

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance

Sonderausgabe 2016
Öffentlicher Dienst

IT-Security im Öffentlichen Dienst

Die Themen:

- Planspiele zum Krisentraining im Rechnerbetrieb
- Cloud-Speicherdienste für Verwaltungen

- Informationssicherheit in der Öffentlichen Verwaltung
- Effiziente und sichere Behördenkommunikation

- Ransomware – warum Erpressungstrojaner so gefährlich sind
- Elektronische Akten aus der Cloud



Auch online verfügbar



Selbstverständlich können Sie die aktuelle Ausgabe unseres Sonderhefts **IT-SICHERHEIT „IT-Security im Öffentlichen Dienst“** auch einfach und bequem online lesen – egal, ob am PC oder via Smartphone. Probieren Sie es aus ...

www.datakontext.com/download/branchenguide



Mit dem E-Paper zu unserem **Branchenbuch IT-Sicherheit 2016** geben wir Ihnen wieder einen umfassenden Überblick rund um die verschiedenen Aspekte der IT-Sicherheit. Wir zeigen auf, wo überall Gefahren für Ihre Unternehmens-IT lauern, und erleichtern Ihnen die Suche nach den passenden Produkt-Anbietern und Dienstleistern, die Ihnen als Experten mit Rat und Tat zur Seite stehen.

<http://www.datakontext.com/branchenguide>



Das Sonderheft **IT-SICHERHEIT Best Practice** berichtet über erfolgreich umgesetzte Security-Projekte in Wirtschaft beziehungsweise Verwaltung und erlaubt einen Einblick, welche Sicherheitsanforderungen in der täglichen Praxis gefragt sind. Die Neuauflage des Sonderhefts finden Sie unter ...

www.datakontext.com/branchenguide

Impressum

IT-SICHERHEIT
Fachmagazin für Informationssicherheit und Compliance
Sonderausgabe: IT-Security im Öffentlichen Dienst

Verlag:
DATAKONTEXT GmbH
Augustinusstraße 9d, 50226 Frechen

Vertrieb
Jürgen Weiß
Tel.: 0 22 34/98 94 9-71
Fax: 0 22 34/98 94 9-32

www.datakontext.com
fachverlag@datakontext.com

Redaktion:
Dr. Martin Zilkens

Thomas Reinhard-Rief
reinhard@datakontext.com

Herausgeber:
† Bernd Hentschel

Layout:
Britta Happel
happel@datakontext.com

Anzeigen- & Objektleiter:
Thomas Reinhard-Rief
reinhard@datakontext.com

Abonnement:
Jahresabonnement € 85,-
(für Studenten und GDD-Mitglieder: € 50,-)
Einzelheft € 15,- zzgl. Versandkosten
Erscheinungsweise: sechs Ausgaben

Satz: Britta Happel, DATAKONTEXT
Druck: AZ Druck und Datentechnik GmbH, Kempten

© DATAKONTEXT
Mit Namen gekennzeichnete Beiträge stellen nicht unbedingt die Meinung der Redaktion oder des Verlages dar. Für unverlangt eingeschickte Manuskripte übernehmen wir keine Haftung. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Verfasser alle Rechte, einschließlich der weiteren Vervielfältigung zu gewerblichen Zwecken. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Titelbild: fotolia.com
Fotos: Firmenbilder; DATAKONTEXT; © (Tiberius Gracchus, James Steidl, Tom Wang, Yong Hian Lim, ra2 studio, DigitalGenetics, buchachon, Ioana Davies (Druu), Luminis)/Fotolia.com

1. Jahrgang 2016 • ISSN: 1868-5757

Mit zunehmender Digitalisierung wächst das Sicherheitsbedürfnis

Liebe Leserinnen und Leser,

mit zunehmender Digitalisierung wächst das Sicherheitsbedürfnis – das ist eine der Erkenntnisse unserer heutigen Zeit. Gerade Unternehmen, die öffentliche Verwaltung und die Betreiber sogenannter Kritischer Infrastrukturen (KRITIS) mussten in den letzten Jahren lernen, sich mit den Gefährdungspotenzialen gut strukturierter, zielgerichteter Cyberangriffe auseinanderzusetzen.

Aktuell geistert ein neues Schlagwort durch die Presse: Ransomware. Bereits im März dieses Jahres sah sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) genötigt, eine Publikation mit dem Titel „Risikoanalyse Krankenhaus-IT“ zu veröffentlichen, in der dargestellt wurde, wie Krankenhäuser ihre IT-Abhängigkeiten kritischer Prozesse analysieren und Risiken ermitteln können. Hintergrund: Kurz vorher war es in Krankenhäusern bundesweit zu mehreren IT-Sicherheitsvorfällen gekommen, die durch einen Verschlüsselungs-Trojaner (Ransomware) verursacht worden waren.

Vor einem Monat nun gab das BSI die Ergebnisse einer im Rahmen der Allianz für Cyber-Sicherheit durchgeführten Umfrage bekannt, der zufolge ein Drittel (32 Prozent) aller befragten Institutionen der deutschen Wirtschaft in den letzten sechs Monaten von Ransomware be-

troffen war. Die Auswirkungen von Locky, Tesla-Crypt & Co. reichten vom kurzzeitigen Ausfall einzelner Arbeitsplätze bis hin zum Stillstand der Produktion und dem Verlust wichtiger Daten, die nicht wiederherstellbar waren.

Derartige Beispiele zeigen, dass Cyberangriffe auch in Zukunft eine große Gefahrenquelle darstellen werden. Hierauf müssen sich Wirtschaft und Verwaltung gleichermaßen einstellen. Neben präventiven Maßnahmen, die Sicherheitsexperten in den Institutionen ergreifen müssen, um Schadfälle zu verhindern, sollten mittelfristig aber auch Strukturen und Prozesse geschaffen werden, die im Falle eines Störfalles greifen und einen Totalausfall beziehungsweise Folgeschäden vermindern. Denn zu hoffen, dass man von derlei Angriffen verschont bleibt, ist in der heutigen Zeit extrem fahrlässig.

Auf den kommenden Seiten betrachten Autoren aus Wissenschaft und Praxis verschiedene IT-Security-Themen aus dem Blickwinkel des öffentlichen Sektors. So gehen die Autoren Dr. Johannes Neubauer und Dr. Michael Neubauer in ihrem Beitrag auf Stör- und Systemausfälle in Rechenzentren ein (S. 6 ff.). Das Autorenteam Ralf Maxim und Frank Lehnert stellt einen Cloud-Speicherdienst für Verwaltungen vor (S. 10 ff.) und Jacqueline Naumann beschreibt die einzelnen Schritte zur Einführung eines Informations-Sicherheits-Manage-

ment-Systems (ISMS) im Öffentlichen Dienst beziehungsweise in einem KRITIS-Unternehmen (S. 12 ff.).

Der Frage, warum Erpressungstrojaner so gefährlich sind, geht Thomas Uhlemann in seinem Fachbeitrag nach (S. 21 ff.). Die Experten Matteo Cagnazzo, Patrick Wegner und Norbert Pohlmann vom Institut für Internet-Sicherheit stellen ihre sichere Kommunikationsplattform namens „Quvert“ vor (S. 24 ff.) und zu guter Letzt geht Gerd Zilch in seinem Beitrag näher auf das Thema Dokumentenmanagement ein (S. 28 ff.).

Ich wünsche Ihnen viel Spaß und einen fachlichen Mehrwert beim Lesen der Ausgabe.

Mit freundlichen Grüßen

Dr. Martin Zilkens

Behördlicher Datenschutzbeauftragter der Landeshauptstadt Düsseldorf und Vorstandsmitglied der Gesellschaft für Datenschutz und Datensicherheit e.V.

Dr. Martin Zilkens



Anzeige

„Wir wissen, dass jede Organisation eine eigene DNA hat. Sie auch?“

Hans-Jürgen Grabe, Kompetenzzentrum Informationssicherheit

SECURisk
Member of the
DATA CENTER
GROUP

JETZT UMFASSENDE BERATUNG ANFORDERN

Die SECURisk DNA-Strategie.

SECURisk erarbeitet Konzepte zum Schutz Ihrer Unternehmens-DNA, denn wenn es um Informationen geht, sollten Sie nichts dem Zufall überlassen. Wir bieten die Basis für mehr Effizienz und Sicherheit.

SecuRisk GmbH

In der Aue 2 | 57584 Wallmenroth

Phone +49 2741 9321-0

Fax +49 2741 9321-111

info@securisk.de | securisk.de

Alle IT-Sicherheitsanbieter auf it-sicherheit.de!

Täglich News aus der IT-SICHERHEIT-Redaktion
Größte Jobbörse im Bereich IT-Sicherheit
Größtes Verzeichnis von Anbietern und Produkten
Verständliche Sicherheitstipps und -videos
Aktuelle Sicherheitshinweise und -empfehlungen

Ihr Ansprechpartner:
Sebastian Wacowski, B.Sc.
Projektleiter IT-Sicherheit.de
Tel. +49 (0)209 9596 762
wacowski@internet-sicherheit.de

www.it-sicherheit.de
Der Marktplatz IT-Sicherheit

In Kooperation mit:



securityNews

securityNews: Kostenlose App für mehr Sicherheit im Netz



- 🎯 Kostenlose App vom Institut für Internet-Sicherheit
- 🎯 Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- 🎯 Warnung vor Sicherheitslücken in Standardsoftware, dank BSI-Schwachstellenampel
- 🎯 Konkrete Anweisungen für Privatanwender und Unternehmen

>> www.it-sicherheit.de



Mit freundlicher Unterstützung von:



Top IT-Nachwuchs auf Recruiting-Messe

Präsentieren Sie Ihr Unternehmen dem IT-Security-Nachwuchs von morgen und gewinnen Sie schon jetzt die **besten Nachwuchskräfte** am 16. September 2016! Treffen Sie persönlich Top-Talente beim Match-Making!

Melden Sie Ihr Unternehmen an unter:
cscg.de/recruiting-messe





Editorial

3 Mit zunehmender Digitalisierung wächst das Sicherheitsbedürfnis

Training

6 Planspiele zum Krisentraining im Rechnerbetrieb

Cloud Computing

10 Cloud-Speicherdienste für Verwaltungen

Informationssicherheit

12 Informationssicherheit in der Öffentlichen Verwaltung

Ransomware

21 I ran some Ransomware – warum Erpressungstrojaner so gefährlich sind

Behördenkommunikation

24 Effiziente und sichere Behördenkommunikation

Dokumentenmanagement

28 Elektronische Akten aus der Cloud

Service

2 Online-Service

2 Impressum



www.datakontext.com/newsletter



facebook.com/itsicherheit



twitter.com/it_sicherheit24



IT-SICHERHEIT



Planspiele zum Krisentraining im Rechnerbetrieb

Es gibt nur wenige qualitative und quantitative Studien über Störfälle und Systemausfälle in Rechenzentren. Systemanbieter wie Amazon oder Akamai haben mittlerweile eine so große Verbreitung, dass selbst ein Teilausfall ihrer Systeme große Auswirkungen auf das Internet hat [1],[2]. Die Ursachen und die daraus resultierenden Maßnahmen werden meist nur in kurzen Presse-notizen dargestellt. Eine systematische Bewertung der Maßnahmen in einem wissenschaftlichen Sinne ist eine seltene Ausnahme.

Auf der Seite der Anwender ist es nicht anders. Auch hier wird viel über die ausgefeilten Sicherheitskonzepte der Rechenzentren berichtet. Selbst über mehrstündige Ausfälle wie zum Beispiel bei Finanz Informatik GmbH der Sparkassen im September 2015 gibt es meist nicht mehr als eine kurze Presse-notiz.

Die Erfahrungen aus der Praxis der Autoren zeigt deutlich: Gleichgültig wie ausgefeilt die Sicherheits- und Redundanzkonzepte in den Rechenzentren sind: Ausfälle gibt es immer wieder und in diesen Fällen ist der Ausbildungs- und Trainingsstand der Mitar-

beiter ein Schlüsselfaktor für die schnelle Störbeseitigung.

Das Training von Krisensituationen in einem Rechenzentrum ist wegen der kontinuierlichen Nutzung der Systeme und der häufig knappen Personaldecke nicht einfach. Wir stellen im Folgenden ein Planspiel vor, das mit Hilfe eines Simulators Trainingssituationen ermöglicht, die unabhängig vom Tagesgeschäft genutzt werden können. Das unterliegende Planspielkonzept berücksichtigt einerseits abstrakte technische Zusammenhänge und andererseits externe und interne

Stressmomente, die durch Kunden oder Menschen auf die Betriebsmannschaft einwirken.

Status quo

Die meisten Managementsysteme, die sich mit Sicherheit und Qualität in Rechenzentren beschäftigen, legen einen besonderen Schwerpunkt darauf, Probleme von Beginn an zu vermeiden. So sieht zum Beispiel die ISO 27001 nach BSI-Grundschutz eine systematische Bewertung der Risiken im Rahmen der Aufstellung des Managementsystems vor. Eine solche Vorgehensweise hat einige grundsätzliche Probleme.

Das Sicherheitssystem bezieht meist nur solche Risiken ein, die wahrscheinlich und vorhersehbar sind. Darüber hinausgehende Fehlersituationen werden im Wesentlichen durch eine allgemeine, an organisatorischen Fragen orientierte Notfallplanung berücksichtigt. Das Thema Training hat in diesem



Zusammenhang nur eine untergeordnete Bedeutung:

Ein Beleg dafür kann zum Beispiel darin gesehen werden, dass der rund 120 Seiten umfassende BSI-Standard 100-4 nur zwei Seiten dem Thema Training widmet.

Die Notfallplanung (zum Beispiel nach ISO 27001) beschäftigt sich im Wesentlichen mit dem Wiederanlauf nach einem Ausfall. Die Suche nach Fehlern ist beispielsweise nicht Gegenstand der Notfallplanung.

Die Fähigkeit, in Krisensituationen zu improvisieren und auch unerwartete Probleme systematisch zu lösen, gehört zu den Schlüsseigenschaften einer robusten Organisation [3]. Es zeigt sich, dass das Thema Training von solchen Situationen in der Praxis und in den einschlägigen Normen eine untergeordnete Bedeutung hat. Da, wo Trainings in

Notfallkonzepten berücksichtigt werden, haben sie vielmehr einen theoretischen Charakter. So sieht der BSI-Grundschutz Planspiele eher als ein Konzept zur Evaluierung der formellen Notfallplanung als ein individuelles Training der jeweiligen Mitarbeiter. Die geringe Neigung, sich mit tatsächlichen Krisenübungen dem Thema Training zu nähern, hat sicher auch damit zu tun, dass es in den meisten Rechenzentren weder die personellen noch die technischen Ressourcen gibt, um eine größere Fehler- oder eine komplexe Ausfallsituation parallel zum laufenden Betrieb zu üben. Externe Trainingssysteme, wie sie zum Beispiel für Kraftwerke oder auch im medizinischen Bereich üblich sind, gibt es im Bereich der IT faktisch nicht.

Gleichzeitig zeigt sich in der Praxis immer wieder, dass alle Redundanzkonzepte und vorausschauendes Risikomanagement Ausfälle nicht generell verhindern können. Störfälle und Krisensituationen treten auch dort auf, wo normkonform, professionell mit hochverfügbarer Hardware gearbeitet wird. Gerade die hohe Verfügbarkeit heutiger Rechenzentren führt dazu, dass die Erfahrung bei der Fehlersuche und Fehlerbeseitigung bei den Betriebsmannschaften nachlässt.

Alle diese Überlegungen haben dazu geführt, mit einem simulationsgestützten Planspiel den Rahmen für bessere Trainingsmöglichkeiten von Krisensituationen zu eröffnen. Eine Arbeitsgruppe der Technischen Universität Dortmund hat einen ersten Prototyp für ein Planspiel konzipiert. Er soll im Frühjahr des Jahres 2016 mit Mitarbeitern der Citkomm in Hemer praktisch erprobt werden. Im folgenden Abschnitt wird zunächst das dem Planspiel unterliegende Spielkonzept skizziert. Anschließend werden die für das Projekt eingesetzten softwaretechnischen Methoden erläutert.

Planspielkonzept

Das Planspielkonzept besteht aus mehreren Komponenten:

- einem Modell eines Rechenzentrums, das die wesentlichen technischen Abläufe simuliert.
- einem Regelprozessablauf, der wichtige Funktionen im Normalbetrieb eines Rechenzentrums abbildet. Hierzu gehören zum Beispiel das Starten und Stoppen von Systemen und die Überwachung von Systemparametern sowie die Beseitigung von einfachen Störungen im Betrieb.

- kaufmännischen Geschäftsprozessen, beispielsweise die Akquisition von Aufträgen über ein vereinfachtes Börsensystem, Managementprozesse, die die unterschiedlichen Abteilungen innerhalb des Rechenzentrums modellieren.
- einem Spielleiter, der im Verlauf des Spieles die Aufgabenstellung erläutert, überwacht und die Lösungsversuche der Probanden steuert. Er kann auf vielfältige Weise in den Spielverlauf eingreifen, Modellparameter ändern und so anspruchsvolle Fehlersituationen in das Simulationsmodell einbringen. Er kann auch soziale Einflüsse durch vorbereitete Kundengespräche oder Managementanfragen in die Spielsituation einbringen.

Das Spielkonzept sieht vor, dass das Technikmodell in gewissen Grenzen an das Arbeitsumfeld der Probanden angepasst werden kann. Typische Schwerpunkte für das Planspiel können zum Beispiel folgende Aufgaben sein:

- das Training von Mitarbeitern zu systematischer Fehleranalyse auch bei starken externen Stressoren.
- die Bewältigung von Krisen in einem komplexen organisatorischen Umfeld.

Die eingesetzten Softwarewerkzeuge ermöglichen eine weitgehend modellgesteuerte Programmierung, sodass das Simulationsziel in einem gewissen Bereich durch Customizing gesteuert werden kann. Nach dem Customizing beginnt die eigentliche Planspielphase, in der die Teilnehmer eine Spielsituation ohne Fehler im Modell bewältigen müssen.

