4 2017

Datareport

IT-Sicherheit

Das Risiko meistern

Inhalt

Ransomware, Social Engineering, Botnetze. Cybercrime hat Hochkonjunktur. IT-Sicherheit muss daher in die Offensive gehen.

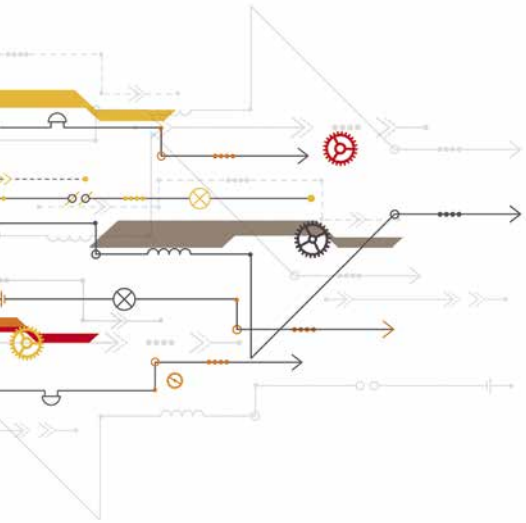
8

Werner Degenhardt tritt dafür ein, die „Human Firewall“ zu stärken. Der Psychologe spricht im Interview über den menschlichen Faktor in der IT.

14

34

Ein falscher Klick, und die Schadsoftware ist auf dem Rechner. Wir geben Tipps, wie man gefährliche E-Mails erkennt.



Liebe Leserinnen, liebe Leser,

es ist Zeit für offensive Maßnahmen. Gegen Angst, gegen Lethargie und Stagnation. Für mutiges Handeln und Veränderung. Ganz ohne Absicht zieht sich diese Botschaft wie ein roter Faden durch diese Ausgabe der Datareport. Beim Durchsehen der fertigen Artikel ist mir sofort eines meiner Lieblingskinderbücher in den Sinn gekommen: „Ronja Räubertochter“ von Astrid Lindgren. Als Ronja zehn Jahre alt ist, verlässt die Räubertochter ihr schützendes Zuhause und streunt allein im Wald herum. Bei Kälte und Schnee und bis tief in die Nacht hinein. Mit der Angst des Räubervaters, der ständig um seine Tochter besorgt ist, geht diese konsequent durch ‚Sich-Üben‘ um: Sie berücksichtigt seine Sicherheitshinweise, stellt sich den Gefahren aber ganz bewusst. Lindgrens Botschaft: Wer sich der Gefahr stellt, findet Wege, ihr zu begegnen.

Die Gefahren unserer digitalen Welt lauten zwar nicht Kälte und Nacht, auch werden wir nicht von Wilddruden bedroht. Unsere Bedrohungen heißen vielmehr Cyberattacke, Veränderung und Komplexität. Und wenn wir genau hinschauen, gehört wohl auch die Unwissenheit dazu. Die Ängste, die sie auslösen, sind vielfältig und führen oft zu Schweigen und Stillhalten. Dabei gibt Angst die richtigen Impulse, wenn sie über das Nachdenken zum Handeln führt.

Vorschläge, wie wir mit unseren modernen Gefahren umgehen können, finden sich jede Menge in diesem Heft. Wir zeigen auf, wie man sich durch aktives, vorausschauendes Handeln gegen Cyberattacken in Stellung bringt. Beschäftigen uns mit der Frage, warum Ängste im Umgang mit IT hemmen können, obwohl das nicht sein muss. Und gehen der Frage nach, warum wir unsere föderale Struktur nicht als Störfaktor für Entwicklung ansehen sollten.

Ihre
Britta Heinrich
(Leiterin Öffentlichkeitsarbeit)

81 Prozent der Bürger wünschen sich ein Bürgerkonto

Ein Bürgerkonto als Verbindungsplattform zwischen Behörden und Privatpersonen begrüßen 81 Prozent der Bevölkerung. Zu diesem Ergebnis kam das Unternehmen Pricewaterhouse Coopers in einer Studie zur bürgerseitigen Akzeptanz von Online-Verwaltungsangeboten in Deutschland. Laut der Erhebung haben 67 Prozent der Bürger in der Vergangenheit digitale Dienstleistungen ihrer Verwaltung in Anspruch genommen, 61 Prozent würden dies auch zukünftig tun. 90 Prozent der Bürger, die bereit wären, Verwaltungsvorgänge online zu erledigen, würden ein Bürgerkonto nutzen. Die Vorteile darin sehen drei Viertel der Befragten vor allem in der Zeitersparnis, dem Komfort und einer geringeren Umweltbelastung. Ebenso viele sorgen sich um Missbrauch oder Manipulation ihrer Daten, die sie den Institutionen zur Verfügung stellen. Die Verwaltung genießt großes Vertrauen: 82 Prozent der Befragten würden ihrer Stadtverwaltung den Zugriff auf ihre Daten erlauben.

IT-Planungsrat beschließt Details zum Portalverbund

Der IT-Planungsrat, das IT-Steuerungsgremium von Bund und Ländern, hat sich auf Grundprinzipien für die IT-Architektur des geplanten Portalverbundes aller Verwaltungsportale verständigt. In der Oktober-Sitzung hat er zudem neue Standards beschlossen, um Daten zu erfassen, einzusehen und auszutauschen. Dazu gehören XDomea, XFall oder XBau. Hintergrund ist das Onlinezugangsgesetz. Es verpflichtet Bund, Länder und Kommunen, bis 2022 ihre Verwaltungsleistungen elektronisch verfügbar zu machen und auf einem gemeinschaftlichen Portal anzubieten. Darüber hinaus haben die Chefs aus Bundeskanzleramt sowie aus Staats- und Senatskanzleien der Länder eine neue Einrichtung, die Föderale IT-Kooperation, beschlossen. Mit ihr erhält der IT-Planungsrat einen operativen Unterbau.

Sachsen-Anhalt entwirft E-Government-Gesetz

Die Landesregierung Sachsen-Anhalt will die Verwaltungen durch das E-Government-Gesetz (EGovG LSA) bis 2022 zur elektronischen Aktenführung verpflichten. Mit dem Gesetz schafft Sachsen-Anhalt einen rechtlichen Rahmen für die digitale Verwaltung auf Landesebene. Das EGovG LSA sieht vor, Akten und Vorgänge sowie Korrespondenzen elektronisch zu führen und zu bearbeiten. Es ist Teil der Digitalen Agenda des Landes, mit der analoge Prozesse umgestaltet und die elektronische Zusammenarbeit gefördert werden sollen. Dadurch soll der Datenaustausch zwischen Bürgern und Verwaltung sowie zwischen unterschiedlichen Behörden erleichtert werden. Das 2013 in Kraft getretene E-Government-Gesetz des Bundes verpflichtet die Länder zu eigenen gesetzlichen Regelungen.

eID: Deutschland erledigt als erster EU-Staat Hausaufgaben

Deutschland hat im September als erster EU-Staat Unterlagen bei der EU-Kommission eingereicht, um den elektronischen Identitätsnachweis (eID) einzuführen. Dieser Schritt ist nötig, um nationale Ausweise europaweit anerkennen und nutzen zu können. Die eID ermöglicht es, sich online auszuweisen und Verwaltungsdienste abzurufen. So kann im EU-Ausland ein Gewerbe angemeldet, ein Kfz zugelassen oder eine Steuererklärung abgegeben werden. Die EU-Mitgliedsstaaten sind nach der EU-Verordnung zur elektronischen Identifizierung (eIDAS) dazu verpflichtet, ab 29. September 2018 ihre Verwaltungsverfahren für die deutsche Online-Ausweisfunktion zu öffnen. Ob sie selbst auch elektronische Identitätsnachweise nutzen wollen, steht ihnen frei.

Digitalisierung: Deutschland ist Mittelmaß

Deutschland gehört zwar zu den innovationsstärksten Ländern der Welt, schneidet aber bei der Digitalisierung nicht gut ab. Handlungsbedarf bestehe beim Breitbandausbau, der Digitalisierung der Verwaltung, bei Forschung und Technologie und bei digitalen Geschäftsmodellen. Das sind Ergebnisse des „Innovationsindikators 2017“. Im allgemeinen Ranking belegt Deutschland Platz 4, hinter der Schweiz, Singapur und Belgien, bei der Digitalisierung Rang 17 (Nummer 1: Finnland). Der Innovationsindikator vergleicht die Innovationsleistung von 35 Ländern. Auftraggeber sind die Akademie der Technikwissenschaften und der Bundesverband der Deutschen Industrie. Mehr unter www.innovationsindikator.de.

Studie: Wirtschaft sieht Potenzial für Blockchain

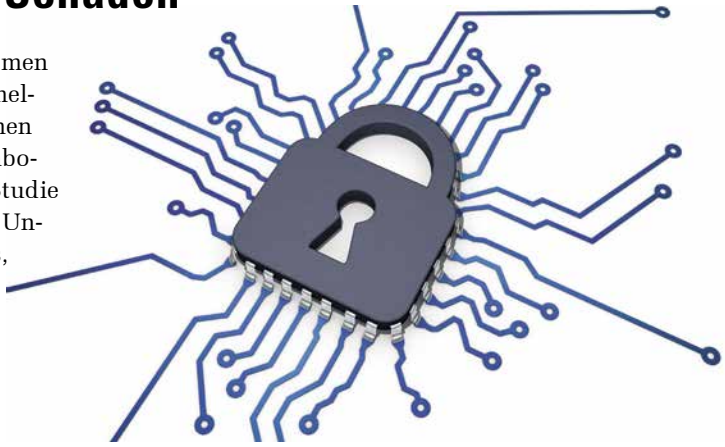
Die Blockchain-Technologie gewinnt für die deutsche Wirtschaft an Bedeutung. Zu diesem Ergebnis kommt die Studie „Potenzialanalyse Blockchain“ des Unternehmens Sopra Steria Consulting. Demnach schreiben 40 Prozent der befragten Fach- und Führungskräfte der Technologie großes Potenzial zu. 79 Prozent der Befragten kennen den Begriff Blockchain. 47 Prozent der Unternehmen prüfen den internen Einsatz, 21 Prozent arbeiten bereits an Prototypen. Sie hoffen, dass so Prozesse schneller, einfacher und günstiger werden. Mithilfe von Blockchain lassen sich Daten dezentral halten. Jede Transaktion wird verschlüsselt in einem Netzwerk verteilt dokumentiert und bestätigt. Mehr unter www.soprasteria.de.

Europa: freier Fluss für freie Daten

Unternehmensvertreter begrüßen das Ziel Estlands, den digitalen Binnenmarkt in der Europäischen Union voranzutreiben. Ein harmonisierter digitaler Binnenmarkt werde pro Jahr 415 Milliarden Euro zur Wirtschaftsleistung der EU beitragen und Hunderttausende neue Jobs schaffen, so Bernhard Rohleder, Hauptgeschäftsführer des IT-Verbandes Bitkom. Estland hatte im zweiten Halbjahr 2017 den Vorsitz des EU-Rats inne und will den grenzüberschreitenden Datenfluss in Europa fördern. Der freie Datenverkehr soll zur fünften Grundfreiheit der EU werden, so wie der freie Verkehr von Personen, Dienstleistungen, Waren und Kapital. Letzteres sind die Grundprinzipien des EU-Binnenmarktes.

