoher Usability, die keine hohen Investitionskosten benötigen. Zielgruppen sind ganz klar Unternehmen, die die Schwellenwerte nach dem BSI-KritisV noch nicht überschritten haben und Betreiber von Kritischen Infrastrukturen selbst sowie deren Lieferanten. Abbildung 22 zeigt die Heterogenität der Unternehmen, die ein weites Spektrum an Entwicklungs-Knowhow aufweisen. Reine Hardware-Entwickler sind genauso vertreten wie reine Softwarehäuser. Aus der Zusammenarbeit entstehen in der Folge Ideen, die ein einzelnes Unternehmen alleine nicht realisieren könnte.

18.7 Beispiel der Entwicklungsarbeit

In der Zusammenarbeit der verschiedenen Unternehmen und Forschungseinrichtungen ergeben sich immer wieder neue Fragestellungen, mit den die Unternehmen durch ihre Kunden konfrontiert werden. Diese Fragestellungen werden dann zusammen mit Partnern, die Gewerke zum Projekt beisteuern können, diskutiert und anschließend ein Projektteam aufgestellt, das sämtliche Aspekte der Produktentwicklung abdecken kann. Durch diesen Prozess sind auch die Projekte entstanden, die im Folgenden beschrieben werden.

18.8 Nano-Firewall

Gegenstand des Projektes ist die Entwicklung einer preiswerten, aber dennoch robusten und energiesparenden Nano-Firewall. Die innovative Hardware wird auf Basis der Embedding Component Technology (EMBEDDING) entwickelt, die maßgeblich von der TU mitentwickelt wurde. Das EMBEDDING wird im Projekt erstmalig für die komplexen Strukturen eines ARM v8-Controllers und der Peripherie angepasst. Das Gerät soll in den Bereichen IoT, Gebäudeautomation und Industrie 4.0 eingesetzt werden. Durch die Kombination mehrerer Einzelmodule zu einem Verbund (Clusterung) erfolgt die Skalierung der Leistungsparameter für den jeweiligen Einsatzzweck.

Die Software der Nano-Firewall wird in Hinblick auf die Leistungsfähigkeit des ARM-Moduls so angepasst, dass trotz neuer Sicherheits-Features eine performante Prüfung der eingehenden Pakete erfolgt. Diese Features umfassen Deep Packet Inspection (DPI) und Protokollkonverter, um den unautorisierten Fremdzugriff auf Maschinen-, Sensoren- oder Gebäudefunktionen, die mit proprietären Protokollen laufen, unterbinden zu können.

18.9 ScanBox

Projektziel ist die Entwicklung einer Appliance zur Erhebung und Dokumentation des Sicherheitsniveaus in KMU. Das Gerät soll, im Gegensatz zu üblicherweise statischen Erhebungen, ohne manuellen Eingriff das Sicherheitsniveau der überwachten Infrastruktur permanent evaluieren und automatisiert Handlungsempfehlungen ableiten. Dabei sollen Scan, Analyse und Penetrationswerkzeuge evaluiert, entwickelt und die konsolidierten Scan- und Monitoring

-Ergebnisse in zielgruppenspezifischen Berichten zusammengefasst werden. Diese setzen die detektierten Sicherheitslücken in Bezug zu den im Vorfeld gewichteten Unternehmenswerten und Sicherheitszielen um, um daraus automatisiert konkrete Handlungsempfehlungen abzuleiten. Projektziel ist die Implementierung eines automatischen Usability-Beobachters. Dieser beobachtet sowohl die Benutzerinteraktion mit dem System, als auch die Validität und Verständlichkeit (Usability) der vorgeschlagenen Katalogmaßnahmen. Im Laufe der Benutzung durch den örtlichen (autodidaktisch herangebildeten) Verantwortlichen passt sich das System an dessen Erfahrungshorizont an. Die empfohlenen Gegenmaßnahmen basieren auf den Empfehlungen des BSI zum IT-Grundschutz. Über die Integration der Common Vulnerabilities and Exposure (CVE) Datenbank soll ein Bezug zu den vom BSI entsprechend empfohlen Gegenmaßnahmen hergestellt werden.