Das Spielkonzept sieht dabei eine Aufgabenstellung vor, die auch bei Wirtschaftsplanspielen verwendet wird. Vom Rechenzentrum abzuarbeitende Aufträge werden von einer kaufmännischen Abteilung an einer Börse akquiriert. Anschließend werden diese mit Hilfe der Simulation im Rechenzentrum abgearbeitet und hierfür wird dem Rechenzentrum ein virtueller Geldbetrag überwiesen. Nach der Eingewöhnungsphase geht es zunächst darum, in einem optimal eingerichteten Rechenzentrum die Erlöse zu maximieren.

In der zweiten Phase wird das Spiel dadurch modifiziert, dass Systemkomponenten im Bereich der technischen Simulation

ausfallen. Zur Beseitigung der Fehler müssen die Teilnehmer die Fehlersituationen anhand von Überwachungsprotokollen und Logfiles analysieren und so fehlerhafte Einstellungen korrigieren. Während der Arbeit müssen die üblichen Berichte und Interaktionen mit dem Management weiter fortgeführt werden. Die Spielleitung sorgt dafür, dass außerdem über Telefonanrufe und E-Mails weitere Störgrößen in das Spiel eingebracht werden. Darüber hinaus ist geplant, im Rahmen einer Masterarbeit eine ausgefeilte Version des Simulators und des Planspiels zu entwickeln. Am Ende könnte ein Dienstleistungsangebot stehen, das Rechenzentren für Trainingszwecke angeboten wird.

Modellgesteuerte Softwareentwicklung

Für die Erstellung des Spielprototyps Krisenplan werden verschiedene Werkzeuge des Lehrstuhls für Programmiersysteme der TU Dortmund eingesetzt, die es ermöglichen, die Anwendung in graphischen Modellen auf einem hohen Abstraktionsniveau zu beschreiben. In der klassischen Softwareentwicklung würde diese ...

- manuell in einer sogenannten universellen Programmiersprache,
- unter Verwendung einer komplexen Systemumgebung und
- mit vielen Programmbibliotheken und damit einhergehend einer hohen Lernkurve

entwickelt. Aktuelle Lösungen für die Entwicklung von Anwendungen oder Geschäftsprozessen beziehen Experten mit profunden Fachkenntnissen – hier für die Abläufe in einem Rechenzentrum – in die Modellierung ein. Dabei wird berücksichtigt, dass diese meist wenig bis keine Programmierkenntnisse besitzen.

Mit der Einführung von softwaregestützten Werkzeugen zur Geschäftsprozessmodellierung bietet sich die Möglichkeit, Inkonsistenzen zwischen Anforderungen und technischer Umsetzung zu vermeiden. Auch wenn solche Modelle kein Allheilmittel sind, ermöglichen sie, die in der Branche vielgefürchtete „semantische Lücke“ zu reduzieren. Damit sind die Abgründe zwischen Fachexperte (im vorliegenden Fall der Trainer) und Techniker, bezogen auf Terminologie, Erfahrung und Mentalität, gemeint. Aus Sicht der Autoren sind sie die Quelle für

Missverständnisse zwischen Fachseite und IT-Abteilung.

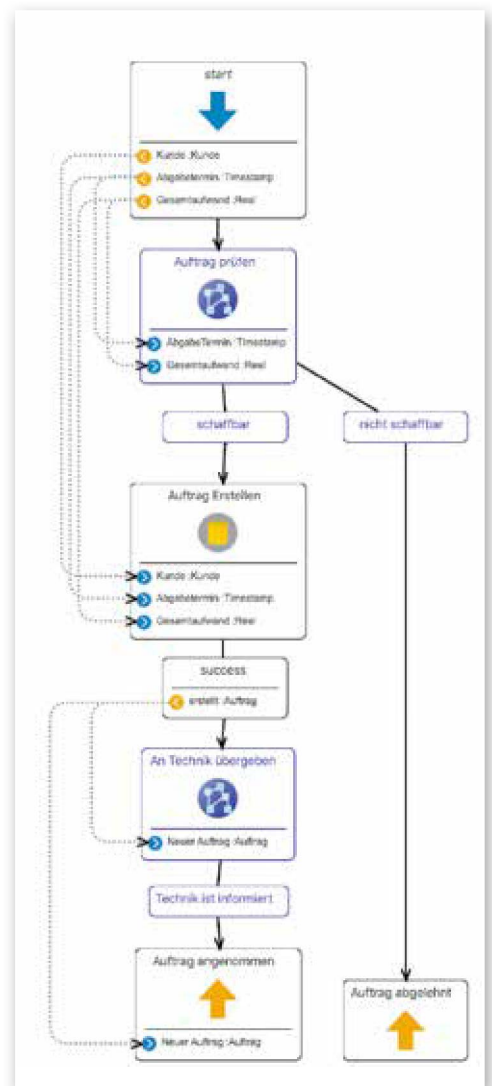
Bei näherem Hinsehen muss eingestanden werden, dass dieser Traum nur in sehr spezifischen Szenarien und mit starker Nachbesserung durch ein engagiertes IT-Team wahr wird. Hierbei wird das Modell des Spielleiters nachträglich noch von Technikern verfeinert, damit es auch wirklich in ein lauffähiges Programm umgesetzt werden kann. Leider gestalten sich dadurch nachträgliche Änderungen durch den Spielleiter ungleich schwieriger, da diese Änderungen berücksichtigt werden müssen.

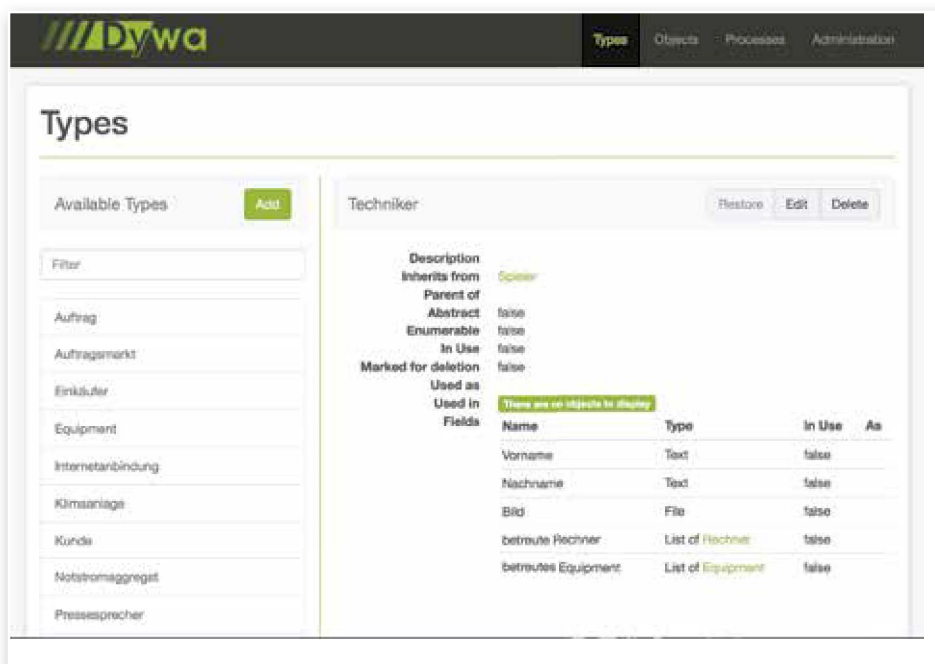
Moderne Software wird meist für eine ganze Branche oder einen generischen Anwendungsfall entwickelt. Die individuellen Anforderungen werden durch sogenanntes Customizing berücksichtigt. Ähnliches ist auch für den Spielsimulator notwendig, weil das Spielerlebnis auch davon abhängt, dass die Probanden sich im Spiel „zu Hause“ fühlen. Kommerziellen Modellierungswerkzeugen fehlt bisher die Unterstützung für die Berücksichtigung von Varianten. In der Literatur wird der Bedarf an der Umsetzung von variantenreichen Systemen häufig unter dem Begriff Produktlinien zusammengefasst. Alle aktuellen Geschäftsprozessmodellierungsstandards sind auf feste Bindungen zwischen einer Geschäftsaktivität und der Software, die sie implementiert, beschränkt. Das bedeutet im Umkehrschluss, dass jede Variante explizit über entsprechende Entscheidungspunkte modelliert werden muss. Für das vorliegende Spiel hätte das die Konsequenz, dass auch kleine Veränderungen in den Anforderungen zu einer unverhältnismäßig großen Veränderung des Ursprungsmodells führen weil nicht nur die Variante, sondern der gesamte neue Geschäftsvorfall in das Modell eingefügt werden muss.

Das ist weit von dem Ideal einer Vereinfachung entfernt, die die Geschäftsprozessmodellierung überhaupt erst so reizvoll macht. Die am Lehrstuhl erstellten Werkzeuge [4] folgen einem ganzheitlichen Prinzip, bei dem die Entwicklung der Spielbestandteile (häufig wird hierfür der Begriff Datenmodell verwendet) und der Spielabläufe Hand in Hand geht. Ferner wird die Geschäftsprozessmodellierung um leicht verständliche Abwandlungen von bekannten und bewährten Funktionalitäten aus

dem Bereich der Programmiersprachen erweitert, wie zum Beispiel Customizing, Interoperabilität und Agilität (Anpassbarkeit). Der Rechenzentrumsexperte konnte so auch während des Entwicklungsprozesses des Spiels Erweiterungen und Korrekturen an dem Modell vornehmen [5].

Die Entwicklung des Planspiels Krisenplan profitiert davon, dass die Ergebnisse der Entwicklung allen Beteiligten eines Rechenzentrums (und nicht nur den Technikern) verständlich sind. Dabei wird sichergestellt, dass Spielentwurf und Spielsimulator stets in einem konsistenten Zustand bleiben. Dadurch kann ein kontinuierlicher Verbesserungsprozess (KVP) auf natürliche Art und Weise umgesetzt werden. Weiterhin besteht die Herausforderung bei einem derartigen Spiel darin, bei den jeweiligen Spielern eine Identifikation mit der Spielsituation zu erzeugen. Auch das führt zu dem Bedarf an ei-





ner einfachen Möglichkeit, Varianten des Spiels zu erzeugen, ohne mit der Entwicklung immer und immer wieder von vorne zu beginnen. Auch die Trainingssituationen selbst bedürfen der Abwechslung und bieten damit Variantenreichtum, um verschiedene Entwicklungsstufen (sogenannte Level) oder auch Trainingseinheiten abzubilden. Hier können die angesprochenen Werkzeuge DyWA (Dynamic Web Application) und jABC4 (Java Application Building Center)

ihre Stärken ausspielen, die eine Entwicklungsumgebung für die Erstellung der oben erläuterten Modelle bieten und eine ausführbare Web-Anwendung erzeugen.

Die Projektgruppe ProBio [6] ist auch die letzten Schritte zu vollständig modellierten Anwendungen angegangen, wenn auch aus dem Blickwinkel von Anwendungen für den Bereich Biomedizin. Die hieraus entstandene Modellierungsumgebung erlaubt es, ne-

ben Spielbestandteilen und Spielabläufen auch die verschiedenen beteiligten Spielerrollen sowie die Benutzeroberfläche zu modellieren. Das Ergebnis ist ein Spiel, das ein Spielleiter zu großen Teilen ohne Hilfe auf seine Bedürfnisse anpassen kann und das über eine Weboberfläche erreichbar ist. Damit ist auch gewährleistet, dass die Installation und die Verteilung des Spiels kein Problem darstellen. Da die gesamte Kommunikation über das Spiel abläuft, wird lediglich ein Rechner oder Tablet mit einem Webbrowser und einem Internetanschluss benötigt. Selbst mobile Trainingseinheiten sind damit in erreichbarer Nähe.

Damit sind die Möglichkeiten der technologischen Unterstützung von Krisenplan noch nicht ausgeschöpft. An der TU Dortmund wird derzeit eine Masterarbeit betreut, die eine direkte Echtzeit-Kommunikation zwischen dem Spiel und den Spielern sowie dem Spielleiter an ihrem Webbrowser ermöglichen soll. Dies ist für ein Spiel mit Echtzeitsimulation von großem Wert und stellt im Bereich der Webtechnologien eine besondere Herausforderung dar. ■

Literaturhinweise

- [1] Miller, R. (7. 8 2011). *Outage in Dublin Knocks Amazon, Microsoft Data Centers Offline*. Abgerufen am 28. 12 2014 von Data Center Knowledge : <http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/>
- [2] Sverdlik, Y. (19. 8 2015). *Lightning Strikes Google Data Center, Disrupts Cloud Services*. Abgerufen am 28. 12 2015 von Data Center Knowledge i: <http://www.datacenterknowledge.com/archives/2015/08/19/lightning-strikes-google-data-center-disrupts-cloud-services/>
- [3] Neubauer, M. (2010). *Krisenmanagement in Projekten* (3. Ausg.). Springer Wissenschaftsverlag.
- [4] Neubauer, J. et al. (2014). *Prototype-driven development of web applications with dywa in Leveraging Applications of Formal Methods, Verification and Validation. Technologies for Mastering Change*. S. 56-72.
- [5] J. Neubauer, B. Steffen (2013). *Plug & Play Higher-Order Process Integration*. IEEE Computer Nr. 11, August 2013, IEEE Computer Society
- [6] FB Informatik Lehrstuhl 5. (2016). *Endbericht der Projektgruppe ProBio*. TU Dortmund.



DR. JOHANNES NEUBAUER,
wissenschaftlicher Angestellter TU Dortmund



DR. MICHAEL NEUBAUER,
Geschäftsführer KDZ Citkomm

Cloud-Speicherdienste für Verwaltungen

Es gibt immer mehr Anzeichen dafür, dass der Einsatz von Cloud-Speicherdiensten in der deutschen öffentlichen Verwaltung wachsen wird. Am Wichtigsten allerdings ist, dass dafür nur sichere Angebote eingesetzt werden dürfen: Die Schutzwürdigkeit der Bürgerdaten muss stets gewährleistet sein.

Die Digitalisierung aller Vorgänge macht auch vor den Verwaltungen nicht halt. Im privaten Umfeld erleichtern die klassischen Funktionalitäten einer Cloud wie Cloud-Speicher, File-Sharing, Datenaustausch, Backup und Restore, Zugriff auf Daten und Dateien über das Internet oder die Zusammenführung von Daten aus unterschiedlichen Endgeräten das digitale Leben. Sei es für das Speichern von Urlaubsfotos oder das Teilen von Inhalten – dass unsere privaten Daten „irgendwo“ liegen, ist inzwischen fast selbstverständlich und oft unvermeidlich. Gleichzeitig ist es nachvollziehbar, dass man Annehmlichkeiten aus dem persönlichen Gebrauch auch in der Arbeit einsetzen möchte.

Weitere Vorteile von Cloud-Speicherlösungen liegen unter anderem im schnellen Zugriff auf Daten und im Abruf von verschiedenen – und auch mobilen – Endgeräten aus (Smartphone, Tablet etc.). Im Rahmen einer Flexibilisierung der Arbeitswelt wird der Aspekt, auch vom „Home-Office“ oder von unterwegs auf die zentral abgelegten Daten zuzugreifen, eine wachsende Rolle spielen.

Andererseits ist eines ganz klar: Jeder ist dafür, wie er mit seinen Daten umgeht, selbst verantwortlich. Das Recht auf informationelle Selbstbestimmung besagt aber nicht nur dies, sondern eben auch, dass die Verantwortung von Bund, Ländern und Kommunen für die Daten ihrer Bürger ernst zu nehmen ist. Das Vertrauen der Bürger in ihre Verwaltungen ist ungebrochen groß und ein Gut, das nicht nur unschätzbar, sondern, wenn einmal verloren, auch unwiederbringlich ist. Laut Artikel 4 Abs. 2 der Landesverfassung NRW hat jeder Anspruch auf Schutz seiner personenbezogenen Daten. Die NRW-Kommunen sind diesem Schutz zudem nach Datenschutzgesetz NRW verpflichtet.

All dies hat das Kommunale Rechenzentrum Minden-Ravensberg/Lippe (krz) zum Anlass genommen, eine sichere Cloud-Speicherlösung für seine Kommunen, deren Beschäftigte sowie Politik und Bürgerschaft zu entwickeln.

Die Sicherheitsstandards der kommerziellen Cloud-Anbieter sind für den Einsatz im öffentlichen Dienst nicht ausreichend. Entscheidender Nachteil der bekannten kommerziellen Lösungen wie Google Drive, Dropbox, MS-Skydrive, Teamdrive usw. ist sicherlich die Tatsache, dass Kunden und Nutzer hier nicht sicher sein können, wo ihre Daten letztendlich abgespeichert werden. Unter Umständen werden die Daten in großen Cloud-Rechenzentren gespeichert, deren Standorte nicht in der EU beziehungsweise in Deutschland liegen und somit nicht den deutschen Datenschutzgesetzen unterliegen. Auch die großen Anbieter haben diesen Unterschied erkannt (Telekom, Microsoft etc. werben inzwischen mit der Datenhaltung am Standort Deutschland). Doch ist der Standort nicht der einzige Faktor. Im letztjährigen Sonderheft „Öffentlicher Dienst“ dieser Publikation hat Dr. Martin Meints, IT-Sicherheitsbeauftragter von Dataport AöR „Möglichkeiten der Nutzung von Cloud-Services in der öffentlichen Landes- und Kommunalverwaltung“ [1] beleuchtet. Er benennt drei Anforderungen, damit ein Cloud-Service nach deutschem Recht genutzt werden kann:

1. Bindung des Dienstleisters an europäisches und nationales Datenschutzrecht.
2. Einhalten eines angemessenen Niveaus der Informationssicherheit. Hier nennt er insbesondere den Standard ISO 27001 auf Basis von IT-Grundschutz.
3. Vermeiden konkurrierender Gesetzgebung.