Datenklau: 55 Milliarden Euro Schaden

Durch Datendiebstahl entsteht deutschen Unternehmen jährlich ein Schaden von rund 55 Milliarden Euro. Das meldet der IT-Verband Bitkom. 53 Prozent der Unternehmen sind 2016 und 2017 Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Laut einer Bitkom-Studie zur Unternehmenssicherheit wurden in jedem sechsten Unternehmen sensible Daten gestohlen, vor allem E-Mails, Finanzdaten, Kundendaten, Informationen aus Forschung und Entwicklung oder Mitarbeiterdaten. In 62 Prozent der Fälle waren aktuelle oder ehemalige Mitarbeiter der Unternehmen die Täter.
Mehr dazu auf www.bitkom.org.



eGovernment Award für Dataport

Dataport hat in der Kategorie Rechenzentrum den eGovernment Award 2017 der Fachzeitschrift eGovernment Computing erhalten. Die Leser der Zeitschrift wählten die Gewinner. Johann Bizer, Vorstandsvorsitzender von Dataport, nahm die Auszeichnung entgegen. Schirmherr des Wettbewerbs ist das Bundesinnenministerium. Dataport hat die zuvor auf sechs Standorte aufgeteilten Rechenzentren in einem Twin Data Center zusammengefasst, das sich an zwei Standorten befindet und identisch aufgebaut ist. Dadurch sind die Daten im Störfall gegenseitig abgesichert. Zertifikate des Bundesamtes für Sicherheit in der Informationstechnik und der TÜV Informationstechnik GmbH bestätigen: Das Twin Data Center ist eines der sichersten Rechenzentren in Europa. Es verwaltet Daten von Polizei, Justiz und Behörden und hat mehr als 600 Verfahren in Betrieb. Dank einer skalierbaren Infrastruktur lassen sich seine Kapazitäten flexibel erweitern oder anpassen.

Neue Plattform für Strafverfolgungsbehörden

Strafverfolgungsbehörden können nun übergreifend eine gemeinsame Analyse- und Arbeitsplattform nutzen. Die von Dataport betriebene Plattform dForensik kombiniert massendatentaugliche Speichersysteme und Software für die IT-Forensik. Staatsanwälte, Richter, Steuerfahnder und Polizisten können auf ihr digitale Beweismittel wie Computer- oder Smartphone-Daten speichern, analysieren und austauschen. dForensik wird zentral in Dataports Twin Data Center betrieben. Dieser zentrale Betrieb ermöglicht es, behörden- und bundeslandübergreifend auf die archivierten Daten zuzugreifen. Das erleichtert den Austausch der häufig sehr umfangreichen Ermittlungsdaten. Über einen sicheren VPN-Zugang (Virtual Private Network) können Ermittler auch mobil auf die Daten zugreifen.

Polizei 1: Dataport erteilt Auftrag an Trivadis

Das IT-Unternehmen Trivadis wird Dataport auch in Zukunft bei der Pflege und Entwicklung von Fachverfahren für die Polizei unterstützen. Die in einem Rahmenvertrag festgelegten Leistungen des Dienstleisters für Dataport umfassen unter anderem Architekturberatung, Softwareentwicklung auf der Basis von Java-, Oracle- und Business Intelligence-Technologien sowie Projekt- und Testmanagement. Schwerpunkte der Zusammenarbeit sind die Unterstützung beim störungsfreien Betrieb der Systeme, Wissenstransfer, die Transformation von Prozessen und die Modernisierung vorhandener Anwendungen. Das Unternehmen Trivadis arbeitet seit 2013 mit Dataport zusammen. Dataport betreibt in seinem Rechenzentrum generell diverse Fachverfahren für die Polizeien seiner Trägerländer.

Polizei 2: Polizei Hamburg nutzt erstmals mobile App

Die Hamburger Polizei nutzt eine von Dataport entwickelte mobile Anwendung, die App ComVor mobil. Zum Einsatz kam sie erstmals im Juli 2017 während des G20-Gipfels in der Hansestadt. Sie erleichtert die Arbeit der Polizisten, weil Daten direkt von unterwegs abgefragt oder eingegeben werden können. Die mobile Anwendung ist nicht in öffentlichen App-Stores erhältlich und kann nur auf Diensthandys der Polizei eingespielt werden. Die Daten werden im Twin Data Center von Dataport gespeichert. Im Juni nutzten bereits 400 Polizisten die App, bis zum Jahresende sollen es 1.400 sein.

Datensicherheit

Das Datenschutz-Paradoxon

Wenn ich über betrieblichen Datenschutz und Sicherheit spreche, wird immer entgegnet: „Aber die Leute teilen doch eh ihre ganzen Daten via Social Media, da müssen wir uns jetzt nicht so anstellen.“ Ausgehend davon könnte eine Bank sagen: „Die Menschen lassen ihre Geldbeutel in unverschlossenen Autos liegen, dann können wir die Schließfächer auch auflassen.“ Genau hier liegt das Problem: Wenn Menschen Daten bewusst teilen, berechtigt mich das noch lange nicht, beim Umgang mit mir anvertrauten Daten schlampig zu sein. Mache ich mich über Menschen lustig, die aus Unwissenheit zu freigiebig mit ihren Daten sind, liegt der Fehler bei mir.

Michael Hirdes beschäftigt sich seit vielen Jahren hauptberuflich und ehrenamtlich mit dem Spannungsfeld zwischen Datenschutz und IT-Sicherheit. Außerdem ist er Vorstandsmitglied des Chaos Computer Club e.V. (CCC).

Wir haben in den letzten Jahren großen Konzernen die Deutungshoheit über Informationen gegeben und sie dabei stark unterstützt. Umfragen zufolge beziehen ein signifikanter Teil der Erwachsenen und ein noch größerer der Heranwachsenden Informationen zu jedwedem Thema über „soziale“ Medien. Hierfür sind zum einen die Bürger selbst verantwortlich, die nicht gelernt haben, Quellen zu überprüfen, zum anderen „die Politik“, die aktiv verhindert hat, dass die öffentlich-rechtlichen Medien ein zeitgemäßes Angebot bereitstellen – und nicht zuletzt die Unternehmen, die dieses geschlossene Ökosystem umarmen und unterstützen.

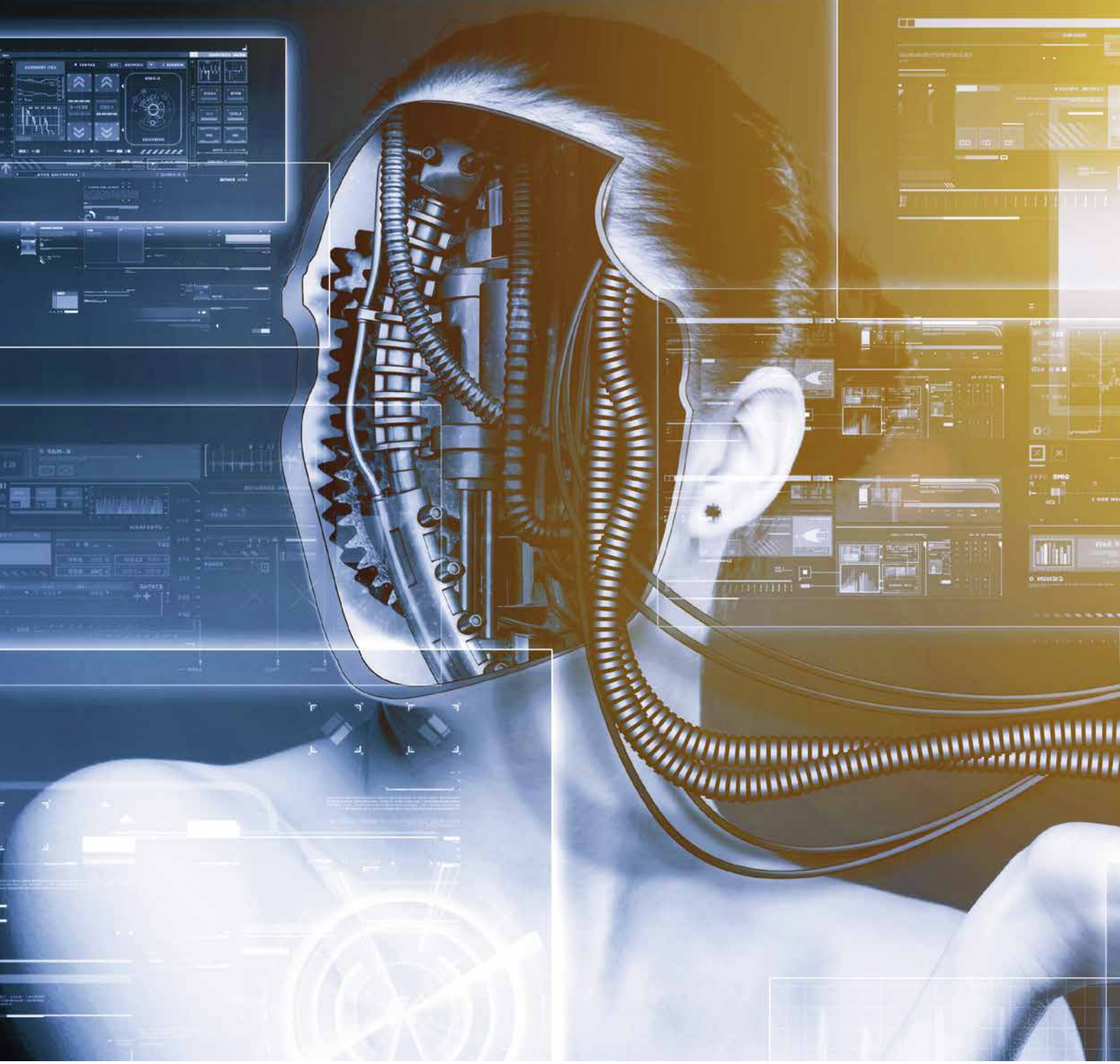
Das Problem, auf das wir durch die Monopolisierung von Informationen zusteuern, liegt auf der Hand: Einige weltweite Player verfügen über die Inhalte und können damit nach Herzenslust verfahren, Nutzerdaten weiterverkaufen oder die Dienste abschalten. Menschen, die diese Entwicklung kritisch sehen und technisch oder monetär nicht in der Lage sind, daran teilzuhaben, werden aus dem gesellschaftlichen Diskurs ausgeschlossen.

Aber die Leute teilen doch eh ihre ganzen Daten via Social Media.

Besonders kritisch wird es, wenn die Daten von Unbeteiligten ohne deren Zustimmung an Unternehmen gegeben werden wie bei Whatsapp/Facebook. Benutzer gehen immer zu dem Dienst, bei dem ihre Freunde sind. Unternehmen und vor allem Behörden sollten das aber nicht weiter befeuern, sondern Alternativen bereithalten. Die Verwaltung setzt mehr und mehr auf Digitalisierung – es darf aber nicht sein, dass wieder Menschen auf der Strecke bleiben.

Abschließend bleibt festzuhalten, dass es natürlich wünschenswert wäre, wenn Bürger verantwortungsbewusster mit ihren Daten umgingen. Behörden und Unternehmen sind aber in der Pflicht, mit gutem Beispiel voranzugehen und verschlüsselte Kommunikation anzubieten, Datensparsamkeit und Datenschutz zu leben. Das wirkt sich auf die Mitarbeiter aus, die das dann weitertragen und kritischer mit Daten umgehen.

//Michael Hirdes



IT-Sicherheit

Sichere Daten – eine Illusion

Die Kriminalität im Internet boomt. Es wird zunehmend leichter und finanziell einträglicher, sich an den Daten von Menschen zu vergreifen. Die Verwaltung muss handeln: Bisherige Methoden zum präventiven Datenschutz greifen nicht mehr. Es ist Zeit für aktive Schritte zum Schutz vor Cyberangriffen.

Technische Infrastrukturen können noch so gut abgesichert sein: Der Faktor Mensch ist ein erhebliches Risiko.

Freitag, 8. Mai 2015. Die Büroleiterin einer Abgeordneten greift zum Telefon und lässt sich mit der IT-Hotline des Deutschen Bundestages verbinden. Tage darauf stellt sich heraus: Über eine scheinbar harmlose E-Mail wurde in den Büros mehrerer Abgeordneter ein Link geöffnet, der einen Trojaner ins System des Deutschen Bundestages einschleuste. Mehrere Programme mit wenigen Kommandozeilen erlaubten Hackern den Zugriff auf Accounts von Administratoren des Bundestagsnetzwerks. In der Folge wurden monatelang Daten von den knapp 12.000 registrierten Nutzern des Netzwerks abgeschöpft.