18.10 Alarmierungspriorisierung

Die Daten aus Heizungstechnik und Trinkwasserversorgung als Teil der Gebäudeleittechnik (GLT) sollen Entscheidungen auf Basis von Intuition und Erfahrung zugunsten einer daten- bzw. statistikbasierten Entscheidungslogik ersetzen. Damit soll erreicht werden, dass durch neue Analysemethoden die gesamte Heizungsanlage und Trinkwasserversorgung prozesstechnisch optimiert werden. Dafür soll ein innovatives Alarmierungstool die Alarme durch Abgleich mit älteren Vorgängen priorisieren und zeitsparend aufbereiten. Durch die Analyse des Anlagenzustands kann somit die Instandhaltung effektiver organisiert und durch die Auswertung historischer und aktueller Daten eine Energieauswertung erstellt werden. Neuronale Netze sollen es ermöglichen, dass die Zusammenhänge sich ändernder Parameter automatisch erkannt und durch historische Daten verglichen werden, um etwaige Trends vorhersagen zu können. Da das Wesen der Daten bekannt ist, kann eine vollautomatisierte Energieverbrauchrechnung aufgestellt werden, um so ein preisgünstiges Tool zu erhalten und der EEG zu genügen.

Lessons Learned

- Sichere Kritische Infrastrukturen sind essentiell für das Funktionieren moderner Gesellschaften.
- In Kooperationsnetzwerken arbeiten Unternehmen aus unterschiedlichen Branchen miteinander an gemeinsamen Entwicklungsprojekten.
- Die Entwicklungsprojekte führen zu neuen Produkten, die helfen, Infrastrukturen abzusichern.

---

[1] Definition „Kritische Infrastrukturen" nach „KRITIS", Bundesministerium des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).

[2] Nähere Informationen finden sich dazu unter: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html.

[3] Ein Überblick zu weiteren Sektoren findet sich unter: https://www.jurion.de/gesetze/bsi_kritisv/.

Autorenverzeichnis

HEIKO BEHRENDT

ist beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) in leitender Funktion für die Durchführung datenschutzrechtlicher und sicherheitstechnischer Audits zuständig. Als zertifizierter ISO 27001 Auditor unterstützt er Organisationen auf dem Weg der Implementierung eines Informationssicherheitsmanagementsystems (ISMS) bis zur Zertifizierung.

E-Mail

mail@datenschutz-expert.de

GERD M. FUCHS

ist seit 17 Jahren als Rechtsanwalt mit eigener Rechtsanwaltskanzlei tätig. Davor bzw. daneben war bzw. ist er u.a. als Jurist etwa beim öffentlichen und privaten Rundfunk, in Internetunternehmen und-Agenturen sowie bei einem Internetverband tätig. Seine Kanzlei FOXLAW® ist auf das Recht der neuen Medien, Wettbewerbs-, Urheber-, Marken, Vertrags- und Datenschutzrecht spezialisiert.

E-Mail

Anwalt@foxlaw.de

MADLEN BÖER

forscht im EFRE Projekt Digital Value Anwendungszentrum bei Prof. Dr. Hartmann zur Digitalisierung von KMU in Berlin an der HTW Berlin.

E-Mail

Madlen.Boeer@HTW-Berlin.de

LEONHARD GEBHARDT

forscht im EFRE Projekt Digital Value Anwendungszentrum bei Prof. Dr. Hartmann zur Digitalisierung von KMU in Berlin an der HTW Berlin.

E-Mail

Leonhard.Gebhardt@HTW-Berlin.de

OLAF BORRIES

arbeitet seit 1999 bei der Polizei Berlin. Er ist dort seit knapp 10 Jahren Sachbearbeiter im Bereich Cybercrime im engeren Sinne und betreut seit 2014 die Zentrale Ansprechstelle Cybercrime (ZAC) in Berlin.

E-Mail

zac@polizei.berlin.de

VANESSA GRÜHSER

ist bei der IHK Berlin die Ansprechpartnerin für den Wissens- und Technologietransfer. Teil dieser Arbeit ist die Organisation von Kooperationen zwischen der Wirtschaft-Wissenschaft. Dafür stellt sie seitens der IHK, zusammen mit der HWK Berlin (Frau Wiktor) und Berlin Partner die Plattform maktreif.berlin zur Verfügung.