Mit seiner BSI-Zertifizierung erfüllt das Kommunale Rechenzentrum Minden-Ravensberg/Lippe (krz) in Lemgo alle drei Kriterien, die für die über das Internet zur Verfügung gestellten Dienstleistungen gefordert sind. Das krz ist seit über 40 Jahren der Informatik-Dienstleister der Kreise Minden-Lübbecke, Herford und Lippe sowie aktuell von 34 Städten und Gemeinden aus diesen Kreisgebieten. Als kommunaler Zweckverband besitzt das krz den Status einer Körperschaft des öffentlichen Rechts. Es unterstützt etwa 8.000 PC-Arbeitsplätze mit rund 10.500 Geräten in den Verwaltungen des Verbandsgebietes. Direkt oder indirekt werden über 11 Mio. Einwohner in NRW mit Services aus Lemgo betreut.

Bereits 2007 wurde das krz als erstes Kommunales Rechenzentrum in Deutschland nach ISO 27001 auf der Basis von IT-Grundschutz durch das BSI zertifiziert, die jüngste und bisher dritte Re-Zertifizierung für weitere drei Jahre erfolgte 2015. Seit 2014 bietet es die „krz DataBox“, eine Cloud-Speicherlösung, als Alternative zu kommerziellen Lösungen für seine kommunalen Kunden an. Die Funktionen der DataBox sind nahezu identisch mit denen der kommerziellen Lösungen und bieten darüber hinaus eine Verschlüsselungsmöglichkeit an.

Neben den üblichen Standardfunktionen, wie das Hochladen von Daten in benutzerbezogene Datenräume in der Cloud, den Dateiaustausch über Up- und Download-Links und das Einbinden von Datenräumen als Netzlaufwerk, bietet diese Softwarelösung noch weitere entscheidende Vorteile, die teilweise auch sicherheitsrelevant sind.

Ein Outlook-Add-in fügt sich in die vorhandene Outlook-Anwendung ein, hier erfolgt das Versenden eines Links, der auf die DataBox verweist. Diese Alternative zum Versenden von E-Mails mit großem Anhang entlastet wirksam das E-Mail-System. Zusätzlich ist der Versand der Nachricht dadurch durchgehend verschlüsselt. Zur Nachverfolgung

und Absicherung kann der Nutzer zudem einstellen, dass er per E-Mail benachrichtigt wird, wenn Dateien aus der DataBox heruntergeladen werden. Auch von mobilen Geräten (Smartphones und Tablets) kann ein Großteil der Funktionen auch über die eigenen iOS- und Android-Apps genutzt werden. Besonders erwähnenswert ist außerdem die Verschlüsselung mit der sog. Triple-Crypt-Technologie, die ermöglicht, besonders sensible Daten und Dokumente dreifach zu schützen. Die Daten werden auf dem Endgerät, auf dem Transportweg (über das SSL-Protokoll) und auf dem eigentlichen Datenspeicher verschlüsselt.

In seinem Eckpunktepapier von 2013 zum Cloud Computing [2] hat das BSI die permanente „Überwachung der bereitgestellten Dienste“ als Sicherheitsempfehlung angeraten. Diese kann über eine BSI-Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz gewährleistet werden. „Damit CSPs nachweisen können, dass sie auch bei hohem Schutzbedarf bezüglich Vertraulichkeit und Verfügbarkeit ausreichend Sicherheit gewährleisten, ist eine Zertifizierung des Informationssicherheitsmanagements sinnvoll. Vorzugsweise sollten CSPs nach ISO 27001 auf Basis von IT-Grundschutz, ISO 27001 oder einem anderen etablierten Standard zertifiziert sein.“

Des Weiteren gibt das Papier an, für den „Aufbau einer soliden Sicherheitsarchitektur für Cloud Computing sollten die im Folgenden beschriebenen Aspekte betrachtet werden“:

Rechenzentrumssicherheit

- Server-Sicherheit
- Netzsicherheit
- Anwendungs- und Plattformsicherheit
- Datensicherheit
- Verschlüsselung und Schlüsselmanagement

Fußnoten

- [1] Dr. Meints, Martin: Möglichkeiten der Nutzung von Cloud-Services in der öffentlichen Landes- und Kommunalverwaltung. in: *IT-Sicherheit. Fachmagazin für Informationssicherheit und Compliance. Sonderausgabe IT-Sicherheit im Öffentlichen Dienst.* (2015), S. 38 - 41
- [2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile&v=4

ID- und Rechtemanagement

- Authentisierung
- Autorisierung

Die BSI-Zertifizierung des Zweckverbandes krz gilt nicht nur für alle selbst genutzten oder für Kunden zur Verfügung gestellten Anwendungen und IT-Systeme, sondern auch für den vollständigen Betrieb des Rechenzentrums im Informationsverbund. So erfolgt der Betrieb der Cloud in der BSI-zertifizierten Infrastruktur. Auch die speziell auf Cloud Computing bezogenen BSI-Anforderungen werden hiermit erfüllt.

Die Verankerung der krz DataBox in die Struktur des Rechenzentrums ergibt daher viele Vorteile für die Anwender. Wesentliche Kriterien sind hier neben der Einhaltung der strengen Datenschutzbestimmungen die Ablage der Daten auf hochverfügbaren Storage-Systemen im gesicherten Data Center. Die vom BSI geforderte Rechenzentrumssicherheit wird unter anderem durch eine permanente Spiegelung der Daten an zwei Standorten gewährleistet.

Die Kommunen profitieren darüber hinaus von der Einbindung in den Verbund des kommunalen Rechenzentrums. Die Authentifizierung kann mühelos über das zentrale Active Directory erfolgen. Darüber hinaus erlaubt es das flexible Rollen- und Rechtekonzept, nahezu alle Anwendungsvarianten in der vorhandenen Rechtestruktur abzubilden. Auch hier konnten die Anforderungen an ein ID- und Rechtemanagement laut BSI-Eckpunktepapier erfüllt werden. Sämtliche Aktivitäten werden dabei reversionssicher protokolliert. Zudem werden alle Übermittlungen beim Hoch- und Herunterladen auf Viren überprüft. All diese Funktionalitäten unterstreichen den grundsätzlichen Ansatz der Lösung: Auf Daten und Dokumenten sicher zugreifen und diese mit anderen teilen, egal von wo und über welche Geräte.

Ein weiteres Beispiel für einen Bereich, in dem Sicherheit von höchster Wichtigkeit ist und in dem aus diesem Grund die DataBox eingesetzt wird, ist die Nutzung in kommunalen Leitstellen, zum Beispiel für Feuerwehren oder im Katastrophenschutz: Seit Anfang des Jahres 2015 setzt die Kreisleitstelle Herford die Lösung ein, um ihre sensiblen Daten zu übermitteln. Für die Aktualisierung von Einsatzplänen und andere wichtige Informationen sendet der stellvertretende Leitstellenleiter nur noch einen Download-Link per E-Mail an die Wehrführer. Dies ersetzt den aufwendigen Transport durch Kuriere, um aktualisierte Pläne zu den zuständigen Stellen zu bringen. Der E-Mail-Verkehr schied von vornherein aus, da die Datenmengen mit den Plänen für die neun Wehren und das detaillierte Kartenmaterial zu groß für den Versand sind.

Die Feuerwehren im Wittekindskreis können damit in den Wachen, aber auch direkt am Einsatzort, auf alle wichtigen Informationen zugreifen – diese werden nicht nur jederzeit von der Kreisleitstelle aktualisiert, sondern auch die Wehrführer und Einsatzleiter können wichtige Nachrichten schnell und unkompliziert hochladen und weitergeben. Dass die Daten dabei stets auf Viren überprüft werden, ist besonders wichtig, da die größtenteils ehrenamtlichen Wehrführer teilweise auch über ihre privaten Geräte arbeiten.

Die jüngsten Entwicklungen weisen darauf hin, dass der Einsatz einer sicheren Speichermöglichkeit immer wichtiger wird: Die massiven Spam-Angriffe der letzten Wochen zeigen zudem, dass die direkte E-Mail-Kommunikation an ihre Sicherheitsgrenzen stößt. Um den Risiken zu begegnen, musste der E-Mail-Verkehr samt Anhängen vielerorts über die übliche Überwachung hinaus radikal eingeschränkt werden. Eine Ablage von Daten an einem geschützten Speicherort, auf den nur verschlüsselt zugegriffen wird, präsentiert sich als eine sichere Alternative. ■

RALF MAXIM,
Geschäftsbereichsleiter Speichermanagement
und Service Desk, krz

FRANK LEHNERT,
Abteilungsleiter Revision,
Sicherheit und Datenschutz, krz

Informationssicherheit in der Öffentlichen Verwaltung

Als Angestellte im Öffentlichen Dienst oder eines KRITIS-Unternehmens [1] werden Sie vermutlich gerade dabei sein, Ihr eigenes Informations-Sicherheits-Management-System (ISMS) einzuführen. Das neue IT-Sicherheitsgesetz, das der Bundestag am 12.6.2015 verabschiedet hat und das am 24.7.2015 veröffentlicht wurde, zielt darauf ab, die Informationssicherheit in Deutschland zu erhöhen, und stellt dabei die Anforderung an die sogenannten KRITIS, bis Anfang 2018 ein ISMS einzuführen und dieses ISMS nach der ISO 27001 [2] zertifizieren zu lassen.

KRITIS-Sektoren

In § 2 Abs. 10 des IT-Sicherheitsgesetzes werden die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen als Kritische Infrastrukturen genannt. Weiterhin nennt das IT-Sicherheitsgesetz in § 8 Abs. 1 die Möglichkeit, Mindeststandards für die Sicherheit der Informationstechnik ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes zu erlassen. Bild 1 zeigt die Sektoren, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) nennt.

Sektoren kritischer Infrastrukturen

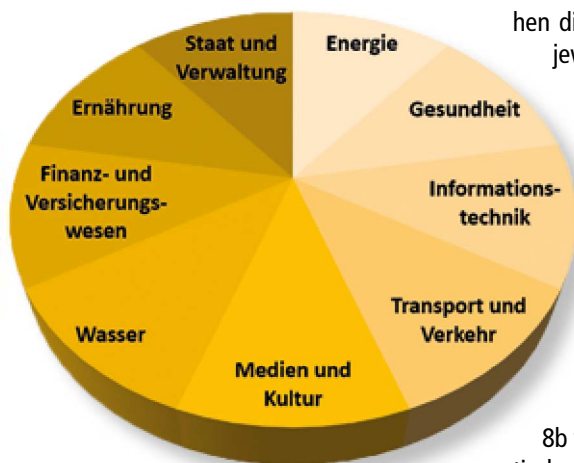


Bild 1: KRITIS-Sektoren nach BSI

Treffen erster Vorkehrungen

Neu hinzugekommen sind im IT-Sicherheitsgesetz die §§ 8a bis 8d. § 8a nennt die Pflicht der KRITIS zur Umsetzung von angemessenen organisatorischen und techni-

schen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse. Die Frist für die Umsetzung beträgt zwei Jahre nach Inkrafttreten der Rechtsverordnung [3]. Der Nachweis für die Erfüllung der Anforderungen kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Verordnung war beim Bundesministerium des Inneren (BMI) als Referentenentwurf ab 13.1.2016 einzusehen. Die Verordnung nennt eine 500.000er-Regel, nach der Unternehmen zu den KRITIS gehören, wenn jeweils 500.000 oder mehr Bürger von ihrer Leistung betroffen sind. Die Bewertungsskala der Verordnung kann beim BMI eingesehen werden. Aus ihr gehen die Schwellenwerte hervor, die für die jeweiligen Sektoren ausschlaggebend sind, ob eine Organisation zu den KRITIS gehört oder nicht. Man darf erwarten, dass die Schwellenwerte in den nächsten Jahren sukzessive herabgesetzt werden, um zukünftig die gesamte Infrastruktur in Deutschland sicherer zu machen.

Einrichten einer Meldestelle

Zurück zum IT-Sicherheitsgesetz: In § 8b wird gefordert, dass die Betreiber Kritischer Infrastrukturen dem BSI binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung eine Kontaktstelle für die Kommunikationsstrukturen benennen müssen. Diese Stelle muss jederzeit erreichbar sein. Die KRITIS haben dabei erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betrie-

benen Kritischen Infrastrukturen führen können oder bereits geführt haben, zu melden. Die Meldung muss Angaben zu der Störung und den technischen Rahmenbedingungen enthalten, ebenso die vermutete oder tatsächliche Ursache, die Art der betroffenen Einrichtung oder Anlage sowie die Branche des Betreibers. Das Gesetz gibt aber auch die Möglichkeit, dass Organisationen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. § 8c gibt an, dass die § 8a und § 8b nicht auf Kleinstunternehmen sowie kleine und mittlere Unternehmen anzuwenden sind.

Bußgeldkatalog

§ 14 ist ein weiterer neuer Paragraph, der die Bußgelder definiert. In § 14 heißt es, ordnungswidrig handelt, wer vorsätzlich oder fahrlässig die genannten Vorkehrungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft oder eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder eine Störungsmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. Diese Ordnungswidrigkeiten können mit Geldbußen zwischen fünfzigtausend und hunderttausend Euro geahndet werden.

Recht auf Erhebung von Nutzerdaten

Auch im Telekommunikationsgesetz gab es Änderungen. § 100 Abs. 1 gestattet nun dem Diensteanbieter, die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Einschränkungen der Verfügbarkeit von Informations- und Kommunikationsdiensten oder unerlaubter Zugriff auf Telekommunikations- und Datenverarbeitungssysteme werden als mögliche Störungen genannt.

Aufbau der ISO 27001:2013

Wenn Sie oder Ihre Kunden den KRITIS-Sektoren angehören, werden Sie nicht umhinkommen, ein ISMS in Ihrer Organisation einzuführen. Für Ihre ISMS-Einführung gibt es gute Nachrichten. Die ISO/IEC

27001:2013 basiert nämlich seit 2013 auf der neuen ISO High Level Structure [4]. Die International Organization for Standardization (ISO) hatte diese Struktur 2010 herausgegeben, um zukünftig eine leichtere Umsetzung unterschiedlicher Normen in einer Organisation zu ermöglichen. Bild 2 zeigt den Aufbau dieser High Level Structure. Alle ISONormen, die nach 2010 veröffentlicht werden, sind in dieses Schema eingepasst. Das bedeutet, die Normen haben gleiche Kapitel und nahezu identische Unterkapitel und Anforderungen. Unterschiede zeigen sich nur hinsichtlich der jeweiligen Ausprägungen einer bestimmten Norm. Siehe Bild 2.

Kommen wir nun zum Aufbau der ISO/IEC 27001:2013. Diese ISO-27001 ist in zehn Kapitel, wovon die ersten drei Kapitel der Einführung dienen, gegliedert. Nur die Kapitel 4 bis 10 haben normativen Charakter und werden bei einer ISO 27001-Zertifizierung geprüft. Weiterhin enthält die ISO 27001 einen Anhang A, der Maßnahmenziele und Maßnahmen enthält, die ebenfalls als Prüfungsgrundlage dienen. Diese Maßnahmenziele sind direkt aus der ISO 27002, Kap. 5-18 abgeleitet. Bild 3 zeigt Ihnen den Aufbau der ISO 27001, den Sie mit der ISO High Level Structure aus Bild 2 vergleichen können. Siehe Bild 3.

Die einzelnen Kapitel

Das Kapitel 4 KONTEXT DER ORGANISATION fordert, dass sich die Organisation Gedanken über ihren Sinn und Zweck macht. Sie muss sich bspw. die Fragen stellen: Welche Produkte oder Dienstleistungen bieten wir an? Womit positionieren wir uns auf dem Markt? Was unterscheidet uns von unseren Wettbewerbern? Was erwarten unsere Kunden von uns? In Kapitel 4.1 POSITIONIERUNG DER ORGANISATION muss die Organisation Themen auswählen, die ihr Kerngeschäft ausmachen. Also vor allem Prozesse, mit denen die Organisation ihr Geld verdient und die für die Informationssicherheit rele-



Bild 2: Aufbau der ISO High Level Structure



Bild 3: Aufbau der ISO 27001:2013

vant sind. Weiterhin soll die Organisation in Kapitel 4.2 INTERESSIERTE PARTEIEN alle Parteien, auch Stakeholder genannt, kennen und deren Anforderungen berücksichtigen. Diese interessierten Parteien sind in jedem Fall die Kunden, die Mitarbeiter und die Lieferanten. Darüber hinaus muss sie bei der Betrachtung der interessierten Parteien auch an eventuelle Kontakte zu Behörden denken. Anschließend muss die Organisation in Kapitel 4.3 ANWENDUNGSBEREICH klären, ob und wo sie das ISMS einführen möchte. Hat die Organisation nur einen oder mehrere Standorte? Soll das ISMS im ganzen Unternehmen, über alle Standorte oder nur in einem kleinen IT-Bereich eingeführt werden? Wenn alle diese Anfangsfragen beantwortet sind, kann die Organisation die Entscheidung fällen, ein ISMS einzuführen. Diese Entscheidung fällt in Kapitel 4.4 INFORMATIONSSICHERHEITSMANAGEMENT-SYSTEM.

Kapitel 5 FÜHRUNG nimmt die oberste Leitung in die Pflicht. Die oberste Leitung muss

in Kapitel 5.1 FÜHRUNG UND VERPFLICHTUNG die Verantwortung für das ISMS übernehmen und sich dazu verpflichten, die Einführung zu unterstützen. In Kapitel 5.2 POLITIK muss die oberste Leitung eine Politik, auch Strategie bezeichnet, vorgeben. In dieser Politik muss sie ihre Verpflichtung für Informationssicherheit gegenüber ihren Kunden, Mitarbeitern und Lieferanten klar dokumentieren. Im Kapitel 5.3 ROLLEN, VERANTWORTLICHKEITEN UND BEFUGNISSE muss sie Verantwortliche für das ISMS bestimmen. Sie muss also mindestens eine Person benennen, die sich um die ISMS-Einführung kümmert, und diese Person den Mitarbeitern bekannt machen. Diese Person muss mit den notwendigen Befugnissen ausgestattet werden, um Änderungen durchsetzen zu können. Ein Informationssicherheitsbeauftragter wird von der Norm nicht konkret gefordert, aber es ist sinnvoll, diese Rolle in der Organisation zu besetzen. Der Informationssicherheitsbeauftragte wird sich dann ähnlich einem Projektleiter um die ISMS-Einführung

kümmern und in Awareness-Schulungen [5] das Bewusstsein der Mitarbeiter für Informationssicherheit erhöhen. Weiterhin muss die oberste Leitung einen internen Auditor für die ISO 27001 benennen, der nach Einführung des ISMS regelmäßige interne Audits durchführen wird.