Ein Hack von vielen in den vergangenen Jahren. Es trifft nicht nur Behörden, sondern auch Unternehmen der Privatwirtschaft aus allen Branchen. Das Webportal Yahoo verlor 2014 eine Milliarde Datensätze von Kunden. Dem Online-Händler Ebay wurden 145 Millionen Mailadressen und Passwörter entwendet, die Bank J.P. Morgan verlor 83 Millionen Datensätze von Kunden. Es gibt unzählige weitere Beispiele.

Erpressung, Datendiebstahl, Datenhandel – darum geht es Cyberkriminellen vor allem. Der Weg führt immer über die Infektion von einzelnen Rechnern, die an Netzwerke angebunden sind.

Die größten Bedrohungen

Der Jahresbericht 2017 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) listet die vorrangigen Infektionswege auf. Da ist zum Beispiel Ransomware: Diese Schadsoftware kapert Computer und verschlüsselt die Festplatten, im Anschluss wird durch Cyberkriminelle Lösegeld gefordert. Beim Social Engineering wiederum täuschen die Angreifer eine persönliche Beziehung vor oder machen Gewinnversprechen. Das Opfer wird abgelenkt und unter emotionalen Druck gesetzt. Schließlich erlaubt es den Zugriff auf den Rechner, gibt Daten heraus oder zahlt scheinbar fällige Gebühren. Spam nennt man unerwünschte E-Mails, die oft Links oder Anhänge enthalten, um Schadsoftware auf den Rechner zu bringen. Botnetze sind ein Verband von ferngesteuerten Schadprogrammen, die eingeschleust werden, um später die Installation weiterer Spionageprogramme zu ermöglichen.

Es wird schlimmer

Laut Bundeskriminalamt (BKA) haben über 70 Prozent der 2016 gemeldeten 80.000 Straftaten

aus der „Kriminalstatistik Cybercrime“ einen Bezug zu Computerbetrug: Es geht überwiegend um Kreditbetrug, Betrug über Daten von Zahlungskarten, Abrechnungsbetrug und Überweisungsbetrug. Abgefangene Daten werden im Darknet zum Verkauf angeboten, einem Online-Netzwerk im Deep Web, das parallel zum frei verfügbaren Internet existiert und verschlüsselte Transaktionen erlaubt.

Gravierende Folgen

Abgesehen davon, dass die Anzahl der Delikte in den vergangenen Jahren sprunghaft angestiegen ist, gibt es eine hohe Dunkelziffer. So stellen zum Beispiel nur 18 Prozent der Unternehmen, die über Ransomware erpresst werden, überhaupt eine Strafanzeige. Laut einer Umfrage des IT-Verbandes Bitkom aus dem Jahr 2016 ist bereits jeder zweite Internetnutzer Opfer von Cybercrime geworden. Die Hälfte davon hat finanzielle Einbußen hinnehmen müssen – durch direkte illegale Geldtransaktionen, aber auch durch das Auffangen der Folgeschäden wie dem Verfügbarkeitsverlust von Daten und dem Ausfall von Hard- und Software.

Nicht nur in finanzieller Hinsicht bedeuten die Schäden, die durch Cyberkriminelle hervorgerufen werden, eine immense Bedrohung für Wirtschaft und Staatsgefüge. Der Schutz von Daten, der reibungslose Ablauf von Handels-, Produktions- und Verwaltungsprozessen sowie der Schutz kritischer Infrastrukturen sind die Säulen unserer modernen Gesellschaft. Nicht umsonst hat die Bundesregierung – wie auch Regierungen anderer Länder – eine Strategie zum Schutz kritischer Infrastrukturen. Darunter sind Anlagen und Systeme mit wichtiger Funktion für die Gesellschaft zu verstehen: Krankenhäuser, Energie- und Wasserversorger, Telekommunikationsstrukturen, Finanzwesen, Transportnetze, Einrichtungen der Justiz und des Rettungswesens.

Die öffentliche Verwaltung muss sich wappnen: Durch das Prinzip „Online zuerst“, die Umformung von bisher nur offline verfügbaren Bürgerservices zu praktikablen Lösungen in Form von E-Government, wird sie zunehmend abhängiger vom Einsatz kompetenter IT-Dienstleistungen. Jeder online verfügbare Service für Bürger bietet eine neue Angriffsfläche für Cyberkriminelle. Egal, ob es sich um Antragsverfahren, die Digitalisierung von Kulturgütern, die Digitalisierung von Akten oder um Beteiligungsprozesse handelt.

Was ist mindestens zu tun?

Präventiver und reaktiver Schutz ist also obligatorisch für alle Institutionen. Präventiv bedeutet: die technischen Infrastrukturen absichern. Als Grundlage dienen die Richtlinien und Standards zur IT-Sicherheit, wie sie in Deutschland vom BSI oder vom Bundesamt für Finanzen (BaFin) herausgegeben werden. Rechenzentren, Cloud-Services und vor allem mobile Endgeräte müssen möglichst gut geschützt sein. Reaktiv bedeutet: so schnell, wie es geht, auf Gefahren zu reagieren und Sicherheitslücken zu schließen. Am besten in enger Kooperation mit anderen Betroffenen. Dies geschieht seit Jahren über CERTs – sogenannte Computer Emergency Respon-

CYBERCRIME-STRAFTATEN IN DEUTSCHLAND

82.649 Fälle von Cybercrime im engeren Sinne (+80,5 %)

253.290 Fälle mit dem Tatmittel Internet unter allen in der PKS* erfassten Straftaten (+3,6 %)

972 Fälle von Ransomware (+94,4 %)

2.175 Fälle von Phishing im Onlinebanking (–51,4 %)

** Polizeiliche Kriminalstatistik*

Zahlen aus dem Bundeslagebild Cybercrime 2016. Vergleichswerte beziehen sich auf den Vorjahresbericht mit Zahlen aus dem Jahr 2015.

Quelle: BKA 2017

se Teams. Diese Computer-Notfallteams gibt es in Wirtschaft und Behörden, auf nationaler und internationaler Ebene. Sie stehen in enger Abstimmung zueinander, informieren sich gegenseitig über aktuelle Bedrohungen, Schwachstellen und Fehlkonfigurationen. Sie entwickeln gemeinsam neue Schutzmaßnahmen.

Proaktives Handeln ist angesagt

Die bestehenden Schutzmaßnahmen haben ihre Berechtigung. Aber: Cyberattacken werden immer professioneller und treten wesentlich häufiger auf. Daher muss jede Institution, die Daten verwaltet, noch einen Schritt weiter gehen. Proaktives Handeln ist das Stichwort. Damit sind aktive und offensive Sicherheitsmaßnahmen gemeint, nicht mehr nur die reine Verteidigungshaltung. Dataport hat dies erkannt und arbeitet derzeit am Aufbau eines Security Operations Center (SOC), das in weiteren Stufen zu einem Cyber Defence Center (CDC) ausgebaut werden soll.

Das SOC bei Dataport hat verschiedene Aufgaben:

1. Die Angriffserkennung soll die täglich zehn Millionen Log-Events, die über die Server laufen, auf bekannte Angriffsmuster automatisiert analysieren. Ausgewertet werden die Sicherheitsprotokolle von Betriebssystemen, Firewalls und Netzwerkkomponenten. Daraus lassen sich dann die hochkritischen Bedrohungen herausfiltern.
2. Damit sich im Falle eines Angriffs innerhalb der ersten Stunden oder sogar Minuten Gegenmaßnahmen ergreifen lassen, sollen Bedrohungen schneller erkannt werden. Das geschieht in erster Linie über automatisiert ausgewertete Protokolle: Ein sogenanntes SIEM-System (Security Information and Event Management) durchsucht die Log-Daten und meldet kritische Ereignisse sofort, damit diese umgehend bearbeitet werden können.
3. Angriffe werden detailliert analysiert. Wie, wann und wo sind sie erfolgt? Mit diesem Wissen ist es möglich, Lücken im Sicherheitssystem so schnell wie möglich zu schließen.
4. Das Thread-Hunting sucht aktiv nach Schwachstellen und Gefährdungen mithilfe von Big Data- und KI-Systemen.

Zeit für die Offensive

Insbesondere staatliche Institutionen unterliegen höchster Sorgfaltspflicht im Umgang mit Nutzerdaten. Sie sollten einen treuhänderischen Umgang mit diesen Daten pflegen und gleichzeitig die digitale Souveränität gewährleisten. Der Staat darf die Datenhoheit nicht verlieren, zugleich müssen die Bürger jederzeit Zugriff auf ihre Daten haben und wissen, dass deren Sicherheit gewährleistet ist. Es gibt keinen hundertprozentigen Schutz gegen Cyberkriminalität. Behörden und deren IT-Dienstleister sind aber verpflichtet, alles nur Denkbare zu unternehmen für den größtmöglichen Schutz der ihnen anvertrauten Daten. Cyberattacken darf nicht mehr nur reagierend begegnet werden: Es ist Zeit für offensive Maßnahmen.

//Andrea Brücken

Wir arbeiten alle zunehmend mit mobilen Endgeräten, die besonders anfällig sind für Angriffe durch Cyberkriminelle.

Sicherheitslücken als Risiko

Schon kommt d

Mindestens jedes zweite deutsche Unternehmen ist betroffen, aber die Firmen breiten gerne den Mantel des Schweigens darüber aus: Hacker stehlen Daten, verschlüsseln Festplatten und erpressen Geld. Das Schweigen ist ignorant, die Haltung dahinter eigennützig, kurzsichtig und vor allem gefährlich.

„Beiersdorf: Mehr Gewinn trotz Hackerangriff“ titelte der Norddeutsche Rundfunk (NDR) in seinen Nachrichten vom August 2017. Auch andere Medien – vor allem Börsen- und Finanznachrichten – sparten nicht mit Lob: „trotzt Hackerangriff, Angriff abgeschüttelt, Rekordgewinn“. Die Nachricht lautete: Die Bilanz stimmt. 35 Millionen Euro Umsatzverlust fallen bei einem Halbjahresumsatz von 3,5 Milliarden offensichtlich nicht ins Gewicht.

Dennoch, nicht alle großen Unternehmen sind glimpflich davongekommen bei den globalen Cyberangriffen in den Sommermonaten 2017. Diese zielten mithilfe von eingeschleusten Trojanern vor allem darauf, Geld zur Freigabe verschlüsselter Daten zu erpressen. Viele Firmen verzeichneten spürbare finanzielle Einbußen und Beeinträchtigungen ihrer Produktionsabläufe. Der Lebensmittelkonzern Mondelez, die Reederei Maersk und der Ölkonzern Rosneft gaben die Störung von IT-Systemen, Telefonanlagen und Produktionsanlagen zu. Sicherheitslücken in älteren Versionen des Betriebssystems Windows von Microsoft

Egal, um welche Branche es geht: Industrielle Produktionsabläufe können durch Angriffe aus dem Cyberspace empfindlich gestört werden oder komplett zum Erliegen kommen.

er nächste Hack

dienten als Einfallstor für den Trojaner WannaCry. Nur wenige Wochen später profitierte der Trojaner Petya von diesen in vielen Unternehmen immer noch offenen Sicherheitslücken.

Schweig still, es geht nicht anders

Der Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) benennt in Pressemitteilungen, dass in diesem Jahr 71 Prozent seiner Mitgliedsunternehmen mit über 5.000 Mitarbeitern Hackerangriffe zugaben. Die Dunkelziffer ist hoch: Viele Unternehmen bewahren Stillschweigen. Auf Wunsch seiner Mitglieder hat der VDE mittlerweile eine anonyme Plattform zum Erfahrungsaustausch über Cyber-Security eingerichtet.