E-Mail

vanessa.gruehser@berlin.ihk.de

ROLAND HALLAU

ist seit Anfang der 1990er Jahre Beratender Ingenieur bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Dort arbeitet er auch als Projektleiter der Mittelstand 4.0-Agentur-Prozesse. Diese unterstützt kostenfrei bei der Digitalisierung von Produktions- und Arbeitsprozessen mit praxisorientierten Weiterbildungs- und Informationsformaten.

E-Mail

rhallau@tti-md.de

JENS JANKOWSKY

ist Referent für Innovation, Technologie und Energie (Fachbereich Wirtschaftspolitik) bei der IHK Ostbrandenburg.

E-Mail

jankowsky@ihk-ostbrandenburg.de

Prof. Dr.

MATTHIAS HARTMANN

lehrt und forscht in den Fachgebieten Produktion und Logistik sowie Informations- und Technologiemanagement. Er ist Projektleiter des Anwendungszentrums „Digital Value" an der HTW Berlin und Leiter des Labors Unternehmenssimulationen. Vor seiner Berufung an die HTW Berlin arbeitete er für die Unternehmensberatung A.T. Kearney in der Strategic Information Technology Practice.

E-Mail

Matthias.Hartmann@HTW-Berlin.de

Prof. Dr.

MICHAEL HENDRIX

lehrt und forscht im Gebiet Wirtschaftsinformatik im Fachbereich Wirtschaft, Informatik, Recht an der TH Wildau. Er ist Vorstandsvorsitzender der Gesellschaft zur Förderung angewandter Informatik Brandenburg e.V. (GFaI Brandenburg e.V.) und sitzt im Wissenschaftlichen Beirat der IBWF-Akademie, Berlin.

E-Mail

michael.hendrix@th-wildau.de

MICHAEL HOLZHÜTER

arbeitet als wissenschaftlicher Mitarbeiter im Projekt "Lernlabor Cyber-Sicherheit" bei Prof. Dr. Meissen, welches in einem Fraunhofer-Fachhochschul-Laborverbund angesiedelt

ist. Seine Forschungsinteressen liegen im Bereich Weiterbildungen für IT-Sicherheit.

E-Mail

Michael.Holzhueter@HTW-Berlin.de

UWE HOPPE

ist Hauptgeschäftsführer der Handwerkskammer Frankfurt (Oder).

JOERN KINZEL

ist Netzwerkmanager beim Technologiezentrum Teltow. Das von ihm betreute Netzwerk „Digitalisierung und Sicherheit für Kritische Infrastrukturen (DiSiNet)" hat das Ziel, Unternehmen, die Kritische Infrastrukturen betreiben, dabei zu unterstützen, ihre Netz- und Leitsysteme sicher zu betreiben und Sicherheitsvorfälle proaktiv zu erkennen und entgegenzuwirken.

E-Mail

Kinzel@tz-teltow.de

HENRIK KLOHS

arbeitet als Beauftragter für Innovation und Technologie an der Handwerkskammer Frankfurt (Oder). Er ist für die Kontaktvermittlung zu wissenschaftlichen Institutionen zuständig und organisiert Workshops und Informationsveranstaltungen, wie z.B. den IT-Sicherheitstag in Berlin und Brandenburg.

E-Mail

henrik.klohs@hwk-ff.de

Prof. Dr.

TIMO KOB

ist Professor für Wirtschaftsschutz und Cybersicherheit an der FH Campus Wien sowie Gründer und Vorstand der HiSolutions AG, einem Beratungsunternehmen für Informationssicherheit und IT-Management mit Sitz in Berlin und Niederlassungen in Bonn, Köln und Frankfurt.

E-Mail

info@hisolutions.com

KNUT KRICKE

beschäftigt sich seit 2013 mit Mobilen Endgeräten der mobilen Sicherheit. Er hält Vorträge und leistet Aufklärungsarbeit zu den Themen Unternehmensdaten und Zugriffe von extern/mobilen Geräten sowie der Sicherung von Daten gegen Fremdeinwirkung. Knut Kricke ist seit 1996 beruflich in der IT tätig und ist Geschäftsführer der VERTEXakademie GmbH.