Bei der ISMS-Einführung ist das Kapitel 6 PLANUNG von allen Kapiteln das umfangreichste, trotz seiner wenigen Unterkapitel. Im Kapitel 6.1 MASSNAHMEN ZUM UMGANG MIT RISIKEN UND CHANCEN muss die Organisation ihre Themen aus Kapitel 4.1 und die Anforderungen der interessierten Parteien aus Kapitel 4.2 auf mögliche Risiken oder Chancen untersuchen. Diese Risikoanalysen sind in den meisten Fällen sehr umfangreich, zeitaufwendig und – vermutlich – nie erschöpfend. Außerdem muss die Organisation die möglichen Risiken im Zusammenhang mit den Maßnahmen aus Anhang A betrachten und analysieren. Ist die Organisation mit den Risikoanalysen und



Bild 4: Awareness-Veranstaltungen mit Dresdner IT-Unternehmen

der Bewertung der Maßnahmen aus Anhang A fertig, muss sie eine Erklärung der Anwendbarkeit (Statement of Applicability, SoA) erstellen, aus der hervorgeht, welche Maßnahmen aus Anhang A durch die Organisation nun tatsächlich umgesetzt werden. Erst durch die Ergebnisse der Risikoanalysen aus Kapitel 6.1 kann die Organisation in Kapitel 6.2 INFORMATIONSSICHERHEITZIELE Ziele bestimmen, die für sie tatsächlich relevant und sinnvoll sind. Dabei ist zu beachten, dass Ziele klar formuliert und messbar sein müssen. Ein mögliches Ziel wäre bspw. Im Jahr 2016 wird ein Mitarbeiter durch ISO-27001-Weiterbildung zum Informationssicherheitsbeauftragten befähigt. Ein anderes Ziel wäre bspw.: Bis März 2017 sind alle Telearbeitsplätze nur noch mit einem Laptop-Gerätetyp ausgestattet, um die Wartung zu vereinheitlichen und zu vereinfachen.

In Kapitel 7 UNTERSTÜTZUNG beginnt die tatsächliche Umsetzung der zuvor geplanten Ziele. Zuerst werden in Kapitel 7.1 RESSOURCEN die erforderlichen Ressourcen bereitgestellt. Ressourcen umfassen bspw. Finanzen für neue Hardware, Software und Weiterbildung sowie Personal. In Kapitel 7.2 KOMPETENZ werden die bereits vorhandenen Kompetenzen überprüft und fehlende aufgebaut. Ziel von Weiterbildungsmaßnahmen ist ein tieferes Wissen der Mitarbeiter im Bereich Informationssicherheit. Das Kapitel 7.3 BEWUSSTSEIN fordert, dass das Bewusstsein der Mitarbeiter für die Informationssicherheit erhöht wird. In Awareness-Schulungen wird sich in den meisten Fällen der Informationssicherheitsbeauftragte vor die Belegschaft stellen und in Vorträgen erläutern, welche Aspekte der Informationssicherheit zukünftig mehr beachtet werden sollen. Siehe Bild 4.

In Kapitel 7.4 KOMMUNIKATION geht es um die Kommunikationsketten. Hier steht die Anforderung, zu klären, wer wann mit wem worüber und wie kommunizieren muss. Wichtig ist hier, dass alle Mitarbeiter ihre jeweiligen Ansprechpartner kennen, mit denen sie im Notfall kommunizieren müssen. Kapitel 7.5 DOKUMENTIERTE INFORMATION fordert die Dokumentation und deren Lenkung. Gelenkte Dokumente haben einen Titel, einen Autor, einen Prüfer, einen Freigeber, eine Versionsnummer, ein Erstellungsdatum, ein Prüfdatum und ein Freigabedatum. In diesem Kapitel werden die Richtlinien erstellt, die von der ISO 27001 gefordert werden.

Das Kapitel 8 BETRIEB fordert die Umsetzung von Prozessen für die Risikoerkennung, Risikobeurteilung und -behandlung. In Kapitel 8.1 BETRIEBLICHE PLANUNG UND STEUERUNG müssen also Prozesse umgesetzt werden, die es den Mitarbeitern ermöglichen, Risiken zu erkennen und zu melden. In Kapitel 8.2 INFORMATIONSSICHERHEITSRISIKOBEURTEILUNG müssen den Mitarbeitern Möglichkeiten gegeben werden, um Risiken beurteilen zu können. Das kann in Form von Checklisten mit Risiko-Schwellwerten geschehen, in denen man anhand von Themen die Kritikalität abschätzen kann. Kapitel 8.3 INFORMATIONSSICHERHEITSRISIKOBEHANDLUNG fordert Maßnahmen, um bekannte Risiken zu behandeln. Dabei muss auch die Dokumentation von Risiken oder Sicherheitsvorfällen für spätere Auswertungen angefertigt werden.

Das Kapitel 9 BEWERTUNG DER LEISTUNG hat das Ziel, die eingeführten Prozesse dahingehend zu überprüfen, ob sie wirksam sind und so umgesetzt wurden, wie sie geplant waren. In Kapitel 9.1 ÜBERWACHUNG, MESSUNG, ANALYSE UND BEWERTUNG wird gefordert, dass die Organisation geeignete Mittel zur Bewertung einsetzt. Kapitel 9.2 INTERNES AUDIT fordert regelmäßige interne Audits. Dabei werden auch Richtlinien und Arbeitsanweisungen auf ihre Wirksamkeit überprüft. Wichtig ist, dass die Audits von unabhängigen Prüfern durchgeführt werden. Zu beachten ist auch, dass der Informationssicherheitsbeauftragte, der das ISMS einführt, das ISMS nicht selbst auditieren kann, da er gegenüber seiner Arbeit nie vollständig objektiv ist und nicht unparteilich prüfen kann. Die MANAGEMENTBEWERTUNG findet in Kapitel 9.3 statt. Dieses Kapitel fordert von der Ma-

nagement-Ebene, die Bewertungen, Analysen und internen Auditberichte zu überprüfen. Diese Managementbewertung sollte mindestens einmal im Jahr stattfinden.

In Kapitel 10 VERBESSERUNG werden die Ergebnisse aus Kapitel 9 überprüft und Entscheidungen zur weiteren Umsetzung des ISMS getroffen. Kapitel 10.1 NICHTKONFORMITÄTEN UND KORREKTURMASSNAHMEN fordert Entscheidungen zum Umgang mit Abweichungen. Und Kapitel 10.2 FORTLAUFENDE VERBESSERUNG hat das Ziel, im Rückblick auf bereits Bestehendes Verbesserungspotenziale zu finden und das ISMS zu optimieren.

Die ISO 27002 ist ein Standardwerk aus der ISO-27000er-Reihe, das die Best Practice für die Implementierung eines ISMS mit Maßnahmenzielen und Maßnahmen untersetzt. Für die in ISO 27002 genannten Maßnahmen existieren keine Verpflichtungen. Sie sind auch keine Grundlage für die Zertifizierung. Dennoch sollten Sie sich die Maßnahmen ansehen und entscheiden, ob die eine oder andere Maßnahme Ihr ISMS sicherer macht.

Der Anhang A der ISO 27001 enthält 14 informationssicherheitsrelevante Themen, die in unterschiedliche Maßnahmenziele untergliedert sind. Die Themen aus Anhang A wurden direkt aus der ISO 27002 abgeleitet. Bild 5 stellt den Zusammenhang zwischen ISO 27001 und ISO 27002 graphisch dar. Siehe Bild 5.

Bei der Einführung Ihres ISMS müssen Sie den Anhang A in Ihren Risikoanalysen, die in Kapitel 6.1.3 INFORMATIONSSICHERHEITSRISIKOBEHANDLUNG der ISO 27001 gefordert sind, mitbetrachten und bewerten. Die

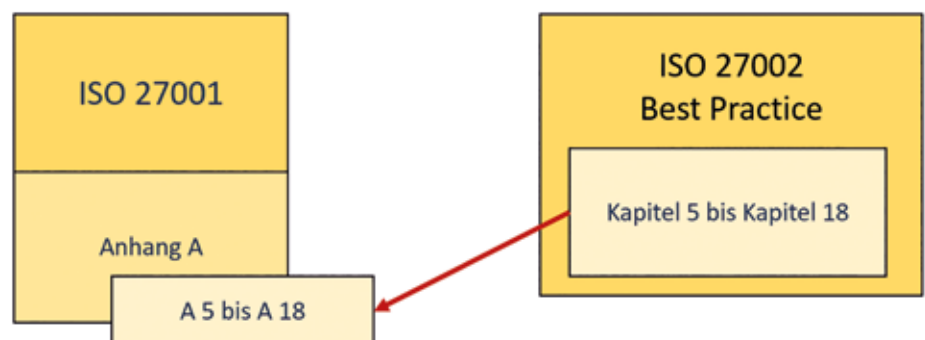


Bild 5: Zusammenhänge zwischen ISO 27001 und ISO 27002

Anforderungen, die der Anhang A dabei liefert, sind sehr allgemein. Wenn Sie kreativ genug sind, können Sie die geforderten Maßnahmen nach Ihrem Belieben umsetzen. In den meisten Fällen reichen die Formulierungen allerdings nicht aus, um eine Vorstellung zu gewinnen, welche Aspekte alle in einen Themenbereich fallen und ein ISMS sicherer machen.

Wer die ISO 27001 umsetzt, könnte sich natürlich in der Zertifizierung auf die allgemeinen Formulierungen berufen. Der Zertifizierung würde das nicht schaden. Allerdings ist Ihre Organisation dann mit so einem ISMS meist nicht wirklich sicherer als ohne dieses ISMS. Sie haben quasi Ihren aktuellen Stand dokumentiert und sind dabei eventuell nicht auf dem Stand der Technik.

Wenn Sie sichergehen möchten, dass Sie alle Aspekte der ISO-27000er-Reihe betrachtet haben, schauen Sie am besten in die ISO 27002 und prüfen sie die dort empfohlenen Implementierungsmaßnahmen.

Die nachfolgenden Informationssicherheitsthemen aus Anhang A sollen einen groben Überblick zu den jeweiligen Maßnahmen geben. Der Umfang der Darstellung ist keinesfalls erschöpfend.

In A5 der ISO 27001 wird ein Satz von INFORMATIONSSICHERHEITSRICHTLINIEN gefordert und deren regelmäßige Überprüfung und, wenn nötig, deren Aktualisierung. Unter dem Informationssicherheitsthema A6 befinden sich zwei Maßnahmenziele, zum einen die INTERNE ORGANISATION und zum anderen die Kombination aus MOBILGERÄTE UND TELEARBEIT.

Im Maßnahmenziel INTERNE ORGANISATION werden Maßnahmen aufgezählt, wie beispielsweise die Festlegung von Informationssicherheitsverantwortlichkeiten, die Aufgabentrennung und der Kontakt zu Behörden und speziellen Interessengruppen.

Das Maßnahmenziel MOBILGERÄTE UND TELEARBEIT fordert die Aufstellung von Richtlinien zum Umgang mit Mobilgeräten und zum Schutz von Informationen auf Mobilgeräten und am Telearbeitsplatz.

Das Informationssicherheitsthema A7 PERSONALSICHERHEIT gliedert sich in drei Be-

reiche. Hier geht es um Sicherheitsaspekte vor, während und nach der Beschäftigung.

Vor der Beschäftigung werden Sicherheitsüberprüfungen für neue Mitarbeiter empfohlen und vertragliche Vereinbarungen mit Beschäftigten, beispielsweise Vertraulichkeitsvereinbarungen in Arbeitsverträgen. Während der Beschäftigung werden alle Mitarbeiter auf die Umsetzung der gültigen Richtlinien verpflichtet. Außerdem werden Bewusstseinsschulungen durchgeführt, um den Mitarbeitern das relevante Informationssicherheitsbewusstsein verständlich zu machen. Weiterhin gilt ein Maßregelungsprozess, der den Mitarbeitern bekannt ist und der bei Informationssicherheitsverstößen zum Einsatz kommt. Für die Zeit nach der Beschäftigung sind ebenfalls Regelungen vorhanden. So müssen ausscheidende Mitarbeiter bspw. auf den Datenschutz und die Vertraulichkeit verpflichtet werden. Außerdem müssen dem ausscheidenden Mitarbeiter alle bisherigen Rechte im IT-System entzogen werden.

In A8 geht es um die VERWALTUNG DER WERTE der Organisation. Zuerst müssen die Werte inventarisiert und einem Mitarbeiter zugeordnet werden, der die Verantwortung für diese Werte übernimmt. Es müssen Regelungen zum ordnungsgemäßen Gebrauch von Werten und deren Rückgabe definiert werden. Für Werte wird außerdem eine Werteklassifizierung empfohlen. Anhand dieser Klassifizierung können Mitarbeiter Werte nach ihrer Kritikalität und Empfindlichkeit beurteilen und so sensibler mit kritischen Werten umgehen. Weiterhin wird ein definierter Umgang mit Datenträgern empfohlen. Die Maßnahmen richten sich hierbei an Mitarbeiter zur Handhabung, Entsorgung und den Transport von Wechsel-datenträgern.

A9 fordert, durch eine ZUGANGSSTEUERUNG den Zugang zu Informationen und informationsverarbeitenden Einrichtungen einzuschränken, und nennt als Maßnahmen die Erstellung einer Zugangssteuerungsrichtlinie und die Beschränkung des Netzzugangs für ausgewählte Mitarbeiter. Weiterhin soll es einen Prozess für die Benutzerregistrierung und Deregistrierung geben.

Die Mitarbeiter müssen sich außerdem der Verantwortung ihrer geheimen Authentisierungsinformationen bewusst sein und diese

geheim halten. Der Zugang zu Systemen und Anwendungen muss darüber hinaus durch sichere Anmeldeverfahren abgesichert werden.

In A10 geht es um KRYPTOGRAPHIE. Dort, wo es sinnvoll ist, sollen kryptographische Maßnahmen zum Einsatz kommen. Auch hier wird eine Richtlinie erwartet. Diese soll den Gebrauch von kryptographischen Schlüsseln und deren Verwaltung regeln.

A11 Physische und umgebungsgebundene Sicherheit ist ein sehr umfangreiches Informationssicherheitsthema mit zwei Maßnahmenzielen. Zum einen sollen hier die SICHERHEITSBEREICHE und zum anderen die GERÄTE UND BETRIEBSMITTEL geschützt werden. Für die Sicherheitsbereiche gilt, dass sie vor unbefugtem Zutritt und vor externen oder umweltbedingten Bedrohungen geschützt werden. Die Geräte und Betriebsmittel sollen so geschützt werden, dass sie ohne Unterbrechung arbeiten können. Das bedeutet, sie müssen richtig platziert werden, ihre Versorgungseinrichtungen müssen bspw. vor Stromausfällen und die Verkabelungen müssen gegen Beschädigung geschützt sein. Das Entfernen von Werten muss unterbunden werden. Arbeitsumgebungen müssen vor unbefugtem Zugriff geschützt sein.

Bei der BETRIEBSSICHERHEIT in A12 geht es darum, einen ordnungsgemäßen Betrieb ohne Unterbrechungen zu gewährleisten. Das heißt, Nachfolger oder Vertreter können durch geeignete Dokumentation Arbeitsaufgaben zeitnah übernehmen, alle Änderungen werden gesteuert. Die benötigten Kapazitäten werden überwacht und sichergestellt. Und es besteht eine Trennung zwischen Entwicklungs-, Test- und Betriebsumgebungen. Weiterhin bestehen ein Schutz gegen Schadsoftware und ein Prozess zur Datensicherung. Ereignisse werden protokolliert und die Protokollinformationen vor Manipulationen geschützt. Zuletzt wird auch die Maßnahme genannt, die Geschäftsprozesse während der Audit-Tätigkeiten zu schützen.

A13 KOMMUNIKATIONSSICHERHEIT gibt Maßnahmen vor, die sich auf die Übermittlung von Informationen beziehen. Hier geht es vor allem um die Sicherheit bei der Übertragung in Netzwerken und die Einhaltung von Geheimhaltungsvereinbarungen.

A14 nennt Maßnahmen, die durchgeführt werden sollen, wenn Organisationen externe Leistungen beschaffen. Es geht hier um ANSCHAFFUNG, ENTWICKLUNG UND INSTANDHALTUNG. Zuerst sollen die Organisationen dabei ihre eigenen Anforderungen analysieren, um festzustellen, was eigentlich gebraucht wird, und erst danach soll nach Leistungen auf dem Markt gesucht werden. Leistungen, die durch die Organisation ausgelagert werden, müssen ebenfalls den eigenen Anforderungen genügen. Dabei sollen die Organisationen die Sicherheit in öffentlichen Netzen und den Schutz von Transaktionen betrachten.

Bei Entwicklungstätigkeiten soll das Thema Informationssicherheit im gesamten Produktlebenszyklus integriert sein. Dabei wird auch der Schutz der Testdaten gefordert.

Bei den LIEFERANTENBEZIEHUNGEN in A15 geht es in erster Linie um die vertraglichen Aspekte. In den Verträgen mit Lieferanten muss das Thema Informationssicherheit eingearbeitet sein. Diese Verträge müssen regelmäßig überprüft werden und bei Bedarf an das neue Informationssicherheitsniveau der Organisation angepasst werden. Für die Lieferkette gilt, dass die Lieferanten die Anforderungen der Organisation kennen müssen. Anschließend muss die Organisation die Lieferantendienstleistungen überwachen und Änderungen steuern.