„Die Krux ist jedoch, dass viele Unternehmen nicht ausreichend IT-Spezialisten finden, die zum einen die Digitalisierung intern vorantreiben und zum anderen die Organisation vor externen Angriffen schützen“, sagt Ansgar Hinz, Chief Executive Officer des VDE. Aus einer Studie der Bundesdruckerei zu „Digitalisierung und IT-Sicherheit 2017“ geht übereinstimmend hervor, dass nur circa jedes zweite Unternehmen in Deutschland seine Mitarbeiter regelmäßig zu IT-Sicherheit schult. 2017 taten dies 46 Prozent von 556 repräsentativ befragten Unternehmen, 2016 waren es 55 Prozent.

Widersprüchliche Angaben

Wird IT-Sicherheit von Unternehmen also nicht ernst genommen, obwohl die Anzahl der Cyberattacken rasant ansteigt? Unternehmen kommunizieren in der Öffentlichkeit eine Haltung, die irritierend anmutet. Grundsätzlich rechnen sie nicht damit, gehackt zu werden. Sie halten ihre IT-Infrastrukturen für sicher.

In einer Studie des amerikanischen Softwareanbieters Citrix unter 500 IT-Entscheidern in Unternehmen ab 250 Mitarbeitern kam zugleich Überraschendes zutage: Acht von zehn befragten Entscheidern in deutschen Unternehmen halten die Kryptowährung Bitcoin vor. Sie sind bereit, im Falle einer Cybererpressung für die Entschlüsselung kritischer Daten zu bezahlen.

Wettbewerb vor Sicherheit

Welche Botschaft steht hinter dieser Haltung? Der ökonomische Wettbewerb dirigiert das Handeln im kapitalistischen Wirtschaftssystem: Gewinn und Erfolg sind relevant. Gilt es also, den Betrieb am Laufen zu halten, egal um welchen Preis? Gehört das Vorhalten von Bitcoins, um Daten aus einer erpresserischen Situation auszulösen, als fester Bestandteil in die Gewinn- und Verlustrechnung von Unternehmen?

Per E-Commerce – dem Online-Vertrieb von Waren und Dienstleistungen – werden jährlich allein in Deutschland über 65 Milliarden Euro umgesetzt, Tendenz steigend. Nach Bekleidung sind Elektronikartikel und Telekommunikation die Hauptgeschäftszweige. Gerade im letzteren sind Sicherheitsfragen immer wieder Gegenstand der öffentlichen Diskussion: Simpelste Technologie-Zugänge wie Smartphones, DSL-Router, Smart-TVs und Geräte, die Teil des Internet of Things (IoT) sind, sind bis dato nur schlecht gesichert. Sie laufen teilweise monate-, wenn nicht jahrelang auf nicht aktualisierter Firmware.

Ignoranz und die Folgen

Dazu kommt: Zentrale Adressverwaltungen in Unternehmen werden immer wieder gehackt. Der Handel mit gestohlenen Nutzer- und Zahlungsdaten ist nur ein Problem von vielen, die durch Cyberkriminalität entstehen. Attacken auf Infrastrukturen und Organisationsprozesse von privaten und öffentlichen Institutionen bedrohen vor allem die Stabilität der globalen Gemeinschaft. Solange der Profit dem Thema Sicherheit untergeordnet ist, stehen die Türen für Cyberkriminelle sperrangelweit offen. Es braucht offensichtlich ein Umdenken, offene Kommunikation und den Willen, gemeinschaftlich Lösungsansätze über die Grenzen von Wirtschaftlichkeit hinaus zu finden.

//Andrea Brücken

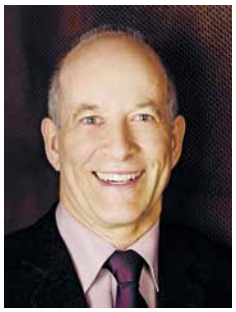
Interview mit Werner Degenhardt

„Die Angst macht ni

Angst vor dem Internet? Das muss nicht der schlechteste Ansatz sein, der Komplexität von Informationstechnik zu begegnen, findet der Psychologe Werner Degenhardt. Allerdings sollte Angst auch im Handeln etwas bewirken. Ein Interview über die Psychologie von IT-Sicherheit und die Notwendigkeit, sich zu sensibilisieren.

Der Eindruck ist, dass Cyber-Angriffe immer perfider werden, Informationstechnik immer verletzlicher wird. Was macht das mit uns?

In dem Blog „Kroker's Look @IT" in der Wirtschaftswoche vom 28. Juni 2017 lesen wir folgende Überschrift: „Trotz WannaCry, Petya & Co: Die Sicherheitsbedenken der Deutschen sind gesunken". Der Beitrag bezieht sich auf den Unisys Security Index, der seit 2007 in einer repräsentativen Verbraucherumfrage erhoben wird. Danach ist Deutschland das einzige der 13 befragten Länder, in dem die Sicherheitsbedenken seit 2014 zurückgegangen sind. Die „German Angst" ist also derzeit nicht das Phänomen, in dem die Deutschen international punkten können. Unter den abgefragten Ängsten ist die Internet-Sicherheit allerdings immer noch die größte. Eine andere länderübergreifende Studie, über die der Harvard Business Review im Mai berichtete, stellt im Einklang damit fest, dass niemand mehr Angst um seine Daten im Internet hat als die Deutschen.



Werner Degenhardt ist Akademischer Direktor der Fakultät für Psychologie und Pädagogik an der Ludwig-Maximilians-Universität in München. Seine Forschungsschwerpunkte sind Human Factors in der Informationssicherheit, soziale Beziehungen im Online-Bereich und Human Computer Interaction. Er engagiert sich in Kampagnen zur Stärkung der „Human Firewall".

Nachdenken, richtig handeln, nicht verkrampft sein.

Die Deutschen nutzen das Internet aber genauso wie die Menschen aller anderen Nationen. Sie zeichnen sich im internationalen Vergleich nur durch eines aus: Sie wissen am wenigsten darüber, welche Daten Online-Dienste sammeln und was sie damit machen. Das heißt, die Angst ist da. Aber was macht sie mit den Menschen? Nichts! Die Ergebnisse der Umfragen lesen sich für mich wie ein Ruf nach intensiven und flächendeckenden Bemühungen um „Awareness" und Training im Umgang mit IT-Technologie und Daten in Schulen, Unternehmen und öffentlichen Organisationen.

Kann man denn mit durchschnittlichem technischen Verständnis überhaupt noch die Kontrolle über die von uns genutzte Technik haben?

Eine ähnliche Frage wurde Klaus Luft, Chief Executive Officer bei Nixdorf, Ende der 1980er Jahre gestellt. Er meinte damals: „Kein Mensch kann sich heute noch alles Wissen aneignen, das nötig ist, die moderne Informationstechnik zu verstehen. Dazu haben wir das Problem noch nicht gelöst, dass das Wissen schneller veraltet, als wir es vergessen können." Klaus Luft meint damit, dass man auch mit einem überdurchschnittlichen technischen Verständnis nicht verstehen kann, was da draußen vor sich geht. Das menschliche Gehirn hat ungefähr 100 Millionen Nervenzellen und 100 Billionen Synapsen, die Nervenzellen untereinander verknüpfen. Das ist so komplex, dass der Anthropologe und Biologe Lyall Watson meinte: „Wenn das Gehirn so einfach wäre, dass wir es verstehen könnten, dann wären wir so einfach, dass wir es nicht könnten."

Der Adressraum von IPv6 (Internet Protocol Version 6) kann 2^{128}, ungefähr 340 Sextillionen, Einheiten mit Internetadressen versehen, die alle untereinander verknüpft sein können. Das ist eine unvorstellbar große Zahl, viel größer noch als 340 Sextillionen. Die Folgen der dadurch entstehenden Komplexität können wir weder verstehen noch vorhersagen.

Einerseits misstrauen die Menschen Staat und Wirtschaft, wenn es um den Umgang mit ihren Daten geht. Andererseits

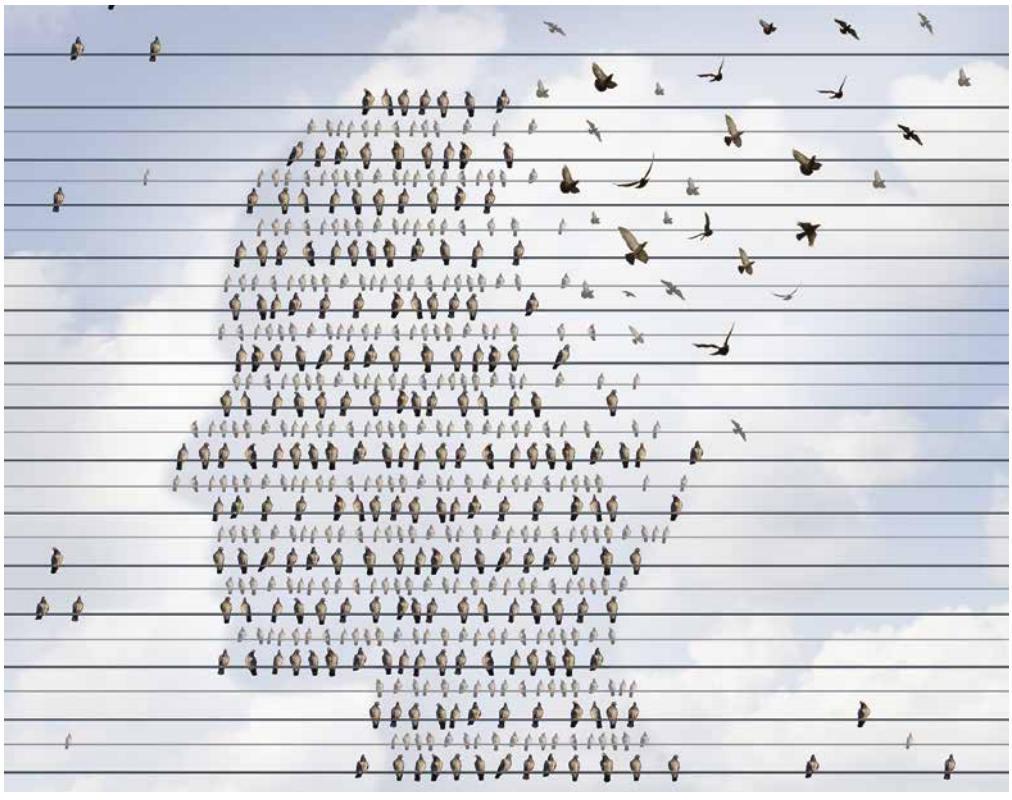
chts mit uns“

verraten sie täglich über Facebook und Co. sehr persönliche Sachen. Ist das nicht paradox?
Ich finde, das ist ein Hinweis darauf, dass es zurzeit an zwei Dingen fehlt: an Wissen und Bewusstsein des Dateneigentümers, der seine Daten hergibt, und an der Kontrolle der Datensammler durch Institutionen, die mächtiger sind als das einzelne Individuum. Solange Initiativen wie „Datenschutz geht zur Schule“ ehrenamtliche Tätigkeiten von Datenschutzaktivisten sind, sind wir weit von einer guten Vorbereitung unserer Kinder auf das Leben in einer digitalisierten Welt entfernt. Man muss von frühester Kindheit an zu vernünftigem Verhalten sozialisiert werden. Gewohnheiten von Erwachsenen zu ändern ist schwer.