E-Mail

kkricke@amassist.eu

MARK LE CORRE

arbeitet im Bereich Cybercrime im engeren Sinne in der Zentralen Ansprechstelle Cybercrime (ZAC) in Brandenburg.

E-Mail

zac@polizei.berlin.de

Prof. Dr.

LUIGI LO IACONO

forscht an webbasierten Medienanwendungen und -technologien sowie an Web, Cloud und Usable Security. In all diesen Themengebieten bestehen umfangreiche Vorarbeiten, die zum Großteil im Rahmen von geförderten Projekten erarbeitet wurden und in zahlreiche Publikationen gemündet sind.

E-Mail

luigi.lo_iacono@th-koeln.de

MANUELA PÜSCHEL

leitet als Chief Operating Officer veschiedene Bereiche (z.B. Konzeptentwicklung für neue IT-Strukturen, Marketing und Social Media, Prozessoptimierung sowie Controlling und Qualitätsmanagement) in der Firma Die Netz-Werker AG.

E-Mail

MP@dnw.ag

HARTMUT SCHMITT

ist Koordinator für Forschungsprojekte beim saarländischen IT-Unternehmen HK Business Solutions GmbH. Er ist seit mehr als 10 Jahren in Verbundvorhaben auf den Gebieten Mensch-Computer-Interaktion, Usability und Software-Engineering tätig. Hartmut Schmitt leitet den Arbeitskreis Usable Security bei der German UPA (deutscher Berufsverband der Usability Professionals).

E-Mail

hartmut.schmitt@hk-bs.de

Dr.

KNUTH THIEL

leitet den Geschäftsbereich Wirtschaft der IHK Ostbrandenburg.

CARSTEN VOSSEL

leitet als Geschäftsführer die CCVOSSEL GmbH in Berlin. Das Unternehmen ist im Bereich Software-Entwicklung tätig.

E-Mail

info@ccvossel.de

MIKE WÄSCHE

ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Dort arbeitet er als Mitarbeiter der Mittelstand 4.0-Agentur-Prozesse. Diese unterstützt kostenfrei bei der Digitalisierung von Produktions- und Arbeitsprozessen mit praxisorientierten Weiterbildungs- und Informationsformaten.

E-Mail

mwaesche@tti-md.de

RALF WAUBKE

forscht im EFRE Projekt Digital Value Anwendungszentrum bei Prof. Dr. Hartmann zur Digitalisierung von KMU in Berlin an der HTW Berlin.

E-Mail

Ralf.Waubke@HTW-Berlin.de

KERSTIN WIKTOR

ist die Beauftragte für Innovation und Technologie (BIT) an der Handwerkskammer Berlin. Sie berät Handwerksbetriebe in den Schwerpunkten Technologietransfer/-Kooperationen.

E-Mail

wiktor@hwk-berlin.de

SASCHA WILMS

leitet das Referat Mittelstand von Deutschland sicher im Netz e.V. (DsiN). Der Verein positioniert sich als zentraler Ansprechpartner für Verbraucher und mittelständische Unternehmen in Fragen zur IT-Sicherheit. Produktneutral und herstellerübergreifend kooperiert er mit dem Bundesministerium des Innern.

E-Mail

info@sicher-im-netz.de

Prof. Dr.

STEFAN WITTENBERG

hält an der HTW Berlin die Professur für Prozessmanagement und ERP-Systeme inne. Er hat 12 Jahre Erfahrung als Führungskraft in der Industrie (Bertelsmann, Bundesdruckerei). Er forscht zu Themen und Gebiete im Bereich von Industrie 4.0, Logistik, Produktionsplanung und -steuerung sowie Geschäftsprozess-optimierung und Informationssicherheit.

E-Mail

Stefan.Wittenberg@HTW-Berlin.de

Prof. Dr.

JAN WIRSAM

ist seit 2015 an der Hochschule für Technik und Wirtschaft und lehrt Operationsmanagement und Innovationsmanagement. Forschungsschwerpunkte sind dabei Digitalisierung, App-Entwicklung, Geschäftsmodell-Innovationen, Start-Ups und Nachhaltigkeit. Zuvor war er in dem Konzern Ricoh in führender Position für den Bereich Druck- und IT-Outsourcing tätig.

E-Mail

Jan.Wirsam@HTW-Berlin.de