Für die HANDHABUNG VON INFORMATIONSSICHERHEITSVORFÄLLEN muss es Verantwortliche geben, die von Mitarbeitern im Notfall informiert werden können. Weiterhin sind Prozesse zu etablieren, anhand derer man Risiken erkennen, beurteilen und behandeln kann. Alle Informationssicherheitsereignisse müssen geeignet gemeldet werden und die Beweismittel müssen aufbewahrt werden.

Ziel dieses Informationssicherheitsthemas ist die Notfallplanung für Krise oder Katastrophe. Die Maßnahmen nennen Umsetzungsmöglichkeiten, beispielsweise Dokumentationen, Prozesse und Verfahren, die vorhanden sein sollten, um im Notfall den Betrieb schnell wieder starten zu können. Hierzu zählt bspw. auch, dass es Kontaktlisten für Ansprechpartner diverser IT-Systeme gibt, die im Notfall zeitnah kontaktiert werden müssen. Als weitere Maßnahme in A17 wird der Aufbau von Redundanzen genannt.

Bei A18 COMPLIANCE geht es um die Einhaltung von gesetzlichen und vertraglichen Anforderungen. Hierzu zählt auch die Einhaltung der Anforderungen aus den Richtlinien der Organisation. A18 fordert außerdem die regelmäßige unparteiliche Überprüfung des ISMS auf dessen Wirksamkeit und Einhaltung der Gesetzlichkeiten.

Auch die empfohlenen Maßnahmen aus der ISO 27002 sind recht allgemein gehalten, aber sie geben einen breiten Überblick über

mögliche Aspekte, die man eventuell vergessen würde. Nun werden Sie vermutlich feststellen, dass Sie durch die empfohlenen Maßnahmen aus der ISO 27002 Ihre Themen gut eingrenzen können, aber doch nicht vollständig technisch oder organisatorisch zum Leben erwecken können. An dieser Stelle empfehle ich einen gezielten Blick in den BSI IT-Grundschutz.

BSI IT-Grundschutz

Der BSI IT-Grundschutz ist mit Stand 2016 in 5 Bausteine (B) gegliedert, welche den Themen angehören: B1 Übergreifende Aspekte, B2 Infrastruktur, B3 IT-Systeme, B4 Netze und B5 Anwendungen. Desweiteren hat der IT-Grundschutz 6 Gefährdungskataloge (G) erstellt. Zu diesen gehören: G0 Elementare Gefährdungen, G1 Höhere Gewalt, G3 Organisatorische Mängel, G4 Menschliche Fehlhandlungen, G5 Technisches Versagen und G6 Vorsätzliche Handlungen.

Zuletzt sollen die Maßnahmenkataloge (M) genannt werden, welche in die Themen M1 Infrastruktur, M2 Organisation, M3 Personal, M4 Hardware und Software, M5 Kommunikation und M6 Notfallvorsorge unterteilt sind.

Bild 6 zeigt die BSI IT-Grundschutz-Kataloge mit Stand 2016. Die Abbildung soll zeigen, dass für jeden Baustein alle Gefährdungen möglich sind und diesen mit den Maßnahmen aus allen Maßnahmenkatalogen begegnet werden kann.



Bild 6: BSI IT-Grundschutz Stand 2016

Tabelle 1 zeigt Ihnen den Umfang der Kataloge mit Stand 2016. Es wird ersichtlich, dass es stellenweise mehrere hundert Elemente für ein Thema gibt. Die ältesten Elemente stammen aus dem Jahr 2009, die jüngsten aus 2014. Die Kataloge sind nicht mehr fortlaufend vorhanden, da regelmäßig Bausteine, Gefährdungen oder Maßnahmen aufgehoben werden.

Es macht bei der ISMS-Einführung keinen Sinn, alle Maßnahmen des BSI von oben nach unten in der Organisation zu implementieren. Vielmehr sollte man anhand der ermittelten Themen, die sich aus den Maßnahmen der ISO 27002 ergeben haben, gezielt nach IT-Grundschutz-Maßnahmen suchen und diese nach Überprüfung übernehmen.

Weiterhin würde eine komplette Übernahme aller IT-Grundschutz-Maßnahmen dazu führen, dass kein Prozess hinter den Maßnahmen steht. Ein fehlender Prozess führt in den meisten Fällen dazu, dass am Ende die Mitarbeiter stark überfordert sind und das ISMS nicht wirksam arbeitet. Die ISO empfiehlt deshalb ab 2010, Managementsysteme über die ISO High Level Structure mit dem PDCA-Zyklus einzuführen und am Leben zu halten.

Der PDCA-Zyklus

Die neue ISO High Level Structure beruht auf dem PDCA-Zyklus [6], was die Einfüh-

rung eines ISMS-Managementsystems erleichtert. Eine kurze Erläuterung zum Aufbau und zur Wirkungsweise des PDCA-Zyklus:

Das ‚P‘ steht für PLAN und beinhaltet alle Tätigkeiten, die zur Planung eines ISMS, so bspw. Sicherheitsprozesse und -ziele, gehören. Die Kapitel 4 bis 6 der ISO 27001 gehören der PLAN-Phase an.

Das ‚D‘ steht für DO und konzentriert sich auf die Umsetzung der zuvor geplanten Prozesse, Ziele, Produkte oder Dienstleistungen. Die Kapitel 7 und 8 der ISO 27001 gehören der DO-Phase an.

Das ‚C‘ steht für CHECK und hat den Kerninhalt, zu prüfen, ob die eigentliche Umsetzung gemäß der Planung erfolgte. Hier spielen bspw. auch interne Audits eine Rolle. Das Kapitel 9 gehört der CHECK-Phase an.

Das ‚A‘ steht für ACT und verlangt Entscheidungen, ob und wie Verbesserungen durchgeführt werden sollen. Leistungsstarkes und Wirksames soll dabei erhalten oder verbessert und Fehlerhaftes korrigiert oder zukünftig verhindert werden. Bild 7 stellt die Normen-Kapitel je Umsetzungsphase graphisch dar. Das Kapitel 10 gehört der ACT-Phase an. Siehe Bild 7.

Der PDCA-Zyklus stellt einen rotierenden Kreislauf während der ISMS-Einführung und

der anschließenden Aufrechterhaltung dar. Es wird somit von Ihnen nicht erwartet, dass Ihr ISMS nach seiner Einführung kein weiteres Verbesserungspotenzial mehr aufweist. Im Gegenteil, es ist im PDCA-Zyklus vorgesehen, dass Sie die Verbesserung Ihrer Prozesse und eingeleiteten Maßnahmen kontinuierlich aufrechterhalten und einen KVP, also einen kontinuierlichen Verbesserungsprozess, einführen.

Das bedeutet, Sie müssen nicht in Sorge geraten, wenn Sie zu Beginn der ISMS-Einführung noch nicht alle Anforderungen erfüllen können, denn nach jeder Iteration wird in der CHECK-Phase ein Review durchgeführt und in der ACT-Phase entschieden, was im nächsten Durchlauf verbessert werden soll.

Ihre ISMS-Einführung

Die ISMS-Einführung sollten Sie als internes Projekt auslegen. Projekte kosten meist viel Geld, sind auf einen beschränkten Zeitraum geplant, führen zu einem neuen Produkt oder einer neuen Dienstleistung und tragen ein gewisses Risiko des Scheiterns in sich.

Wenn Sie bereits sehr prozessorientiert arbeiten und dabei mit dem Thema Informationssicherheit bewusst umgehen, lohnt sich zu Beginn eine GAP-Analyse. In einer GAP-Analyse gehen Sie oder Ihr Berater einfach Anforderung für Anforderung durch die ISO 27001 und gleichen ab, ob Sie die eine oder andere Anforderung bereits erfüllen. Im Anschluss haben Sie einen Überblick über den Umfang an Ressourcen und Kompetenzen und auch über den zeitlichen Aufwand, den Sie einplanen müssen, um die noch fehlenden Anforderungen umzusetzen. Im nächsten Schritt bearbeiten Sie Kapitel für Kapitel die Norm-Anforderungen.

Zu Beginn Ihrer ISMS-Einführung müssen Sie in der PLAN-Phase festlegen, wohin die

Liste Bausteine		Liste Gefährdungen		Liste Maßnahmen	
B1	B1.0 – B1.17	G0	G0.1 – G0.46	M1	M1.1 – M1.80*
B2	B2.1 – B2.12	G1	G1.1 – G1.19	M2	M2.1 – M2.558*
B3	B3.101 – B3.406*	G2	G2.1 – G2.201*	M3	M3.1 – M3.96*
B4	B4.1 – B4.8	G3	G3.1 – G3.123*	M4	M4.1 – M4.469*
B5	B5.1 – B5.25*	G4	G4.1 – G4.99*	M5	M5.1 – M5.177*
		G5	G5.1 – G5.194*	M6	M6.1 – M6.159*

Tabelle 1: Überblick BSI IT-Grundschutzkataloge (*einige Elemente der Reihe wurden aufgehoben)



Bild 7: PDCA-Zyklus

Reise gehen soll. Wie wollen Sie Ihre Mitarbeiter zur Informationssicherheit erziehen? Welche Anforderungen kommen dabei von Ihren Kunden? Welche Anforderungen stellen Sie an Ihre Lieferanten? Diese Phase wird auch als GOVERNANCE bezeichnet.

Für Kapitel 4 und 5 sind in der Regel keine externen Berater nötig, da die Organisationen meist am besten wissen, welche Aufgaben sie nach außen hin vertreten und wer zur Gruppe der Stakeholder gehört. Auch die Politik und die Benennung von Verantwortlichen kann von der Organisation selbstständig durchgeführt werden.

Ab Kapitel 6 wird es für einen internen Mitarbeiter, der das ISMS neben seinen Linienaufgaben einführt, schwer, die Einführungsarbeiten in einer angemessenen Zeit umzusetzen. Wenn Sie Ihre Themen definiert haben, die aus Ihrer Sicht eine Rele-

vanz für die Informationssicherheit haben, müssen Sie etwa 1-2 Tage für eine Risikoanalyse je Thema einplanen. Zusätzlich müssen Sie die Maßnahmenziele aus dem Anhang A für alle Ihre Themen ebenfalls einer Risikoanalyse unterziehen, um sicherzugehen, dass Sie kein offensichtliches Risiko übersehen. Planen Sie also etwa 3-5 Monate für die Umsetzung von Kapitel 6 ein.

Wenn Sie Ihre Risiken und Ziele kennen, können Sie mit der Umsetzung der Richtlinien beginnen. Eine Richtlinie sollte einen Titel, den Geltungsbereich, das Verhalten bei Informationssicherheitsvorfällen und die Verantwortlichkeiten beinhalten. Die Richtlinien müssen außerdem gelenkt werden. Das bedeutet, dass die Richtlinie vor ihrer Veröffentlichung von einer zweiten Person geprüft und freigegeben werden muss. Und die Richtlinie muss eine Versionsnummer besitzen und den Mitarbeitern zugänglich sein.

Der Inhalt einer Richtlinie richtet sich nach dem Wert, der mit dieser Richtlinie geschützt werden soll. Wenn bspw. Mobilgeräte geschützt werden sollen, muss die Richtlinie alle Aspekte beinhalten, die dem Schutz von Mobilgeräten dienen können. Es hat sich dabei als hilfreich gezeigt, bei der Erarbeitung von Richtlinien gezielt an dieser Stelle auch im BSI-Grundschutzkatalog nachzulesen, welche Maßnahmen vom BSI für die jeweiligen Themen vorgeschlagen werden. In der Richtlinie müssen die Mitarbeiter angesprochen werden.

Bei der Einführung eines ISMS sollten regelmäßige Treffen der Verantwortlichen stattfinden. In größeren Organisationen ist die Etablierung eines Informationssicherheitszirkels/IT-Sicherheitskreis sinnvoll.

Welche Themen müssen Sie außerdem beachten? Sie müssen die notwendigen Kom-



DEDICATED TO SOLUTIONS

CYBER SECURITY & INTELLIGENCE: Security integrated.

Digitalisierung und Vernetzung benötigen zuverlässige Informations- und Kommunikationssysteme und sind Schlüsselfaktoren für eine funktionierende Verteidigung, Sicherheit, Wirtschaft und Verwaltung.

Mit dem Anspruch „Security made in Germany“ bietet die ESG die erforderlichen Kompetenzen und Fähigkeiten in einem starken Team:

- ▶ Cyber-/IT-Services
- ▶ Cyber Training Center
- ▶ ESG Cyber Labs
- ▶ Center of Cyber Security Excellence
CCSE Partnernetzwerk

WWW.ESG.DE / WWW.CCSE.ESG.DE
WWW.CYBERTRAINING.ESG.DE

petenzen für Informationssicherheit aufbauen, Sie müssen mittels Awareness-Schulungen Ihre Mitarbeiter für Informationssicherheit sensibilisieren, Sie müssen die Kommunikationsketten definieren und Ihre Dokumentation lenken.

Weiterhin müssen Sie Prozesse einrichten, mit denen Sie Informationssicherheitsverstöße erkennen, beurteilen und behandeln können. Diese Phase wird als RISK MANAGEMENT bezeichnet.

Die Überprüfung der Einhaltung von Regelungen und Gesetzen wird auch COMPLIANCE genannt.

Bei Ihnen bedeutet das, dass Sie einen internen Auditor benennen müssen, der in regelmäßigen Abständen bspw. Ihre Richtlinien überprüft und bewertet, ob diese Richtlinien der aktuellen Gesetzeslage entsprechen und ob die Mitarbeiter sich an diese Richtlinien halten. Darüber hinaus muss der Auditor Ihr IT-System prüfen. Dazu ist Berufserfahrung in der IT unerlässlich. Die Ergebnisse der Audits fließen in einen Auditbericht ein und werden der obersten Leitung zur Prüfung übergeben.

In der Managementbewertung wird die oberste Leitung die Ergebnisse aus den Audits für die Neujustierung des ISMS verwenden und neue Informationssicherheitsziele vorgeben. Durch die neuen Zielvorgaben wird die PLAN-Phase bzw. GOVERNANCE wiederholt angestoßen und das ISMS kontinuierlich verbessert.

Risiken bei der ISMS-Einführung

Eine falsche Reihenfolge, beispielsweise die ISMS-Einführung mit BSI-Maßnahmen zu starten, kann dazu führen, dass Ihr ISMS über viele Jahre lang eingeführt werden

muss, da Sie sich nicht fokussieren können. Ein weiteres Risiko besteht darin, dass die oberste Leitung die Verantwortung für die ISMS-Einführung vollständig einem Mitarbeiter überträgt und sich selbst komplett heraushält. Dieses Vorgehen kann dazu führen, dass keine einzige Maßnahme von anderen Mitarbeitern akzeptiert und angewendet wird. Das ISMS wird so nie vollständig eingeführt.

Ein personelles Risiko kann bestehen, wenn ausgebildete Fachkräfte in den Bereichen ISMS und interne Audits die Organisation verlassen und keine Vertreter aufgebaut wurden. Auch die finanziellen Ressourcen können zu einem Risiko werden, wenn beispielsweise nicht in sichere Hardware oder Software, in externe Beratung oder interne Weiterbildung investiert werden kann.

In den meisten Bundesländern gibt es für informationssicherheitsrelevante Projekte Fördertöpfe des Bundes. Die Beantragung muss schriftlich bei der jeweiligen Förderbank erfolgen. Die Prüfung und Bearbeitung dauert in der Regel etwa 8 Wochen. Bis zur Entscheidung der Förderbanken darf das Projekt natürlich noch nicht begonnen werden, was wiederum ein zeitliches Risiko birgt.

Wenn Sie jetzt mit der ISMS-Einführung beginnen möchten oder müssen, klären Sie intern alle Verantwortlichkeiten und machen Sie die Entscheidung zur Einführung eines ISMS in einer Mitarbeiterversammlung allen bekannt.

Holen Sie sich bei allen Themen immer die richtigen Ansprechpartner aus den jeweiligen Fachabteilungen hinzu, die Ihnen die aktuelle Umsetzung in der Organisation erklären können. So können Sie schnell entscheiden, an welchen Stellen Sie externe

Berater benötigen, und diese ganz gezielt für ISO-27001-Themen beauftragen. ■



JACQUELINE NAUMANN,
M.Sc. Praktische Informatik, Information Security Officer (TÜV), Information Security Auditor (TÜV), Qualitätsmanagementbeauftragte (TÜV)

Frau Naumann ist Dozentin, Beraterin & Auditorin für Informationssicherheit und Qualitätsmanagement.

Sie ist seit 2015 Inhaberin der iXactly IT- und Systemberatung Naumann. Zuvor hat sie über 16 Jahre in der IT-Branche gearbeitet und bspw. als Projektmanagerin für die Stadt Dresden das SAP-SD-Modul in den Fachämtern und das Dresdner Kitaplatz-Vergabesystem eKita eingeführt.

Ihre langjährigen Erfahrungen in der IT-Branche fließen in ihre Seminar- und Beratungstätigkeiten ein. Sie ist Expertin in den Bereichen ISO 27001, ISO 9001, Dokumentation, Softwareentwicklung, Datenbanken, SAP®, Testmanagement, Projektmanagement, Berechtigungsmanagement sowie Change- und Releasemanagement.

Sie ist vom TÜV Süd zertifizierte Qualitätsmanagementbeauftragte (QMB-TÜV, ISO 9001:2015), zertifizierter Information Security Officer sowie Information Security Auditor (ISO 27001:2013) und seit 2016 Vertragspartnerin der TÜV Süd.