Der Staat will, dass die Bürger mehr E-Government-Dienste in Anspruch nehmen. Komplizierte Lösungen dafür, zum Beispiel für Authentifizierung, floppen. Ist IT-Sicherheit mit Usability vereinbar?
Natürlich ist IT-Sicherheit mit Benutzerfreundlichkeit vereinbar. Man muss nur die richtigen Anreize schaffen, damit sich die Hersteller auch Mühe geben. Ein Automobil der Jahrhundertwende wäre für uns ebenso unsicher wie unbenutzbar. Heute steigen wir in einen Leihwagen unbekannten Typs und fahren los. Dieser Fortschritt ist eine Folge von Konsumverhalten, behördlicher Kontrolle und technologischer Entwicklung. Was wir brauchen, ist stärkere Sensibilisierung für Sicherheit und Privatsphäre, Kontrolle durch öffentliche und unabhängige Einrichtungen und Förderung entsprechender Forschung und Entwicklung.

Sind wir Deutschen eigentlich besonders verkrampft, wenn es um die Sicherheit von Technik geht?
Auf eine unbekannte und allem Anschein nach gefährliche Situation – und dabei handelt es sich bei der Informationssicherheit im Internet – mit Angst und Flucht zu reagieren, ist zunächst einmal sehr vernünftig. „Fahren Sie langsam, ich habe es eilig“, soll Adenauer zu seinem Fahrer gesagt haben, weil er sein Ziel sicher erreichen wollte. Erst Angst, dann nachdenken und dann (richtig) handeln scheint mir erfolgversprechender, als erst unüberlegt zu handeln und dann in Angst zu erstarren. Ein Mangel an Hast muss nicht gleich Verkrampfung sein.

// Kirsten Wohlfahrt



Hilft es, der technischen Komplexität geordnete Gedanken entgegen zu setzen? Werner Degenhardt spricht sich für gezielte Sensibilisierung von frühester Kindheit an aus.

Digitalisierung in Kommunen

Zwölf Goldene R

1. Konsequent am lokalen Bedarf orientieren
- Bevölkerungsstruktur beachten
- Innovationsbereitschaft prüfen
- Infrastruktur Breitbandausbau berücksichtigen
- Vorhandene digitale Serviceangebote einbeziehen

2. Alle Bevölkerungsgruppen berücksichtigen
- Lebenswelt für alle
- Nischendenken verabschieden
- Abgrenzungen überwinden / auflösen

3. An vorhandene Strukturen anknüpfen
- Digitale Lösungen gehen nicht in Konkurrenz
- Vorhandene soziale Netzwerke vertiefen
- Zuzugsbereitschaft fördern

4. Planvoll vorgehen
- Fokussierte Mehrjahresplanung
- Stufenweise Entwicklung digitaler Bürgerservices
- Planung auf mindestens fünf Jahre
- Auf bewährte Strategien und Standards aufsetzen

5. Erreichbare Etappenziele definieren
- Weniger ist mehr
- Projektstarts fördern
- Rasche Erfolge mit breitem Nutzen schaffen
- Messbare Erfolgskriterien für Etappenziele

6. Digitale Angebote modular konzipieren
- Gemeinsam genutzte Lösungsplattform
- Einheitliche Serviceinfrastruktur
- Interoperabel
- Skalierbar (in Kommunen unterschiedlicher Größe einsetzbar)
- Übertragbar (durch andere Kommunen mit geringem Aufwand nutzbar)

INFORMATIONEN ZUM PROJEKT

Digitalisierung bietet besondere Entwicklungsperspektiven für den ländlichen Raum, ist aber auch eine Herausforderung für regionale Vielfalt und die kommunale Selbstverwaltung. Bund und Länder werden nicht direkt mit den Sorgen und Erwartungen vor Ort konfrontiert. Die Gestaltung des unmittelbaren Lebensumfelds im ländlichen Raum ist daher eine kommunale Aufgabe. Es gilt, eine bürgerschaftlich organisierte Infrastruktur aufzubauen, die eine Teilhabe der Bürger sichert, Die Kommunalen Landesverbände haben sich daher mit Akteuren des Landes

egeln

8. Mit anderen kooperieren
- Lasten aufteilen
- Kommunale Kooperationen
- Örtliche Nähe ermöglicht arbeitsteilige Entwicklung
- Entfernung erfordert gemeinsame technologische Plattform

9. Nachhaltigkeit sicherstellen
- Innovation ist gut, dauerhafte Wirkung besser
- Einbindung in Gesamtkonzept sicherstellen
- Frühzeitig darauf hinwirken, dass Lösungen sich etablieren

12. Professionelle Begleitung ermöglichen
- Strategische Ziele bestimmen und nachjustieren
- Klare Erfolgskriterien und Meilensteine setzen
- Potenzielle Multiplikatoren identifizieren
- Externe Partner finden und koordinieren

7. Verfügbare Lösungen adaptieren
- Erprobte digitale Lösungen übernehmen
- Einpassung ins modulare Gesamtkonzept
- Von vorhandenen Nutzungsrechten (wirtschaftlich) profitieren

11. Breite Unterstützung organisieren
- Vertreter der Zielgruppen an der Planung beteiligen
- Die digitale Kommune zu einem Anliegen aller machen
- Breite Akzeptanz sicherstellen

10. Fehler zulassen
- Risiken sind zu Beginn nicht durchweg kalkulierbar
- Akzeptanz der Nutzer lässt sich schwer abschätzen
- Im Projektverlauf Erwartungen prüfen
- Lehren für künftige (digitale) Initiativen ziehen

zusammengetan, um die Herausforderungen aktiv anzugehen. Dazu dienen die obenstehenden Thesen – wir freuen uns auf Anregungen, Diskussionen und gemeinsames „Machen“!

EINE INITIATIVE VON:

Schleswig-Holsteinischer Gemeindetag; Schleswig-Holsteinischer Landkreistag; Städteverband Schleswig-Holstein; Schleswig-Holstein Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung; Akademie für die ländlichen Räume Schleswig-Holsteins e.V.; Höhn Consulting GmbH; Dataport.
Mehr auf www.dataport.de

Digitale Verwaltung in Dänemark

Vom Europameister digitalisieren lernen

In Dänemark, einem Vorreiter für digitale Verwaltung, kommt das Amt nicht immer nur online zum Bürger. Sondern es versteckt sich auch in der Bibliothek oder fährt per Lastenfahrrad zum Kunden. Eindrücke von einer Reise nach Kopenhagen, die eine Bremer Delegation im Herbst unternahm.

Hans-Henning Lühr ist Staatsrat bei der Senatorin für Finanzen in der Freien Hansestadt Bremen.

Dänemark ist Europameister im E-Government. Im EU-weiten Ranking belegt es Platz 1. Alle Dänen über 15 Jahre sind verpflichtet, ein digitales Postfach und eine digitale Identität (ID) – die sogenannte „nemID“ – zu besitzen. Mit der Verwaltung erfolgt Kommunikation ausschließlich digital: Anträge oder Steuerbescheide werden elektronisch ausgetauscht. Damit hat Dänemark das umgesetzt, was in Deutschland vielfach noch Vision ist: eine digitale Verwaltung. Der Senat, die Handelskammer Bremen und Vertreter der IT-Wirtschaft unternahmen deshalb im Herbst eine Informationsreise nach Kopenhagen.

Zentrale Elemente der dänischen Digitalisierung sind drei Themenportale für Verwaltungsservices: www.borger.dk (für Bürgerinnen und Bürger), www.virk.dk (Unternehmen), www.sundhed.dk (Gesundheit). Alle staatlichen, regionalen und kommunalen Leistungen sind hier abrufbar. Und das, obwohl es in Dänemark auch das Verfassungsprinzip der kommunalen Selbstverwaltung gibt.

Starkes Mandat für Digitalisierung

Ebenfalls bemerkenswert: Es gibt nur eine Authentifizierungsmethode – für alle Verwaltungsleistungen. Sie ist gesetzlich verpflichtend und wurde gemeinsam mit den Banken entwickelt. Die dänische Regierung nennt als Erfolgskriterien:

- viel Vertrauen in den Staat und eine Bevölkerung, die für Digitalisierung bereit ist.
- ein starkes politisches Mandat – Digitalisierung ist im mächtigen Finanzministerium angesiedelt.
- Kooperation zwischen den staatlichen Ebenen.

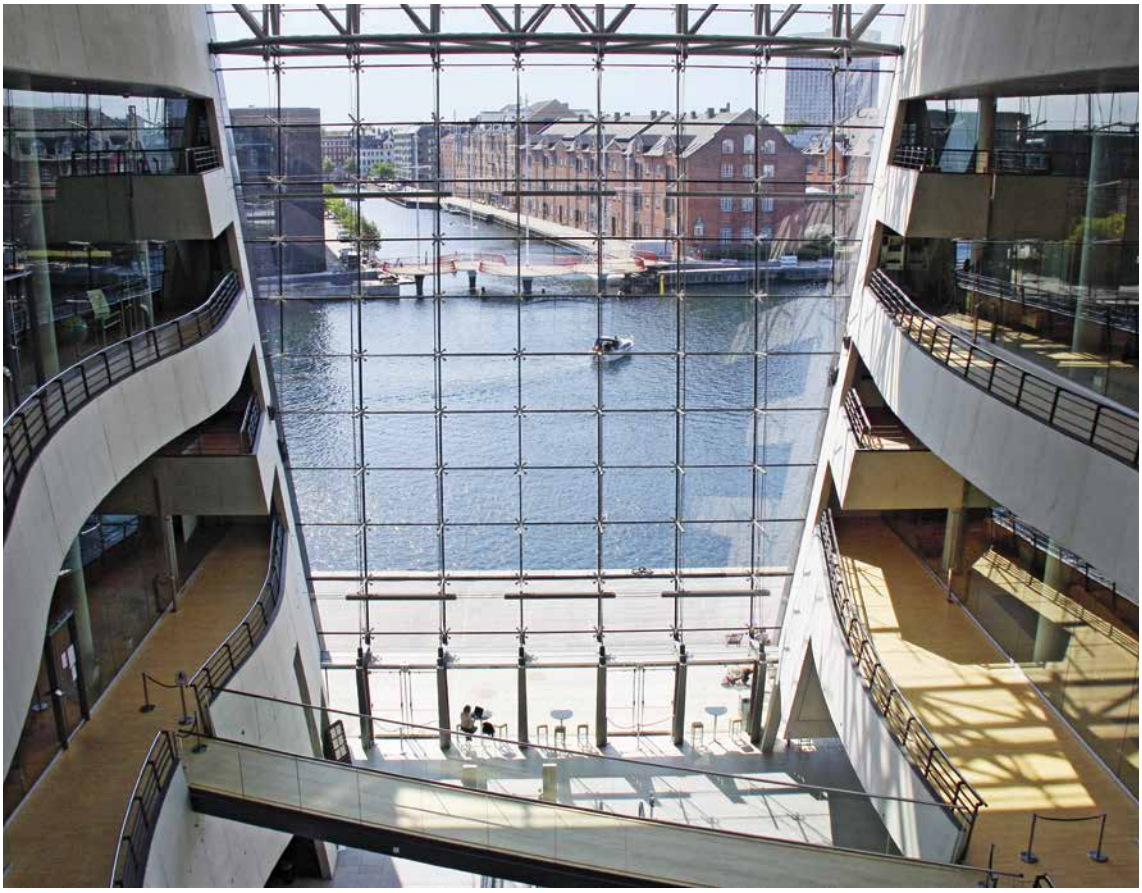
Dass das nicht nur leere Worte sind, konnten wir in vielen Gesprächen unter anderem mit den Vertretern des beim dänischen Finanzministerium angesiedelten Digitalisierungsbüros und den Kommunen verifizieren. Besonders beeindruckend ist, dass die drei staatlichen Ebenen tatsächlich auf Augenhöhe miteinander verhandeln und gemeinsam Strategien entwickeln. Das lassen sie sich auch etwas kosten, so ist das Budget für Strategiebildung in Höhe von 20 Millionen Euro allein schon doppelt so hoch wie das aktuelle Budget des deutschen IT-Planungsrates.

Das Amt kommt per Rad

Der Aufwand ist offenkundig gut investiert. Die Kopenhagener Stadtverwaltung (Kopenhagen ist etwas größer als Bremen) bewertet die durch Digitalisierung ermöglichte Einsparung auf zehn bis 15 Millionen Euro! Statt eigene Bürgerämter zu betreiben, werden für verbleibende Bürgerkontakte in sechs Stadtbibliotheken Servicetische eingerichtet – das sind PC-Arbeitsplätze für Behördenanliegen, Sachbearbeiter sind zum Teil auch vor Ort. Support erfolgt per Telefon. Zur Identitätskontrolle werden Videos eingesetzt. Jugendliche werden von Mitarbeitern der Verwaltung mit einem Infofahrrad besucht – ein Lastenfahrrad mit einem mobilen Tresen und einem Laptop – um dort unkompliziert die nemID einzurichten. E-Mail ist in Zeiten von Facebook oder Instagram für diese Generation nicht mehr up to date.

Was können wir in (Nord-)Deutschland daraus lernen? Die Fokussierung im IT-Planungsrat auf einen Bund-Länder-Portalverbund für E-Government ist zu kurz gedacht. Solange dort nicht Steuer- und Justizleistungen integriert sind, ist er funktional zu sehr eingeschränkt. Auch ist der Abstand zu Dänemark nicht so groß, wenn man bedenkt, dass wir bei Steuer und Justiz IT-Verfahren haben, die genauso hohe Nutzungsraten wie Anwendungen in Dänemark haben (98 Prozent Lohnsteueranmeldungen; 95 Prozent Handelsregistereinträge). Auch hier „zwingen“ wir, elek-

lernen, heißt



Das ist kein Amt, sondern die dänische Nationalbibliothek in Kopenhagen. In sechs Stadtbibliotheken der Hauptstadt wiederum können Bürgerinnen und Bürger Behördengänge online erledigen. Separate Bürgerämter betreibt die Stadt nicht mehr.

tronisch teilzunehmen. Mit der Bremischen Handelskammer haben wir vereinbart, dass in unserem E-Government-Gesetz auch die Unternehmen verpflichtet werden, Rechnungen nur noch elektronisch an die Verwaltung zu schicken.

Für Bürgerinnen und Bürger wollen wir die Verpflichtung nicht. Doch auch hier gehen wir vor wie unser Nachbar. Dort setzt man auf bessere „user journeys“. In Dänemark ist zwar vieles digital, aber die Bürger sind deshalb nicht zufriedener. Dort will man wie wir in Deutschland auf Antragsprozesse verzichten und Verfahren „event-driven“, also anlassbezogen, steuern. Genau wie wir mit unserem Projekt Antragslose Geburtsurkunde, Kindergeld und Elterngeld.

Noch eine Erfahrung der Dänen ist wichtig: Das Vertrauen der Bürger in Staat und Technologie ist der kritische Schlüsselfaktor. Es kann in Zukunft nicht nur um Onlinedienste und Servicekonten gehen, sondern auch darum, wie wir über Protokolle und Nachweise, die die Verwaltung den Bürgern zur Verfügung stellt, das nötige Vertrauen in unsere digitalen Lösungen gewinnen. Dann wird der Amtsschimmel auf der Datenautobahn auch Galopp laufen (können)!

//Hans-Henning Lühr

E-Government-Vergleiche

Estland ist nicht

Alle Welt schaut nach Estland, dem digitalen Vorreiter. Doch Peter Batt, IT-Direktor im Bundesministerium des Innern, ist überzeugt: Der Schlachtruf „Macht alles wie in Estland“ allein bringt die deutsche Verwaltung nicht voran. Stattdessen plädiert er für föderale Vernetzung, um die hiesige Verwaltung zu modernisieren.

Peter Batt leitet die Abteilung Informationstechnik im Bundesministerium des Innern (BMI) und ist IT-Direktor des BMI. Dieser Text ist ein Auszug aus dem Impulsvortrag „Vom E-Government zur föderal vernetzten digitalen Verwaltung“ im Rahmen eines Symposiums in Berlin.

Zu Beginn ein Rückblick: Die Älteren werden sich an die Großrechner mit Lochkarten erinnern, die in deutschen Verwaltungen ab Mitte der 1950er Jahre zum Einsatz kamen. Ab Anfang der 1980er gab es in Wohn- und Kinderzimmern immer mehr Heimcomputer (Commodore 64, Amiga 500). Und wahre Pioniere hatten einen BTX-Decoder und konnten an den ersten deutschen Online-Diensten teilhaben. Das war die Zukunft, dachten wir. Mit ersten Aktivitäten des Domain-Verwalters Denic zu Beginn der 1990er Jahre begann schließlich auch in Deutschland das Internetzeitalter. Das war in etwa in der Zeit, als die Sowjetunion sich auflöste und Estland, das Vorbild modernen E-Governments, wieder eigenständig wurde – und kaum „Legacy-Systeme“, also Altsysteme, hatte.

Warum ist Estland digitaler Vorreiter? Estland ist ein Drittel kleiner als Hamburg. Beim E-Government-Benchmarking der EU war es in einer Vergleichsgruppe mit Malta oder Luxemburg und dort tatsächlich Benchmark. Alles in Estland hat eine Nummer: Haustiere, Autos, Menschen. Das ist toll für den Aufbau von zentralen Registern und damit für schnelles E-Government. In Deutschland würde allein das viel kosten – wegen der hohen Mengen an Riechsalz, die man für die ohnmächtigen Datenschutzbeauftragten bräuchte. Und Estland hatte und hat eine innovations- und investitionsfreudige Führung. Nach der wiedererlangten Souveränität lag der Altersdurchschnitt in der Regierung bei noch nicht einmal 36 Jahren. Spielt das eine Rolle? Noch sehr jung zu sein und etwas neu machen zu können, sich also nicht verändern zu müssen? Letzteres scheint die größte Belastung für die Menschen zu sein.

> **Föderales, vor allem föderal vernetztes Vorgehen ist notwendig.**

Andere Voraussetzungen, andere Benchmarks

Liegt die Faszination von E-Government in Estland vielleicht auch an der Werbung? Die Österreicher zum Beispiel, ebenfalls als E-Government-Gurus zitiert, sind bei aller Qualität in ihrer Vergleichsgruppe gar nicht so weit vorn. Da sind die Niederlande Benchmark. Was lernen wir? E-Government-Guru wird man vermutlich durch Originalität, Jugendlichkeit, eine unkonventionelle Herangehensweise und viel gute PR-Arbeit.

Deutschland ist ein Land, das ein bisschen größer als Estland und verwaltungsmäßig reichlich komplex gestrickt ist. Der Schlachtruf „Macht alles wie in Estland“ ist deshalb kaum geeignet, das Land entscheidend voranzubringen. Und so sind wir auch im EU-Benchmark in einer anderen Vergleichsgruppe. Leider sind wir da auch nicht der Benchmark. Das ist Spanien.

Im Ernst: Die föderale Ordnung, die uns so zu behindern scheint, ist seit dem Zweiten Weltkrieg weltweit nicht unbedingt als Muster des Misserfolgs diskreditiert. Als Jurist fordere ich hier eine Umkehr der Beweislast: Wer an erfolgreichen Grundprinzipien rühren will, muss darlegen, warum jetzt alles anders sein soll. Damit rufe ich nicht zum Beharren auf einer Verwaltung des Jetzt und Hier auf. Diese hat sich endgültig überholt. Wer nicht bereit ist, dieser Wahrheit ins Auge

überall

zu sehen und sich selbst zu ändern, sorgt dafür, selbst überholt zu sein.

Vernetzung als Schlüssel für Veränderung

Ich bin überzeugt: Der Schlüssel ist eine infrastrukturelle und intelligent vernetzte Herangehensweise, die verschiedensten Ansätzen Rechnung trägt und vor allem auch geeignet ist, fortlaufende Veränderung zu erzeugen.

Für alle in dieser Republik gilt dasselbe Grundgesetz. In gleicher Weise brauchen wir bei der Digitalisierung der Verwaltung einen gemeinsamen Rahmen, also gemeinsame Grundprinzipien, Standards, Querschnittsdienste, mit denen wir Vernetzung betreiben und Interoperabilität herstellen. Dafür – und nur dafür – brauchen wir eine starke fach- und ebenenübergreifende Steuerungsverantwortung für die öffentlichen IT-Infrastrukturen. Um digitale Services in Deutschland einheitlich anbieten zu können, ist weiterhin föderales, vor allem aber ein föderal vernetztes Vorgehen notwendig. Bestehende IT-Lösungen von Bund, Ländern und Kommunen müssen von Beginn an Bestandteil dieser Vernetzung sein.

Das Internet basiert auf Vernetzung; seiner Bedeutung für die freie Entfaltung der Persönlichkeit hat das Bundesverfassungsgericht mit dem Urteil zum „Computer-Grundrecht“ Rechnung getragen. Es wäre doch gelacht, wenn ausgerechnet dieses Land mit seiner Vielfalt, mit seinen über 3,5 Millionen kleinen und mittelständischen Unternehmen nicht in der Lage wäre, dieses Erfolgsmodell auch in seiner Verwaltung zu spiegeln. Dass wir dazu in der Lage sind, zeigt die Digitalisierung des Asylverfahrens. Wollen wir auch in den kommenden Jahrzehnten unserem ernsten Auftrag, dem Dienst am Bürger, gerecht werden, müssen wir konsequent auf arbeitsteiliges Verwaltungshandeln setzen. Die Digitalisierung ist dafür ein Schlüssel.

// Peter Batt

Die vollständige Rede von Peter Batt finden Sie auf www.dataport.de.

Digitale Bildung

Die Praxis soll begei

Naturwissenschaftliche Experimente mal anders: Mithilfe von selbst erhobenen Sensordaten sollen Schüler digitale Kompetenz erwerben. Möglich wird dies durch ein Projekt namens „Digitalisierung macht Schule“. Das Projekt wurde während der Digitalen Woche Kiel im Rahmen eines Hackathons vorgestellt.

3. November 2017 im Wirtschaftsgymnasium Kiel. Schülerin Anna-Lena Herrmann ist auf den ersten Blick Feuer und Flamme. Sie steht in ihrem Klassenzimmer am Tisch vor einem Koffer mit einem Ausrüstungsset für naturwissenschaftliche Experimente: Darin befinden sich ein Minicomputer, eine IP-Kamera, Heizungsthermostate, Sensoren für das Erfassen von Temperatur, Bewegung, Licht und Strom. „Digitalisierung macht Schule“ heißt das Projekt, zu dem der Koffer gehört. Die Schulleiterin des Wirtschaftsgymnasiums, Margit Fuhrmann, stellt das Pilotprojekt bei einem Hackathon anlässlich der Digitalen Woche Kiel vor.

Lernen durch Experimente

Ein Hackathon ist eine Wortschöpfung aus „Hack“ und „Marathon“. Ein Hackathon hat zum Ziel, mit allen Anwesenden innerhalb eines festgesetzten Zeitraums nützliche, kreative oder unterhaltsame Softwareprodukte herzustellen. In diesem Fall wird kein Produkt entwickelt, aber Spaß sollen die Schüler haben: Sie erhalten als erste die Gelegenheit, den Umgang mit digitalen Daten im Rahmen naturwissenschaftlicher Experimente zu erproben. Der Koffer liefert einige beispielhafte Unterrichtseinheiten für Versuche. In einem dieser Experimente sollen die Schüler zum Beispiel über Heizungsthermostate und intelligente Gerätesteuerung Wärmeverluste bei offenen Fenstern ermitteln. Sie sollen analysieren, wie Heizungssteuerung effizient eingesetzt und optimiert werden kann. Darüber hinaus sollen die Schüler die vorgegebenen Versuche weiterentwickeln und aus den Ergebnissen neue Experimente gestalten.