Frau Naumann ist Autorin des Fachbuches „Praxisbuch eCATT“ (Verlag: Rheinwerk-Verlag (ehem. Galileo Press), 2009)

Fußnoten

- [1] Organisationen mit kritischen Infrastrukturen und wesentlicher Bedeutung für das staatliche Gemeinwesen, Betreiber von Kritischen Infrastrukturen
- [2] ISO 27001: ISO 27001:2013 Norm für Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen, Original-Ausgabe 2013, deutsche Ausgabe 2015
- [3] Verordnung Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
- [4] ISO High Level Structure: übergeordnete Struktur, um zukünftige ISO-Normen zu vereinheitlichen und gemeinsame Kernthemen vorzugeben
- [5] Bewusstseins-Schulungen für Informationssicherheit
- [6] P: PLAN/Planung, D: DOI/Umsetzung, C: CHECK/Überprüfung, A: ACT/Entscheidung

I ran some Ransomware – warum Erpressungstrojaner so gefährlich sind

Auch wenn nicht allen Nutzern Ransomware ein Begriff ist, verrät das deutsche Pendant „Erpressungstrojaner“ recht schnell, worum es sich handelt: zum einen um klassische Erpressung und zum anderen um Malware, genauer gesagt Trojaner. Warum ist das für den öffentlichen Dienst entscheidend? Allein die jüngsten Vorfälle in zwei nordrhein-westfälischen Kliniken zeigen deutlich, dass Ransomware längst nicht mehr nur Privatanwender im Visier haben. Abgesehen von finanziellen und Imageschäden ist in Zeiten vernetzter Rechner und anderweitiger Geräte ein Komplettausfall des Krankenhausbetriebs eine mehr als ernste Sache. Die Rückkehr ins analoge Arbeitsleben und damit zu Stift und Zettel führt zu mehr Belastung und Zeitaufwand. Darüber hinaus ist in dieser Situation kaum abzusehen, welche langwierigen Folgen so ein Zwischenfall tatsächlich nach sich zieht.

Ransomware-Angriffe sind unter Kriminellen zu einem funktionierenden Geschäftsmodell geworden. Dies lässt sich an den unzähligen Varianten von Malware-Familien ablesen. Im Gegensatz zu zielgerichteten Angriffen, so genannten Advanced Persistence Threats (kurz: APTs) ist das einzelne Opfer für den Angreifer persönlich uninteressant. Wichtig für ihn ist nur, dessen Daten als virtuelle Geiseln zu nehmen, und zwar solche, die dem betroffenen Anwender oder Unternehmen wertvoll genug sind, dafür ein Lösegeld zu zahlen.

Ransomware ist kein neues Phänomen

Grundsätzlich gibt es mehrere Arten an Ransomware, die abhängig vom Betriebssystem unterschiedlich arbeiten. Sie lassen sich in zwei Hauptkategorien einteilen: sogenannte „Crypto-Malware“ (Verschlüsse-

lung) und „Locker“ (Sperrung). Die digitale Erpressungsmasche ist allerdings alles andere als neu. Schon 1989 versteckte sich ein Schädling namens AIDS unter DOS-Dateien und verschlüsselte sie. Anschließend verlangte der Angreifer ein Lösegeld für den Entsperrcode zur Rückgabe der Daten.

In den letzten fünf Jahren ließen sich neue Angriffswellen beobachten, anfangs geprägt von sogenannten „Screenlockern“, die den Zugriff auf das System sperren. Sie erscheinen in vielen Fällen als bildschirmüberlagernde „Warntafeln“ mit der vermeintlichen Nachricht einer Strafverfolgungsbehörde. Darin steht, dass sich auf dem Gerät des Nutzers urheberrechtlich geschützte oder pornografische Inhalte befänden. Mit Zahlung einer Strafgebühr von rund 100 Euro würden keine strafrechtli-

chen Schritte gegen ihn eingeleitet. In einigen Fällen wurden auch Webcam-Bilder hinzugefügt, um den Druck auf das Opfer zu erhöhen. Noch vor ein paar Jahren waren Bezahlmethoden über Ukash und Paysafe Card Codes der Klassiker, mittlerweile wird zum Transfer des Lösegelds auch die bequeme Zahlung per Kreditkarte angeboten.

Erfolg durch Weiterentwicklung

Die Masche hatte Erfolg und entwickelte sich zunehmend zum Kassenschlager – bis heute. Mit dem Unterschied, dass Malware-Autoren immer raffiniertere und komplexere Schädlinge in Umlauf bringen. Zum Beispiel hatte Screenlocker für Windows oder Mac OS X aus Sicht des Angreifers den Nachteil, dass sich die Malware relativ leicht und mit technisch überschaubarem Aufwand entfernen ließ. Aus diesem Grund rückten Verschlüsselungstrojaner mehr und mehr in den Fokus der Kriminellen. Zu einem der bekanntesten Beispielen zählt „CryptoLocker“, der 2013 zum ersten Mal auftauchte und den Hintermännern mit einer implementierten Lösegeldzahlung über Bitcoins, im Gegensatz zu den bisherigen (und womöglich nachweisbaren) Bezahlmethoden, neue Wege eröffnete. Auch die weiterhin kursierenden Screenlocker zogen nach und übernahmen das Zahlungsmodell – aus zwei einfachen Gründen: Zum einen ist es viel schwerer bis fast unmöglich, die

Malware-Autoren solcher Kampagnen ausfindig zu machen, zum anderen lassen sich Nutzer mit einer Lösegeldforderung von einem Bitcoin im Gegensatz zu 200 Euro weitaus schneller ködern, obwohl sie am Ende den gleichen Preis zahlen.

Weltweite Opfer

Dass von solchen Ransomware-Angriffen auch öffentliche Einrichtungen betroffen sind, zeigen internationale Berichte. 2013 überwies eine Polizeidienststelle in Swansea/USA Bitcoins im Wert von 750 US-Dollar für einen verschlüsselten Computer und sah von einer Verfolgung der Angreifer ab. Von einer anderen Polizeistation in Midlothian/USA erbeuteten Kriminelle 2015 606 US-Dollar Lösegeld. Meldungen aus diesem Jahr zeigen allerdings, dass es sich hier um kein rein US-amerikanisches Problem handelt. Die Stadtverwaltung Dettelbach in Unterfranken erlitt finanzielle Einbußen von 490 Euro, nur um einen Bruchteil an Daten wiederherstellen zu können. In Bayern wurde eine Behörde mit 1.900 Mitarbeitern Opfer eines Ransomware-Angriffs, der einen geschätzten Schaden von circa 500.000 Euro verursachte. Auch das Innenministerium in Nordrhein-Westfalen war Anfang des Jahres betroffen und ging aus Angst vor Datenverlust auf die Lösegeldforderung ein.

Warum ist Ransomware so erfolgreich?

Die Gründe für den Erfolg von Ransomware sind relativ einfach. Mittlerweile hat sich eine rege Untergrundszene etabliert, die im sogenannten Darkweb die Entwicklung, das Pflegen und den Verkauf von Malware sowie der nötigen Infrastrukturen in professioneller Arbeitsteilung vorantreibt. Es gibt Spezialisten, die den Schadcode entwickeln, der anschließend über kriminelle Distributionen zum Kauf oder zur Miete inklusive Infrastruktur angeboten wird – von Adresslisten und Spam-Bots bis hin zu ganzen Serverstrukturen. So befremdlich es an dieser Stelle klingen mag, doch das Ganze ist weder neu, speziell oder gefährlicher als alle anderen Malware-Varianten, die täglich in hunderttausendfacher Ausführung auftauchen.

Das Gefährliche daran besteht vor allem in mangelnden oder schlecht umgesetzten Sicherheitskonzepten der zahlreichen Betroffenen. Ein aktuelles und regelmäßig aktualisiertes Antivirenprogramm kann vor

solchen Angriffen schützen – allerdings nicht ohne weitere Vorkehrungen und nie zu einhundert Prozent. Ist ein Angriff erfolgreich und sind die Daten einmal verschlüsselt, bestehen kaum Chancen, sie „auf eigene Faust“ wiederherzustellen. Auch wenn es Fälle gab, bei denen Crypto-Trojaner entschlüsselt wurden, dauerte dies Tage und Wochen. Darüber hinaus ist die Methode nicht immer zuverlässig und funktioniert nur geschätzt in einem von fünf Fällen. Hinzu kommt, dass Ransomware nicht nur eine Bedrohung für klassische Endpunkte wie Server und PC mit Windows-Betriebssystemen ist, sondern auch vermeintlich sichere Systeme wie Linux oder Mac OS X immer wieder erfolgreich angreift. Dies wird besonders dann zu einem Problem, wenn auf Schutzmaßnahmen wie einen Virenschutz verzichtet wurde, diese Geräte aber ein gleichwertiger Teil des Netzwerks sind. Dies gilt zum Beispiel für Smartphones und Tablets, die in der Vergangenheit bei Sicherheitskonzepten häufig vernachlässigt wurden. Doch schon seit 2014 kursieren Ransomware-Varianten auch für Android-Geräte. Auf ihnen sind ebenfalls wichtige Daten gespeichert – in Krankenhäusern unter anderem digitale Patientenakten –, von persönlichen Kontakten und Nachrichten je nach Gerätetyp und -einsatz ganz abgesehen. Dabei ist die Absicherung von Smartphones und Tablets heutzutage nicht umständlicher als bei den klassischen Geräten.

Was also tun?

Regelmäßige Backups der Systeme sind eine simple, aber effektive Methode, um Daten vor Ransomware und anderem Schadcode zu schützen. Da Malware auch Dateien auf Netzlaufwerken verschlüsseln kann, kommen alle externen Laufwerke wie USB-Sticks sowie andere Netzwerk- oder Cloudspeicher hinzu. Die Erstellung solcher Sicherheitskopien sollte allerdings in einem separaten Gerät erfolgen, um die Daten getrennt von den Produktivnetzen zu speichern. Darüber hinaus ist es entscheidend, die Wiederherstellung von Daten in regelmäßigen Abständen zu testen, um im Fall der Fälle schneller und routinierter reagieren zu können.

Veraltete Software ist eine der häufigsten Schwachstellen der IT. Angreifer nutzen bekannte Sicherheitslücken aus und greifen so unbemerkt auf Firmengeräte und -systeme zu. Regelmäßige Patches und Updates der verwendeten Software und Geräte erhöhen den Schutz gegen Ransomware um ein Vielfaches. In diesem Fall – wenn möglich – schafft die Aktivierung automatischer Updates oder ein Besuch auf der Webseite des Anbieters Abhilfe.

Eines der schwächsten Glieder in der Sicherheitskette ist der Mensch. Betrüger wenden oft sogenannte Social-Engineering-Methoden an, um Mitarbeiter zur Preisgabe von



vertraulichen Informationen und zur Ausführung schädlicher Programme zu bewegen. Gefälschte E-Mails von Lieferunternehmen oder Banken und als interne E-Mails getarnte Nachrichten sind Klassiker, um Angestellte zu täuschen. Schulungen und Trainings erhöhen das Sicherheitsbewusstsein und zeigen der Belegschaft, wie sie verdächtige E-Mails erkennen und mit darin enthaltenen Anhängen oder Links vorsichtig umgehen kann.

Ransomware wird häufig als E-Mail-Anhang, zum Beispiel mit der Endung „.PDF.EXE“, verbreitet. Das Kritische dabei ist, dass Windows standardmäßig bekannte Dateierweiterungen ausblendet. Hier hilft es, die Liste der gesamten Dateierweiterungen im Datei-Explorer zu aktivieren, um verdächtige Dateien besser zu erkennen.

Sind Gateway-Mail-Scanner in der Lage, Dateien anhand ihrer Endung zu filtern, lassen sich E-Mails mit angehängten, ausführbaren Dateien („.EXE“- bzw. „*.EXE“-Dateien) blockieren. Darüber hinaus ist es empfehlenswert, auch Dateien mit folgenden Endungen auf Herz und Nieren zu prüfen: *.BAT, *.CMD, *.SCR und *.JS.

In einigen Fällen startet Ransomware vom AppData- oder LocalAppData-Ordner aus. Über Windows selbst oder die Intrusion-Prevention-Funktionen der Schutzsoftware ist es möglich, Regeln festzulegen, um solche Ausführungen zu verhindern.

Wird ein Unternehmensgerät mit Ransomware infiziert, können auch Dateien in freigegebenen Ordnern verschlüsselt werden, sofern der betroffene Nutzer Schreibrechte besitzt. Aus diesem Grund ist es entscheidend, dass Mitarbeiter darauf achten, welche Dateien sie auf freigegebenen Laufwerken speichern. Denn auch sie können durch infizierte Systeme verschlüsselt werden.

In vielen Fällen nutzt Ransomware das Remote Desktop Protocol (RDP), um gezielten Zugang zum Gerät zu erlangen. Unternehmen sind gut beraten, RDP zu deaktivieren, sofern sie es nicht benötigen.

Malware-Autoren bringen regelmäßig neue, raffiniertere Varianten ihrer schädlichen Codes in Umlauf, um einer Erkennung durch Sicherheitssoftware zu entgehen. Hat sich ein Schadprogramm auf einem System ein-

genistet, bleibt es in Stellung für weitere Befehle von seinem Command and Control (C&C)-Server, bevor es seine schädlichen Funktionen ausführt. Das hat den Vorteil, dass selbst dann, wenn Ransomware nicht vom Antiviren-Modul erkannt wird, sie vor Beginn des Verschlüsselungsprozesses der Daten über die Kommunikation mit dem C&C-Server identifiziert werden kann. Sicherheitssoftware verfügt in der Regel über einen Botnet-Schutz, der die schädliche Kommunikation erkennt und den entsprechenden Prozess blockiert.

Ist die Systemwiederherstellung auf dem infizierten Windows-Gerät aktiviert, lässt sich das System auf den letzten bekannten, sauberen Stand zurücksetzen. Einige der verschlüsselten Dateien können allenfalls aus der Sicherung wiederhergestellt werden. Unverzügliches Handeln ist an dieser Stelle entscheidend. Denn die eine oder andere Variante von Ransomware löscht die Wiederherstellungspunkte aus der Systemwiederherstellung, sobald der Schadcode gestartet wird.

Die Nutzung eines Kontos mit Administratorrechten birgt immer ein Sicherheitsrisiko, weil sich auch Malware diese Rechte zunutze machen und so das System noch leichter infizieren kann. Aus diesem Grund ist es ratsam, das Administratorkonto nur in Ausnahmefällen zu verwenden und für alltägliche Aufgaben Nutzerkonten mit eingeschränkten Rechten einzurichten. Keinesfalls sollte die Benutzerkontensteuerung deaktiviert werden.

Was, wenn es zu spät ist?

Bei einer Infektion oder beim ersten Verdacht gilt es zunächst einmal, einen kühlen Kopf zu bewahren. Das Gerät sollte umgehend vom Internet, Firmennetzwerk und, falls möglich, von der Stromversorgung getrennt werden. Dadurch kann die Kommunikation zwischen Malware und C&C-Server noch vor Beginn des Verschlüsselungsprozesses von Dateien und Laufwerken unterbunden werden. Auch wenn es sich dabei um keine sichere Methode handelt, besteht zumindest die Chance, dass einzelne wertvolle Dateien vor der kompletten Verschlüsselung bewahrt werden. Darüber hinaus ist es ratsam, das System über die Hardware abzuschalten. Womöglich wurde die Ransomware so programmiert, dass sie beim normalen Herunterfahren der Software

noch mehr Schaden anrichtet. Diese Maßnahmen geben Betroffenen vor allem wertvolle Zeit, vorhandene Backups einzuspielen und das Ausmaß des Angriffs einzuschätzen.

Opfer eines Ransomware-Angriffs sollten sich von den Experten beim technischen Support ihres Sicherheitsanbieters für das weitere Vorgehen beraten lassen. Im besten Falle ist bereits ein Entschlüsselungstool für diese Malware-Variante verfügbar oder eine Wiederherstellung der Daten auf anderem Wege möglich. Wird Ransomware rechtzeitig erkannt, besteht bei Android-Geräten die Chance, sie schon vor dem Verschlüsseln zu entfernen. In manchen Fällen genügt es, der entsprechenden App die Administrator-Berechtigungen zu entziehen oder das Gerät im abgesicherten Modus zu starten. Liegen Backups vor, ist eine zeitsparende Möglichkeit, das Gerät auf Werkseinstellungen zurückzusetzen.

Was Sie niemals tun sollten: Zahlen? Um keinen Preis!

Auch wenn die oben genannten Beispiele belegen, dass die betroffenen Unternehmen nach Zahlung des Lösegelds ihre Daten zum Teil oder vollständig wiedererlangt haben, ist dringend davon abzuraten, auf die Forderung einzugehen. In unzähligen Fällen tauchten die Daten trotz Zahlung nicht mehr auf. Es gibt also keine Garantie dafür. Hinzu kommt, dass es sich um „Geschäfte“ mit Kriminellen handelt. Lässt sich ein Betroffener auf die Zahlung ein, fördert er die Weiterentwicklung von Ransomware und den Ausbau dieses Schwarzmarktes. Und die Sicherheit, nicht erneut Opfer eines Ransomware-Angriffs zu werden, ist damit nicht gegeben. Im Gegenteil. ■



THOMAS UHLEMANN,
Security Specialist, ESET Deutschland GmbH



Effiziente und sichere Behördenkommunikation

Am Institut für Internet-Sicherheit – if(is) wurde im Rahmen eines wissenschaftlichen Projekts eine innovative Kommunikationsplattform namens „Quvert“ konzipiert und entwickelt. Ausgehend von der Idee, das Kommunikationsverhalten von Jugendlichen auf den Businesskontext zu übertragen, wurde ein erster Prototyp umgesetzt und getestet.

Im Arbeitsalltag bekommt Information eine nie zuvor dagewesene Wichtigkeit. Die richtigen Informationen schnell zur Verfügung zu haben, macht die Arbeit einfacher, besser und schneller. Und: Es war noch nie einfacher als heute, Informationen, Erkenntnisse, Erfahrungen und Wissen in einem Bruchteil von Sekunden mit Kollegen, Partnern oder Bürgern zu teilen. Durch digitale Kommunikation und das Internet ist es möglich geworden, dass jeder Mensch unabhängig von seinem sozialen Status an der globalen Kommunikation aktiv teilnehmen kann.

Diese Kommunikation kann ganz unterschiedlich ablaufen und verschiedene Grade der Effektivität erreichen. Sie kann in einem geschützten oder ungeschützten Kommunikationssystem stattfinden. Sie kann uni- bis multidirektional sein. Letzt-

endlich ist Kommunikation ein komplexes System, das hauptsächlich aus protokollspezifischen, technischen und menschlichen Komponenten besteht.