Der 17-jährige Janik Schulz ist erfreut. Er hat bereits Programmier-Erfahrung. „Im elften Jahrgang haben wir im Unterricht mit der freien Entwicklungsumgebung Lazarus gearbeitet und programmiert. Ich hoffe, dass die Klasse etwas zum Projekt beitragen kann. Jeder Mensch lebt heute digital, die Digitalisierung wird sich weiter in unserem Leben etablieren.“

Engagiert durch digitale Kompetenz

Genau das ist das Ziel des Projektes „Digitalisierung macht Schule“. Schüler sollen über praktische Versuche für die Digitalisierung begeistert werden. Die Projektinitiatoren Dataport, Capgemini und Microsoft erhoffen sich, dass die Schüler lernen, welche Folgen sich aus der Verknüpfung von Daten ergeben. Marc Reinhardt, Head of Public Sector bei Capgemini in Deutschland, denkt langfristig: „Durch die erlangten digitalen Kompetenzen werden die Schüler dazu befähigt, sich souverän in der Welt der Sensorik und Daten zu bewegen. So können sie sich in die Vernetzung ihrer Kommune mit eigenen Ideen gestaltend einbringen – die Smart City wächst so nach und nach aus der Schule als Keimzelle beziehungsweise als Nucleus.“ Renate Radon, Mitglied der Geschäftsführung bei Microsoft, erklärt: „Die konkrete Umset-

Der Nucleus-Koffer: Zubehör für den bewussten Umgang mit digitalen Daten.

stern

Bereit für Forschungsarbeit: Die Gymnasiasten Janik Schulz und Anna-Lena Herrmann freuen sich auf das Digitalprojekt.

Unterricht mal anders: Am Kieler Wirtschaftsgymnasium experimentieren Schüler mit Sensoren und Daten in einer Cloud.

zung von digitaler Bildung und die Vermittlung von Medienkompetenz sind uns ein großes Anliegen. Mit unserer sicheren und leistungsfähigen Infrastruktur ermöglichen wir, dass digitale Daten jederzeit für alle Schüler zur Verfügung gestellt werden und der intelligente Umgang mit diesen geübt wird."

Die Schüler sind derweil schon am Ausprobieren. In kleinen Gruppen bearbeiten sie je einen der vier Lernversuche. Die erfassten Sensordaten werden über den Minicomputer in die von Microsoft und Dataport bereitgestellte Cloud hochgeladen. Alle teilnehmenden Schulen können über die Cloud auf die Ergebnisse zugreifen und mit den vorhandenen Daten weiterarbeiten. „Ich hoffe, dass wir durch das Projekt andere Schüler kennenlernen“, betont die 18-jährige Anna-Lena Herrmann. Digitalisierung sei auch vorher schon ein wichtiges Thema an ihrer Schule gewesen, ergänzt sie. „Erst vor kurzem haben wir neue Computer bekommen. Außerdem gibt es in der ganzen Schule WLAN, das wir gratis nutzen dürfen.“

Digital bis nach San Francisco

Fünf Schulen aus dem Kieler Raum und Bremen sowie acht Schulen aus Hamburg nehmen zunächst an dem fächerübergreifenden Pilotprojekt teil. Es sei Teil des Lehrplans eines beruflichen Gymnasiums, erklärt Schulleiterin Margit Fuhrmann. „Biologie, BWL, Mathematik und Englisch kommen bei uns dafür in Frage. Jeder Fachlehrer gibt für seinen Teil eine Note, wobei eigene Forschungsaufgaben von Schülern als besondere Lernleistung angerechnet werden können. Diese Arbeit ersetzt dann eine Halbjahresnote.“

Eine Vernetzung der Schüler bei dem Projekt sei auch nach Übersee geplant, äußert Margit Fuhrmann abschließend. „Wir haben eine Partnerschaft mit den Convent and Stuart Hall Schools in San Francisco, mit der Austauschprogramme von Schulklassen und Fachschaften geplant sind. Dorthin werden wir unsere Ergebnisse weitergeben.“

//Thomas Schulze
//Andrea Brücken

Schutzbedarf von IT-Verfahren

Gut geschützt im Re

In der Verwaltung geht nichts mehr ohne Informationstechnik. Fallen IT-Verfahren aus oder werden gehackt, kann das mitunter erhebliche Folgen für Staat und Gesellschaft haben. Deshalb werden IT-Systeme nach bestimmten Schutzbedarfen betrieben. Wir erklären, wie Dataport dies im Twin Data Center umsetzt.

Wenn in Schleswig-Holstein ein großer Polizeieinsatz vorbereitet oder durchgeführt wird, ist dabei die Software EPSweb (Einsatzprotokollsystem Web) im Einsatz. Mit dieser Anwendung werden Einsätze vorbereitet und dokumentiert sowie im laufenden Einsatz Informationen bereitgestellt und gesteuert.

Dataport betreibt diese Software in seinem Rechenzentrum unter ganz besonderen Vorgaben: Das Verfahren muss hoch verfügbar sein, geschützt vor Ausfällen, Datenverlust und unbefugten Zugriffen. Denn wenn das System nicht reibungslos läuft oder Unbefugte in es eindringen, könnte das Folgen für die öffentliche Sicherheit haben. Fällt es zum Beispiel aus, könnte die Organisation eines Polizeieinsatzes beeinträchtigt werden.

Deshalb steht das Verfahren nach Vorgabe der Polizei unter einem ganz besonderen sogenannten Schutzbedarf. Um diesen umzusetzen, bedarf es bestimmter Vorkehrungen im Rechenzentrumsbetrieb.

Der Schutzbedarf von EPSweb lautet: „sehr hoch“. Dies ist der höchste Schutzbedarf für IT-Systeme überhaupt. Für jedes IT-Verfahren, das Dataport in seinem Rechenzentrum betreibt, legt die Verwaltung, die mit ihm arbeitet, in einer Risikoanalyse einen Schutzbedarf fest. Dataport und die jeweiligen Behörden analysieren dazu die Verfahren. Es gilt: Je größer die Schäden sind, wenn ein Verfahren ausfällt oder seine Funktion beeinträchtig ist, desto größer ist der Schutzbedarf. Dabei richtet dieser sich nach den folgenden drei Grundwerten: Vertraulichkeit, Integrität (also Korrektheit) der mit dem Verfahren verarbeiteten Daten sowie die Verfügbarkeit des Verfahrens an sich und der mit ihm verarbeiteten Daten – Zugriff auf die Datenbanken zum Beispiel.

IT-Grundschutz ist Pflicht

Wie definiert sich der Schutzbedarf? Allgemein gilt: Es gibt in Deutschland einen Standard für Informationssicherheit, der festlegt, wie IT-Systeme von Bund und Ländern ihrem Schutzbedarf entsprechend betrieben werden müssen, und zwar das Regelwerk IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es beschreibt, wie IT-Systeme betrieben werden müssen, um sicher zu sein. Der BSI-Standard empfiehlt drei Kategorien für den Schutzbedarf von IT-Verfahren: normal, hoch und sehr hoch.

Ein Rechenzentrum an zwei Standorten

Das Polizeiverfahren EPSweb soll hoch verfügbar sein. Dies wird unter anderem durch Georedundanz umgesetzt. Dataport betreibt EPSweb, eine Eigenentwicklung der bayerischen Polizei, seit 2017

IT-Grundschutz

Der Sicherheits-Standard IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) basiert auf der internationalen Norm ISO 27001. Er beschreibt, wie Managementsysteme für Informationssicherheit aufgebaut und betrieben werden müssen. Er beschreibt außerdem Standards für Sicherheitskonzepte und Maßnahmen zur IT-Sicherheit.

IT-VERFAHREN: DREISTUFIGER SCHUTZBEDARF

- **Schutzbedarf normal:** Die Schadensauswirkungen bei Ausfällen oder Angriffen auf die entsprechenden Verfahren und IT-Systeme sind begrenzt und überschaubar.
- **Schutzbedarf hoch:** Die Schadensauswirkungen können beträchtlich sein.
- **Schutzbedarf sehr hoch:** Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen oder Leib und Leben von Menschen gefährden.

chenzentrum

georedundant in seinem Rechenzentrum. Georedundant bedeutet: an zwei Orten parallel. Dafür hat das Rechenzentrum, ein Twin Data Center, zwei identische, räumlich ein paar Kilometer voneinander entfernte Standorte, die über eine redundante Hochgeschwindigkeitsanbindung aneinander gekoppelt sind.

Faktoren für Sicherheit

Neben der Georedundanz gibt es weitere Faktoren, die für die technische Umsetzung eines Schutzbedarfs relevant sind und von Dataport konsequent in seinem Rechenzentrum umgesetzt werden: Das Gebäude, die Infrastrukturen und die Basisdienste sind hier generell nach dem Schutzbedarf der Kategorie „sehr hoch“ zertifiziert. Verfahren können im Rechenzentrum also nach diesem Schutzbedarf betrieben werden, ohne dass weitere Schutzmaßnahmen am Gebäude, der Infrastruktur und den Basisdiensten ergriffen werden müssen.

Drei Sicherheitsszenarien

Dies bedeutet jedoch im Umkehrschluss nicht, dass alle Verfahren im Rechenzentrum nach den Regeln für den Schutzbedarf der Kategorie „sehr hoch“ betrieben werden. Denn nicht alle Verfahren müssen unter höchsten Sicherheitsanforderungen betrieben werden. Die Server, auf denen Anwendungen im Rechenzentrum laufen, sind deshalb in der Standardeinstellung auf den Schutzbedarf „normal“ ausgerichtet.

Wird ein Verfahren implementiert, dessen Schutzbedarf „normal“ ist, vererbt sich dieses Niveau nach unten. Das heißt, auch Infrastrukturen, die für den Verfahrensbetrieb eingesetzt werden, entsprechen nur dieser Kategorie. Soll das Verfahren nach Schutzbedarf „sehr hoch“ betrieben werden, müssten weitere, auf das Verfahren abgestimmte Anpassungen erfolgen, um dieses Schutzniveau zu erreichen. Für den Betrieb von Verfahren hat Dataport dabei generell drei Sicherheits-Szenarien entwickelt. Von diesen Szenarien leiten sich dann die Maßnahmen ab, mit deren Hilfe der Schutzbedarf umge-

DREI GRUNDWERTE BEIM SOFTWARE- UND SYSTEMSCHUTZ

setzt wird. Generell gilt: Besonderer Schutz ist nicht ohne Aufwand – und zusätzliche Kosten für den Verfahrensbetrieb – herzustellen.

Die drei Sicherheits-Szenarien für den Verfahrensbetrieb im Rechenzentrum sind:

Reduzierte Sicherheit
Das IT-Verfahren kann nicht IT-Grundschutzkonform betrieben werden. Verfahren in dieser Kategorie müssen in einer Quarantänezone, abgeschottet von Verfahren mit höherem Schutzbedarf, betrieben werden, damit sie die Infrastruktur des Rechenzentrums und andere Verfahren nicht gefährden. Nach Möglichkeit sollten solche Verfahren, wenn es sich vermeiden lässt, nicht im Rechenzentrum betrieben werden.