Insbesondere im Öffentlichen Dienst ist ein effizientes, smartes und sicheres Kommunikationswerkzeug von essentieller Wichtigkeit im Zuge der immer weiter fortschreitenden Digitalisierung, die auch vor öffentlichen Instanzen keinen Halt macht. Insbesondere Kosten spielen im Öffentlichen Dienst oftmals eine große Rolle. Die zu entwerfenden Werkzeuge sollten also möglichst günstig in Anschaffung und Unterhalt sein, müssen aber ein maximales Maß an Nutzbarkeit, Sicherheit und Schutz von persönlichen Daten mitbringen. Insbesondere innerhalb der öffentlichen Verwaltungen kommt es zur Erhebung und Verarbeitung von personenbe-

zogenen und vertraulichen Daten. Der Bürger muss sich sicher sein, dass die Daten nicht an Dritte weitergegeben werden und er die Hoheit über seine Daten behält. Selbstbestimmung muss durchsetzbar sein, und es müssen Datenschutz und Datensicherheit in hohem Maße „by Design“ umgesetzt werden. Ebenfalls von bedeutender Wichtigkeit ist es, Behördenprozesse und Workflows digital abbildbar zu machen, damit es beispielsweise zu einer Verkürzung von Bearbeitungszeiten kommt. Davon profitieren Kunden und Behörden. Für Mitarbeiter im Öffentlichen Dienst muss das Kommunikationswerkzeug intuitiv nutzbar sein, und es muss deren Arbeitsalltag effektiver gestalten, damit es akzeptiert und effektiv genutzt wird.

Kommunikationsformen

Wieso ist Kommunikation auch für den Öffentlichen Dienst von so essentieller Wichtigkeit? Wie oben bereits erläutert, ist Kommunikation ein Prozess, der dem Ziel dient, Informationen auszutauschen, die das Arbeiten erleichtern sollen. Fach- und Füh-

rungskräfte verbringen den größten Anteil ihrer Arbeitszeit mit Kommunikation. Die Effizienz dieser Kommunikation orientiert sich an der Kommunikationsstruktur sowie an den individuellen Fähigkeiten der jeweiligen Person. Die Kommunikation lässt sich auch klassifizieren, etwa in dienstweggebundene oder ungebundene, rein interne oder organisationsübergreifende, formelle oder informelle sowie Individual- oder Massenkommunikation. Für all diese Formen bietet sich die moderne chatbasierte Kommunikation an. Dadurch können einzelne Anforderungen bedient und teilweise sogar kombiniert werden.

Durch die Einführung eines Chat-Systems, in dem alle Mitarbeiter gleich verbunden sind, können Hierarchien ein Stück weit verflacht werden, sodass alle Teilnehmer eines Kommunikationssystems auf einer Kommunikationsebene stehen und Grenzen der Hierarchie verschwimmen. Die Arbeit flexibilisiert sich hinsichtlich Ort, Zeit, Struktur und Zusammenarbeitsform, wodurch der Grad an Effektivität innerhalb einer öffentlichen Stelle steigt. Die Kommunikationsbeziehung verändert sich also von vertikalen Hierarchieebenen hin zu einer horizontalen, in der Kommunikation auf der gleichen Ebene effektiv stattfindet. Für Genehmigungen oder verbindliche Prozesse kann die vertikale hierarchische Struktur allerdings im Kommunikationssystem ebenfalls abgebildet werden. Es ist sogar möglich und sinnvoll, Nichtabstreitbarkeit in einem modernen Kommunikationssystem zu implementieren respektive einen rechtsverbindlichen Nachweis möglich zu machen.

Neben all den technischen und unternehmerischen Vorteilen, die durch ein solches modernes Kommunikationswerkzeug entstehen, kann die Kommunikationsplattform auch als soziales Tool verstanden werden. Dies ist allerdings nicht die Kommunikationsplattform an sich, sondern die Kommunikationsplattform muss Möglichkeiten und Funktionen bieten, mit anderen Personen über zu definierende Kanäle in Verbindung zu treten. Dadurch lässt sich in einem nächsten Schritt auch kollaboratives Arbeiten einfach umsetzen. Es lassen sich Interaktionen herbeiführen, die Rückkopplungen für Selbstorganisation ermöglichen und „Incentives“ erlauben. Diese Kommunikationskanäle lassen sich im Sinne eines offenen, transparenten und vernetzten, also ei-

nes digitalisierten Verwaltungsapparats verstehen.

Von Grund auf sicher (IT-Security by Design)

Das Austauschen von Informationen und das Thema IT-Sicherheit gehen heutzutage miteinander einher. Chatbasierte Anwendungen ohne entsprechende kryptographische und vertrauenswürdige Absicherung können durchsichtig für Dritte sein und geraten dadurch schnell in Verruf. Gerade bei Anwendungen ausländischer Anbieter kann der Datenfluss die Grenzen Deutschlands und Europas überqueren, wodurch dieser dem Datenschutzrecht und der Politik des entsprechenden Landes unterzuordnen ist. Ebenso lässt die Verwendung von durch Dritte angebotenen Diensten und das zwangsläufig damit verbundene ungewollte Teilen von Informationen den Anwender selbst zum Produkt werden. Gerade an Stellen, wo personenbezogene Daten zusammenlaufen und auch verarbeitet werden, ist die Entscheidung für einen solchen Dienst fatal. Die Hoheit über die eigenen Daten muss folglich in den Händen des jeweiligen Besitzers liegen. Dementsprechend ist neben den bereits genannten Anforderungen an eine moderne Kommunikationsplattform die Absicherung der ausgetauschten Daten auf technischer, allerdings auch auf Ebene des Benutzers, von Bedeutung und somit die IT-Sicherheit als essentieller Faktor aufzugreifen.

„IT-Security by Design“ ist dabei das Stichwort und muss bei der Planung einer modernen und fortschrittlichen Kommunikationsplattform berücksichtigt werden. Dies gilt nicht nur für die Transportwege der Daten. Die Serverkomponenten sowie die Clientseite müssen von Beginn an die IT-Sicherheit einverleibt bekommen. Eine Ende-zu-Ende-Verschlüsselung schafft dabei das nötige Vertrauen und schließt Dritte vollständig aus, die Verifikation der Identität und die Authentifizierung aller Anwender garantieren die Echtheit und Glaubwürdigkeit eines Gegenübers und die langfristige Archivierung von bestimmten Nachrichten ermöglicht die Nachweisbarkeit von Prozessen.

Das E-Mail-System als mittlerweile alteingesessenes Kommunikationswerkzeug ist aus technischer Sicht vergleichsweise unsicher. Das Manipulieren von ganzen Nach-

richten oder das Fälschen des Absenders stellt heutzutage keine technische Herausforderung mehr dar. Möglichkeiten zur Verschlüsselung ganzer Nachrichten existieren bereits seit mehr als 20 Jahren, sind allerdings nicht „Out-of-the-box“ einsetzbar. Geschuldet ihrer Komplexität und nicht vorhandener Benutzerfreundlichkeit finden die Lösungen nur wenig Anklang bei Anwendern sowie IT-Verantwortlichen.

Moderne Kommunikation – effizient, sicher und nutzbar

Im aktuellen Informationszeitalter wächst neben der steigenden Bedeutung der Information auch deren Menge. Oftmals vergehen Stunden, ehe das Ende der abzuarbeitenden E-Mail-Flut zu erkennen ist. Demzufolge ist es umso wichtiger, neben den bereits erwähnten Eigenschaften, die Effizienz der Übermittlung der eigentlichen Information zu steigern. So verbrauchen die Mitarbeiter heutzutage sehr viel Zeit, um den eigentlichen Inhalt einer E-Mail zu erkennen. Die einzelnen E-Mails enthalten sehr viele Formalitäten, wie die persönliche Anrede des schon ohnehin seit Dekaden bekannten Kollegen, die sich doch oft wiederholenden Grußformeln bis hin zur sperrigen Signatur. Die eigentlich relevante Information ist oftmals irgendwo dazwischen zu entdecken.

Die chatbasierte Kommunikation hakt genau hier ein. Am Beispiel der auf Smartphones verwendeten Chat-Anwendungen, die sich mittlerweile auch mit der zugehörigen Desktopanwendung verbinden und synchronisieren lassen, ist die mögliche Steigerung der Effizienz bei der Übermittlung von Informationen zu erkennen. Formalitäten finden selten ihren Weg in einen solchen Chat und Fragestellungen lassen sich nicht selten symbolisch beantworten. Die Informationsflut kann hierdurch gerade bei der internen Kommunikation öffentlicher Instanzen reduziert und weitestgehend optimiert werden.

Diese Problematik, genauso wie die bereits gezeigten Angriffsvektoren, lässt sich mit einer innovativen Kommunikationsplattform aus dem Weg räumen. Unser Prototyp „Quvert“ wurde konzeptionell genau auf diese Herausforderungen zugeschnitten. Neben der von Anfang an bedachten IT-Sicherheit und der Optimierung des Kommunikationsverhaltens bildet die Benutzerfreundlichkeit die dritte Säule des

Fundaments unserer innovativen und modernen Kommunikationsplattform. Zum Schutz vertrauenswürdiger Kommunikation und zur Wahrung der Privatsphäre beinhaltet Quvert ein integriertes, robustes, auf Standards basierendes Verschlüsselungssystem, das nur an wenigen Schnittstellen mit dem Benutzer in Berührung kommt – ganz im Sinne der Benutzerfreundlichkeit, die heute noch bei vielen anderen IT-Sicherheitsprodukten vernachlässigt wird und die Anwender massiv in der Nutzung von Sicherheitslösungen eingeschränkt und behindert. Das Paradebeispiel unzureichender Benutzerfreundlichkeit zeigt die E-Mail-Verschlüsselung, die lediglich durch die Verwendung zusätzlicher Software zur Option wird. Dabei müssen zum verwendeten E-Mail-Client oftmals noch Programme und Add-ons installiert und konfiguriert sowie Schlüssel erzeugt und kompliziert ausgetauscht werden. Ohne fortgeschrittene Kenntnisse in den Bereichen der Computersoftware und im Schlüsselmanagement sind die nötigen Schritte von Laien kaum durchzuführen. Quvert setzt daher zur Absicherung der Kommunikation auf etablierte und vertrauenswürdige IT-Sicherheitstechniken und lässt dabei den Benutzer diese Features nur passiv nutzen.

Zusammenfassend lässt sich für Quvert festhalten: Die IT-Sicherheit wurde bereits in der Konzeptionsphase, also direkt von Beginn an, berücksichtigt (Security by Design) sowie im Sinne der Nutzbarkeit für den Anwender weitestgehend transparent gestaltet. Des Weiteren nimmt die Lösung neue Herausforderungen an und macht die Hoheit der im Kontext des Informationsaustauschs anfallenden Daten zum Thema. Dazu verfolgt Quvert den Ansatz, die zur Vermittlung der Nachrichten benötigten Server in die Hände der jeweiligen Instanz zu geben und diese in den jeweiligen Dienststellen zu betreiben. Ganz nach dem Motto: Ihre Server, Ihre Mitarbeiter, Ihre Daten. In weiteren Schritten adressiert Quvert eine organisationsübergreifende Kommunikation, und das mit derselben Maßgabe an IT-Sicherheit und Authentizität der Nutzer. Erste Konzepte für eine solche Erweiterung der Kommunikationsplattform existieren bereits und verfolgen den Ansatz, verschiedene Stellen miteinander zu vernetzen und die Kommunikation auch übergreifend auf beschriebene Art und Weise effizienter, sicherer und benutzerfreundlicher zu gestalten.

Featurettes

Neben all den bereits beschriebenen Aspekten und Anforderungen ist natürlich auch die Entwicklung von Features und neuen Ideen essentiell für den Erfolg eines modernen Kommunikationssystems. Die Chat-Kommunikation ist eine Basisfunktion von Quvert. Um sich an die Individualität, Flexibilität und Größe von Behörden anzupassen, müssen deutlich mehr Innovationen in der Chat-Applikation realisiert werden. Möchte ein Sachbearbeiter beispielsweise eine Freigabe für einen Vorgang beantragen, muss er heutzutage E-Mails versenden oder Formulare ausfüllen. Dies kostet Zeit und Ressourcen, die eigentlich besser zu nutzen wären. Die Kommunikationsplattform bietet eine „Handshake“-Funktion, die solche Freigabeprozesse digitalisiert abbilden kann. Die Anfrage zur Freigabe wird an den entsprechenden Vorgesetzten versendet, der eine binäre Entscheidung treffen kann: „Freigeben“ und „Ablehnen“. Es wird technisch und kryptographisch sichergestellt, dass diese Entscheidung hinterlegt wird, und im Streitfall kann eine solche Freigabe nach dem Mehraugenprinzip dechiffriert werden und somit ist eine Absprache nicht abstreitbar, sollte ein Gerät nicht auffindbar sein oder ausgetauscht worden sein.



Abb. 1: Handshake für verbindliche Arbeitsabläufe

Weiterhin ist es wünschenswert, die gängige Funktion „Status“, die aus anderen Chat-Systemen bekannt ist, prominenter zu gestalten und mit sinnvollen Funktionen zu erweitern. Beispielsweise mit einem temporär setzbaren Status, beispielsweise „Bahnfahrt“, um mit allen Kontakten in einer Behörde zu teilen, dass die Erreichbarkeit momentan stark eingeschränkt ist. Nach Ablauf der definierten Dauer wird der Status automatisch auf den vorherigen dauerhaften Status zurückgesetzt.

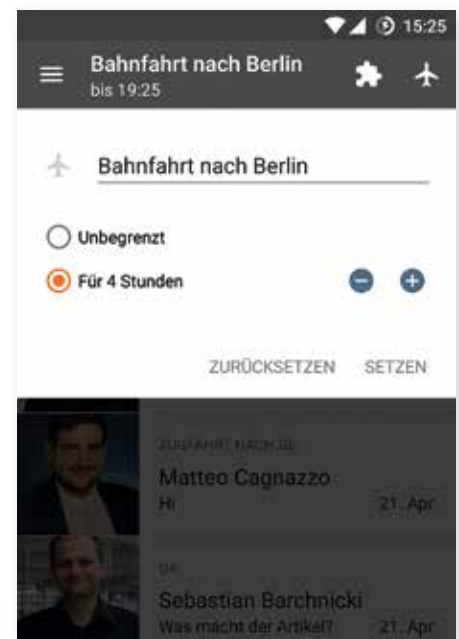


Abb. 2: Anzeige des Verfügbarkeitsstatus

Quvert bietet weiterhin die Möglichkeit, Mitarbeiter mit Kompetenz-„Tags“ auszustatten. Diese bilden die Kompetenzen der einzelnen Mitarbeiter ab. Dadurch können Hard und Soft Skills innerhalb einer Organisation strukturiert und für Kollegen sichtbar gemacht werden. Sucht ein Mitarbeiter beispielsweise Hilfe bei Excel-Tabellen, besteht die Möglichkeit, dass er nach „Excel“ sucht und direkt alle Mitarbeiter und Kontaktinformationen angezeigt bekommt, um Hilfe zu bekommen. Diese einzelnen „Tags“ lassen sich zu einem Netzwerk zusammenfassen, um eine „Kompetenzlandkarte“ zu generieren. Diese kann beispielsweise den Bedarf an Kompetenzen heute und morgen visualisieren und bei Entscheidungen bezüglich Einstellungen von Mitarbeitern helfen. Insbesondere Mitarbeiter, die sich neben der Arbeit weiterqualifizieren oder ein breitgefächertes Wissensspektrum haben, haben somit eine erhöhte Chance, bei Personalentscheidungen intern berufen zu

werden. Weitere Möglichkeiten, um Nutzen aus der Analyse von solchen Kompetenznetzwerken zu ziehen, werden momentan erforscht.

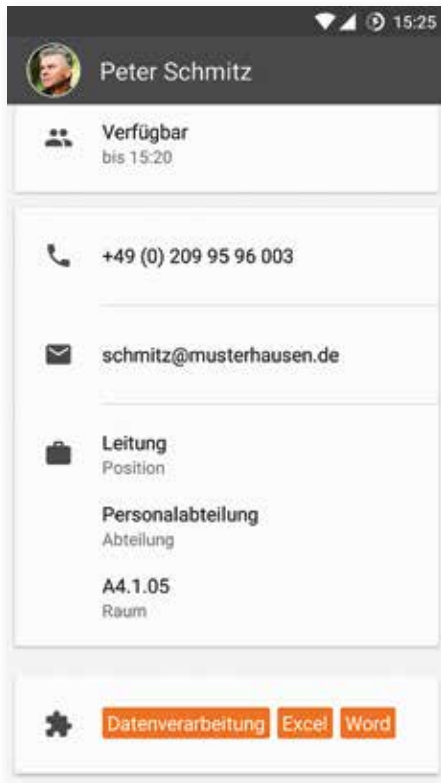


Abb. 3: Darstellung von Kompetenzen

Mit der Darstellung von Kompetenzen lässt sich eine weitere, für soziale Netzwerke typische Funktion etablieren, nämlich Kanäle. Innerhalb eines Kanals kann ein beliebiger Nutzer eine Frage zu einem bestimmten Themengebiet stellen. Diese kann dann in Form eines offenen Forums diskutiert und gelöst werden. Ein Vorteil, der durch dieses Feature entsteht, ist, dass das Unternehmen im Zuge eines transparenten, offenen Unternehmens einzelne Diskussionen veröffentlichten kann und somit den Kunden näher an die Entwicklungsarbeit heranlässt. Ein weiterer Vorteil, der durch Kanäle impliziert wird, ist, dass Mitarbeiter ihr Wissen konservieren und Fragestellungen außerhalb ihres normalen Tagesgeschäfts beantworten können, um dieses etwas variabler zu gestalten.

Weitere Aspekte

Zurzeit arbeiten wir an weiteren Aspekten, die helfen sollen, das Kommunikationssystem Quvert einfach und sicher nutzen zu können. Neben der Chat Kommunikation soll es auch möglich sein, Voice-Nachricht

ten verschlüsselt zu übertragen, um unkompliziert Informationen auszutauschen. Falls der Empfänger in einer Besprechung sitzt und diese noch abhören kann, er aber erkennen möchte, ob die Voice-Nachricht wichtig oder dringlich ist, kann er diese in Text umwandeln, um den Inhalt zu lesen.

Ein weiteres Forschungsthema ist die Minimierung der Lesbarkeit durch andere, die zum Beispiel im Zug, im Flugzeug oder in einer Besprechung neben einem sitzen. Hier soll sichergestellt werden, dass sensible Informationen nicht durch Dritte gelesen werden können.

Fazit

Kommunikation im Öffentlichen Dienst ist ein essentieller Bestandteil für die Produktivität und die Zufriedenheit der Bürger. Nur effizient kommunizierende Dienststellen werden sich im Zuge der Innovationskraft der Digitalisierung erfolgreich darstellen können und einen echten Mehrwert für Bürger, durch beispielsweise kürzere Bearbeitungszeiten, bieten. Die Mitarbeiter in Behörden haben die Möglichkeit, schnell, flexibel und stressfrei intern zu kommunizieren und mehr Zeit und Ruhe für die Vorgesprachen der Bürger zu gewinnen. Dadurch werden Abstimmungsgespräche und Freigaben nur noch Mittel zum Zweck und die kostbare Zeit kann effizient genutzt werden. Es kommt im Allgemeinen zu einer Neuorganisation der Arbeit. Gerade jüngere Generationen können das innovative Konzept, das auf der Instant-Messaging-Funktion aufbaut, schnell adaptieren und effizient einsetzen.

Für den Öffentlichen Dienst ist es von hoher Wichtigkeit, den kulturellen Wandel zur digitalisierten Welt mitzugehen. Kernfaktoren für Öffentliche Verwaltungen sind die Optimierung und die Digitalisierung von Prozessen und Workflows. Wenn alles um uns herum sofort und immer verfügbar ist, aber ein Passantrag beim Bürgeramt 6 Wochen dauert, wird das für eine zunehmende Polarisierung bei der Bürgerschaft und langfristig vermutlich für Unbehagen sorgen. Im Allgemeinen lässt sich festhalten, dass die Personalarbeit, deren wichtigster Bestandteil die Kommunikation ist, durch die Digitalisierung einen Kulturwandel erfährt. An der Stärkung technischer und sozialer Innovationen führt kein Weg vorbei, auch nicht im Öffentlichen Dienst.

Aus diesem Grund wurde Quvert als ein Werkzeug für effiziente und sichere Kommunikation, zum Beispiel in Behörden, entwickelt. Für weitere Informationen oder eventuelle Partnerschaften besteht die Möglichkeit, mit dem Projektteam direkt in Kontakt zu treten (siehe www.quvert.de). Weiterhin sind wir sehr an Ihrem Feedback interessiert und für Kommentare, Kritik und Lob jederzeit offen. ■



MATTEO CAGNAZZO

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und leitet den Forschungsbereich Gesundheitswesen.




NORBERT POHLMANN

ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrust.



PATRICK WEGNER

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und leitet den Forschungsbereich IT-Sicherheits-Apps.



Elektronische Akten aus der Cloud

In deutschen Behörden stapeln sich die Akten bis an die Decke. Regale reihen sich in den Archiven aneinander wie die Perlen einer Kette. Unterlagen wie Anträge, Bewerbungen, Krankmeldungen, Urlaubsanträge, Reisekostenabrechnungen oder Fortbildungsnachweise stauen sich auf zu wahren Dokumentenbergen. Zeitgemäß sind die Papierarchive längst nicht mehr. Wenn Mitarbeiter hier etwas suchen, sind sie zwischen den Aktenbergen meist länger verschwunden. Dabei ist nicht einmal garantiert, dass sie auch fündig werden. Denn häufig sind die Papierakten weder aktuell noch vollständig.

Doch die öffentliche Verwaltung reagiert. So verpflichtet das E-Government-Gesetz des Bundes, elektronische Akten einzuführen – und das bereits bis zum Jahr 2020. Wenn auch Antragsverfahren rechtssicher elektronisch abgebildet werden, sind viele Behördengänge damit überflüssig. Vom Antrag bis zum Bescheid läuft alles elektronisch. „Eine digitale Gesellschaft verlangt auch eine digitale Verwaltung“, sagt NRW-Innenminister Ralf Jäger. „Bürgerinnen, Bürger und Unternehmen erwarten von uns zu Recht, dass sie Verwaltungsangelegenheiten einfach, schnell und ortsunabhängig erledigen können.“

Hohe Messlatte für Sicherheit

Eine Umstellung, die sich mancherorts zu einem Herkulesprojekt entwickelt. Denn E-

Akte-Lösungen müssen zunächst in teils komplexe Systeme und Anwendungslandschaften integriert werden. Als besonders einfach und kostensparend gilt das Dokumentenmanagement aus der Cloud. Doch das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt mit seinem Anforderungskatalog „Cloud Computing“ die Messlatte für eine sichere Cloud-Nutzung hoch und nur wenige Anbieter erfüllen diese strengen Vorgaben.

Mit der sogenannten „E-Akte Public“, einer Lösung aus dem Hause T-Systems, greifen Verwaltungs-Mitarbeiter auf elektronische Dokumente zu, bearbeiten diese nachvollziehbar und speichern sie revisionssicher. Über vorstrukturierte, dynamisch veränderbare Workflows (Ad-hoc-Workflows) lassen

sich Geschäftsgänge mit mehreren Beteiligten initiieren, arbeitsteilig bearbeiten, zeichnen und abschließen. Und das sowohl verwaltungsintern als auch organisationsübergreifend. Auch von unterwegs können die Mitarbeiter per Laptop, Tablet oder Smartphone mobil und gesichert auf Unterlagen und Vorgänge zugreifen.

Gewohnte Benutzeroberflächen

Die Lösung basiert technologisch auf der SharePoint-Technologie von Microsoft. Die öffentliche Verwaltung kann die Kollaborationsplattform nutzen, ohne dass die Mitarbeiter hierfür neue Technologien oder Bedienkonzepte erlernen müssen, denn SharePoint ist bereits vollständig in die Microsoft-Office-Welt integriert. So kann ein Sachbearbeiter direkt aus Outlook heraus Dokumente aufrufen oder verakten. Auch über unterschiedliche Fachverfahren oder Workflow-Anwendungen werden Dokumente einfach innerhalb der gewohnten Benutzeroberflächen erstellt, bearbeitet und gesichert.

Ein weiterer Vorteil: die vielen Möglichkeiten für eine übergreifende Zusammenarbeit. So können zum Beispiel die Mitarbei-

ter unterschiedlicher Verwaltungsbereiche, intern wie auch extern, bei entsprechender Systemarchitektur gleichzeitig online an einem Dokument – zum Beispiel einer Entscheidungsvorlage – arbeiten. Alle Ergänzungen oder Änderungen werden dabei historisiert. Dies beschleunigt den Bearbeitungsprozess und ermöglicht einem betroffenen Sachbearbeiter eine gezielte Klärung im direkten Dialog.

Fachverfahren, Archive und Storage-Systeme einfach anbinden

Um die elektronische Akte möglichst einfach und schnell einführen zu können, arbeitet T-Systems mit einem eigenen App-Framework, auf dem die Lösung aufsetzt. Die Middleware ist nach dem Baukastenprinzip strukturiert. Daher lässt sie sich gut integrieren, an kundenspezifische Fachverfahren anbinden und bei Bedarf erweitern oder an spezielle Anforderungen anpassen.

Zudem unterstützt die E-Akte Public die Anbindung vorhandener Storage-Systeme und

Archive nach dem CMIS-Standard ebenso wie das Langzeitarchiv „ImageMaster“ von T-Systems (s. Kasten). Die Lösung setzt auf den Datenaustausch-Standard XDOMEA der öffentlichen Verwaltung. Das reduziert Inkompatibilitäten mit externen Systemen und erleichtert die Integration. Die offene Lösungsarchitektur bietet somit Investitionssicherheit.

Sicher aus der Cloud

Doch wie gut ist die elektronische Akte gegen den Zugriff Unbefugter gesichert? Immerhin arbeiten immer mehr Mitarbeiter mobil und die Häufigkeit von Cyber-Angriffen steigt stetig. Deswegen ist eine hochsi-

chere IT-Architektur unverzichtbar – besonders bei einer so wichtigen Basislösung wie der elektronischen Akte.

Das beginnt bereits bei der Bereitstellung von IT-Infrastruktur für den einzelnen Mitarbeiter: zum Beispiel PC, Laptop oder Smartphone. Hier bringt eine Desktop-Virtualisierung nicht nur Vorteile für die Mobilität der Mitarbeiter, sondern auch für die Sicherheit. Denn alle Daten sind sicher im Rechenzentrum gespeichert anstatt auf unterschiedlichen Endgeräten. Zudem lassen sich einheitliche Sicherheitseinstellungen leichter umsetzen. Die Mitarbeiter können an jedem beliebigen Rechner und auch außerhalb der

Wiesbaden setzt auf elektronische Akte

Eine moderne, bürgernahe Verwaltung mit einem virtuellen Rathaus, das jederzeit zu einem Besuch einlädt – so präsentiert sich die hessische Landeshauptstadt Wiesbaden. Hinter den Kulissen sorgt Informations- und Kommunikationstechnologie für das Fundament. Bisher papierbasierte Abläufe werden Schritt für Schritt automatisiert und machen die Abläufe effizienter und transparenter – unter anderem dank der elektronischen Akte sowie der Modernisierung des Ratsinformationssystems. Mit diesen Systemen arbeiten mittlerweile über 800 Nutzer aus verschiedenen Ämtern der Stadtverwaltung Wiesbaden. Dies erleichtert ihnen die Arbeit und unterstützt die schnelle, reibungslose Zusammenarbeit (Collaboration). Beides führt wiederum zu mehr Arbeitszufriedenheit, steigert die Produktivität und optimiert die Prozesse. Die einmaligen Investitionen zahlen sich in jedem Fall aus. Darüber hinaus ist die Lösung nachhaltig, da etwa Papier- und Kopierkosten in größerem Umfang wegfallen. „Gemeinsam mit unseren Partnern haben wir eine serviceorientierte Architektur geschaffen, um die Stadtverwaltung auf zukünftige Herausforderungen durch immer komplexere Aufgaben mit weniger Personal vorzubereiten“, sagt Dr. Thomas Ortseifen, stellvertretender IT-Leiter, IT-Referent und Projektmanager der Landeshauptstadt Wiesbaden. Für die Wiesbadener bringt das einen besseren Service und mehr Bürgernähe.

Langzeitarchiv im Rechenzentrum

Die öffentliche Verwaltung muss rechtsrelevante E-Mails ordnungsgemäß archivieren. Doch ein Exchange-Standard-Postfach eignet sich dafür nicht. Zum einen ist es aus Kostengründen auf 100 Megabyte begrenzt. Zum anderen speichert es Outlook-Datendateien (PST) dezentral auf zahlreichen lokalen Fileshares. Das birgt Sicherheitsrisiken und verursacht erhebliche Betriebskosten. Daher haben sich das Justizministerium und das Baden-Württembergische Ministerium für Wissenschaft, Forschung und Kunst für eine Enterprise-Content-Management-Suite namens „ImageMaster“ von T-Systems entschieden, um 12.500 Postfächer zu archivieren.

Dabei wurden die Fileshares in einem hochsicheren Rechenzentrum des Anbieters zentralisiert und so alle lokalen PST-Dateien unterbunden. Anstelle der E-Mails in den lokalen Postfächern stehen nun Links mit einer Größe von wenigen Kilobyte, die den Speicherplatz pro E-Mail reduzieren. Dennoch lassen sich alle rechtsrelevanten E-Mails jederzeit wieder herstellen, da sie im Rechenzentrum revisionssicher langzeitgespeichert sind. Positiver Nebeneffekt: Die benötigten Zeiträume zum Back-up der Exchange-Umgebung sowie die Kosten sinken. Für die Ministeriumsmitarbeiter änderte sich nichts: Alle Funktionen wie „Antworten“ und „Weiterleiten“ stehen wie gewohnt zur Verfügung.

Verwaltung über gesicherte Netzverbindungen mit Laptop, Tablet oder Smartphone arbeiten.

Cloud-Betrieb mit hohen Sicherheitsstandards

Die E-Akte Public macht einen solchen zentralen Betrieb sowohl als browserbasierte Web-Lösung wie auch als virtualisierte und vollständig mandantenfähige Lösung möglich. Dabei eignet sie sich neben dem lokalen Betrieb beim Kunden auch für den Einsatz bei kommunalen oder externen Dienstleistern im Rahmen von „Private Clouds“.

Derartige „Private Cloud“-Infrastrukturen befinden sich bei der öffentlichen Verwaltung und ihren Dienstleistern bereits im Aufbau oder Betrieb. Die Nutzung solcher Plattformen entlastet die Kunden bei den Investitionskosten sowie den Betriebs- und Wartungsaufgaben. „Private Clouds“ müssen allen Vorgaben hinsichtlich Sicherheit, Datenschutz und Verfügbarkeit wie den „IT-Grundschutz-Katalogen“ und den BSI-Kriterien für Cloud Computing genügen.

Microsoft SharePoint verfügt über umfangreiche Funktionalitäten für den Schutz von

gespeicherten Inhalten, wie zum Beispiel die systemseitige Überwachung von Aufbewahrungsfristen und Schutz vor unerlaubten Veränderungen. Dies bedeutet, dass SharePoint nachgewiesen revisions-sicher betrieben werden kann.

An rechtlichen Anforderungen ausgerichtet

Die Lösung bezieht die zentralen Aspekte des E-Government-Gesetzes (EGovG) ein. So ermöglicht die Integration von De-Mail der öffentlichen Verwaltung, mit der E-Akte Public das Potenzial zur Optimierung von Geschäftsprozessen aus zuschöpfen. Aber auch Spezialanforderungen an eine rechtssichere elektronische Archivierung werden erfüllt, wie etwa die Technische Richtlinie TR-03125 (TR-ESOR) des Bundesamts für Sicherheit in der Informationstechnik. Zudem hält die Lösung das Grundprinzip der „Nachvollziehbarkeit des Verwaltungshandelns“ ein. Hierzu zählen die Historisierungsfunktionen ebenso wie spezielle Dokumentations- und Nachweisfunktionen. So müssen Mitarbeiter zum Beispiel angeben, ob sie die vorgeschriebenen Arbeitsschritte im Geschäftsgang erledigt haben.

Zu einem regelkonformen Betrieb gehört auch immer, organisatorische Regelungen zum Verfahrensbetrieb festzulegen und einzuhalten. Die E-Akte Public wurde auf Grundlage der Regelungen entwickelt, die sich im neuen „Organisationskonzept Elektronische Verwaltungsarbeit“ des Bundesinnenministeriums, in der Registratur-Richtlinie (RegR), in den jeweiligen Geschäftsordnungen und Dienstanweisungen sowie in der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) finden. ■

Interview mit Gerd Zilch,

IT-S: Herr Zilch, die E-Akte Public kann auch aus der Cloud heraus betrieben werden. Dienstleistungen aus dem Rechenzentrum genießen inzwischen zwar mehr Vertrauen, restlos ausgeräumt sind die Bedenken aber noch nicht. Was entgegnet Sie den Skeptikern?

Gerd Zilch: Es ist zunächst einmal legitim und völlig richtig, sich mit dem Sicherheitsaspekt auseinanderzusetzen. Denn Cloud Services müssen höchsten Sicherheitsstandards gerecht werden. Es braucht viel Erfahrung, um eine Legacy-IT bei laufendem Betrieb in die Cloud zu transformieren. Datenschutz und Datensicherheit dürfen dabei genauso wenig auf der Strecke bleiben wie Compliance-Anforderungen.

IT-S: Wie gehen öffentliche Verwaltungen dabei am besten vor?

GZ: Indem sie sich Cloud-erfahrene Partner suchen, die höchste Sicherheitsstandards vorweisen können. Damit stellen sie sicher, dass sie mit der Transformation in die Cloud Datenschutzgesetzen, Vorgaben von Steuerbehörden und Auditierungsanforderungen entsprechen. Für die öffentlichen Verwaltungen ist es auch wichtig zu wissen, wo sich ihre Daten genau befinden, zum Beispiel in welchem Rechenzentrum. Dabei ist die Verschlüsselung sämtlicher Daten natürlich ein absolutes Muss. Schon in unserem eigenen Interesse empfehlen und implementieren wir Sicherheitsmaßnahmen, die das Niveau vieler Anwender deutlich übertreffen.

IT-S: Wie findet man einen solchen Partner?

GZ: Wichtige Fingerzeige liefern Zertifizierungen, die etwa das Bundesamt für Sicherheit in der Informationstechnik (BSI) vergibt. Es sollte außerdem ein Provider gewählt werden, der ausreichend Erfahrungen vorzuweisen hat und einen Ende-zu-Ende-Komplett-Ansatz verfolgt. Der Partner muss die Anforderungen an ein Cloud-Security-Konzept klar überblicken können.



GERD ZILCH,
Senior Solution Consultant
bei T-Systems

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance

<kes>

Die Zeitschrift für
Informations-Sicherheit

Infotag

Wirtschaftsspionage

Jetzt anmelden unter

www.datakontext.com/infotag_spionage



23.11.2016 in MÜNCHEN

Kostenpauschale: 95,- Euro zzgl. MwSt.

IT-SICHERHEIT- und <kes>-Abonnenten:
75,- EUR zzgl. MwSt.

Mit freundlicher Unterstützung:





BUSINESS SOLUTIONS

Präzision und Geschwindigkeit.
Virenschutz für das gesamte Unternehmen.



ENDPOINT ANTIVIRUS



GATEWAY SECURITY



MOBILE SECURITY



SECURE AUTHENTICATION



FILE SECURITY



COLLABORATION



ENDPOINT SECURITY



DESlock+ DATENVERSCHLÜSSELUNG



MAIL SECURITY



VIRTUAL MACHINE

Autorisierte ESET Distributoren:



BEWÄHRT. SICHER. AUSGEZEICHNET.