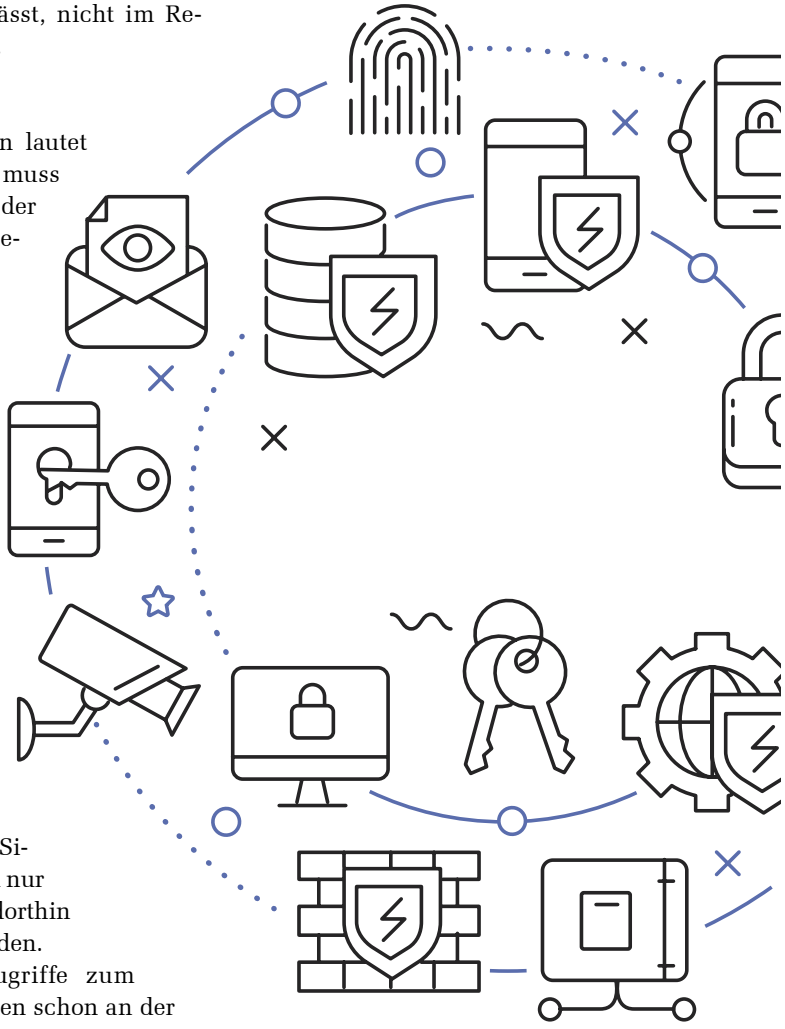
Standardsicherheit
Der Schutzbedarf für Verfahren lautet in dieser Kategorie „normal“. Er muss wie alle Schutzbedarfe von der Verwaltung, die mit den entsprechenden Verfahren arbeitet, in Auftrag gegeben werden.

Erweiterte Sicherheit
Die Verfahren in dieser Kategorie haben Schutzbedarfe in den Kategorien „hoch“ und „sehr hoch“. Für diese Schutzbedarfe „hoch“ und „sehr hoch“ fordert das BSI sogenannte Z-Maßnahmen (Z = Zusatz). Für den Schutzbedarf „hoch“ sind bei Dataport folgende Maßnahmen Standard:

› Firewalls filtern die ein- und ausgehende Kommunikation nach Quelle, Ziel und Port.
› Die Zonen der erweiterten Sicherheit sind abgegrenzt, es kann nur durch dedizierte Freischaltung dorthin oder von dort kommuniziert werden.
› Mehrere Firewall-Stufen: Zugriffe zum Beispiel aus Landesnetzen werden schon an der ersten Firewall geprüft und gegebenenfalls nicht zugelassen.
› Hinter einer zusätzlichen Firewall teilt sich die Zone in mehrere Virtual Local Area Networks (VLAN), also Teilstücke des Netzes auf, welche je Verfahren eingerichtet werden. Somit ist es nicht möglich, zwischen Verfahren unkontrolliert zu kommunizieren.
› Darüber hinaus können weitere Maßnahmen umgesetzt werden, zum Beispiel eine transparente Datenbankverschlüsselung oder der Betrieb zusätzlicher Paketfilter.

Um nun das Schutzbedarfsniveau „sehr hoch“ zu erreichen, müssen weitere individuell auf das jeweilige Verfahren abgestimmte Maßnahmen umgesetzt werden. Welche das sind, damit IT-Systeme hoch verfügbar sind und nicht manipulierbar, wird auch hier in der Risikoanalyse festgestellt.

//Kirsten Wohlfahrt
//Britta Heinrich



Fachkräfte-Nachwuchs

Trainee bei Dataport

So viele waren es noch nie: Zehn Nachwuchskräfte sind in diesem Jahr bei Dataport als Trainees eingestiegen. Seit 2009 bietet Dataport ein Programm für IT-Trainees an, um Hochschulabsolventen oder Absolventen mit ersten beruflichen Erfahrungen als neue Fachkräfte für sich zu gewinnen. Wir stellen zwei der neuen Trainees vor.

Um neue Fachkräfte zu gewinnen, bietet Dataport seit Jahren ein Programm für IT-Trainees an. Bewerben können sich Hochschulabsolventen, egal ob sie im Anschluss ans Studium erste berufliche Erfahrungen gesammelt haben oder nicht.

Das Training on the Job dauert 18 Monate. Die Trainees durchlaufen in dieser Zeit drei Abteilungen. Welche das sind, wird aufgrund verschiedener Faktoren festgelegt: individuelle Interessen und die Fachrichtung des Studienabschlusses sowie freie Kapazitäten in den Fachbereichen. Trainees arbeiten von Anfang an als vollwertige Mitarbeiter im Unternehmen mit und werden ihrer Qualifikation entsprechend mit Fach- und Führungsaufgaben betraut. Die Win-Win-Situation im Anschluss: Trainees erhalten eine Festanstellung und bleiben Dataport als kompetente und engagierte Mitarbeiter erhalten. Die nächste Auswahlrunde startet im Frühjahr 2018.

Zehn Trainees sind in diesem Jahr an Bord gekommen. Damit ist dies der am stärksten besetzte Trainee-Jahrgang seit dem Beginn des Programms 2009. Zwei dieser Nachwuchskräfte stellen ihre Motivation für die Teilnahme am IT-Trainee-Programm vor:


Sebastian Marx

Sebastian Marx verfügt sowohl über einen Bachelor in International Management with Engineering als auch über einen Master in BWL. Vor seiner Zeit bei Dataport hat er ein Jahr als Junior Business Developer bei einem IT-Unternehmen gearbeitet. „Wir Trainees kommen aus ganz verschiedenen Branchen mit unterschiedlichen Vorgeschichten. Was uns alle verbindet, ist die Affinität zur Technik“, erläutert er. „Der Aufbau des Trainee-Programms ermöglicht es uns von Beginn an, ein unternehmensweites Netzwerk aufzubauen.“ Die erste Station von Sebastian Marx ist der Bereich Lösungen, dort arbeitet er an Projekten zur Digitalisierung der Justiz mit.


Kim Ayleen Laackmann

Kim Ayleen Laackmann hat einen Bachelor in Umwelttechnik und einen Master in Renewable Energy Systems. Im Anschluss arbeitete sie zwei Jahre als Projektingenieurin im Energiemanagement und in der Energieeffizienzberatung. Ihre erste Station bei Dataport ist das Projektmanagement, sie arbeitet an der Digitalisierung im Kulturbereich mit. „Aus meinem Studium und meiner Arbeit als Ingenieurin bringe ich vertieftes Grundwissen für naturwissenschaftliche und technische Zusammenhänge mit. Das und mein persönliches Interesse für IT kann ich hier ins Berufsleben mit einbringen“, erklärt sie. „Das Trainee-Programm ist für mich interessant, weil ich durch die einzelnen Stationen das Unternehmen und die Abteilungen kennenlernen kann. Dadurch bekomme ich eine gute Orientierung für meine berufliche Zukunft bei Dataport."

//Andrea Brücken

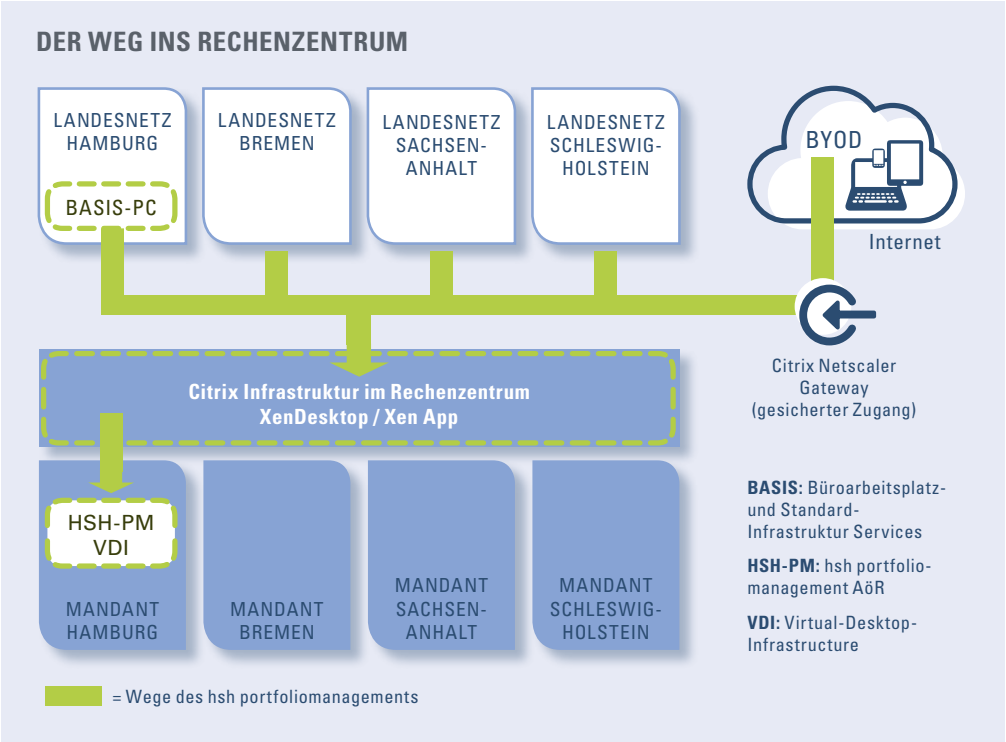
Bring your own device

Virtuelle Clients im

Wenn Mitarbeiter mit ihren eigenen Laptops und Smartphones auf das Netzwerk eines Unternehmens zugreifen und in ihm arbeiten können, nennt man das BYOD – Bring your own device. Der hsh portfoliomanagement AöR hat Dataport genau dies mithilfe von virtuellen Clients ermöglicht.

Die hsh portfoliomanagement AöR wurde im Januar 2016 gegründet und brauchte innerhalb weniger Monate einen funktionierenden IT-Basisbetrieb. Sie beauftragte daher Dataport, die komplette IT-Infrastruktur für die beiden Standorte in Kiel und Hamburg einzurichten. Die hsh portfoliomanagement AöR benötigte ein Netzwerk mit 50 bis 60 standardisierten Arbeitsplätzen inklusive der Anbindung von Telekommunikations- und Multifunktionsgeräten.

Diese sogenannte BASIS-Ausstattung – BASIS steht für Büroarbeitsplatz- und Standard-Infrastruktur Services – war für Dataport in der Umsetzung an sich nichts Neues. Neu allerdings war, sie für einen Auftraggeber aus dem Finanzwesen einzurichten. Die hsh portfoliomanagement AöR unterliegt als Finanzinstitut den Regelungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zur Bank-IT und deren Betrieb. Diese entsprechen in Teilen den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI), sind für Finanzinstitute aber keine Empfehlungen, sondern zwingend zu erfüllende Auflagen.



Virtuelle Clients

Darüber hinaus war geplant, dass Mitarbeiter der HSH Nordbank AG die Arbeit der hsh portfoliomanagement AöR unterstützen können. Die Nordbank-Mitarbeiter besitzen eigene oder durch die Bank gemanagte Geräte und arbeiten in wechselnder Besetzung. Extra für sie passende Arbeitsplätze einzurichten, wäre ein sehr aufwendiger und auch teurer Schritt gewesen.

„Wir erkennen einen großen Vorteil darin, dass die Mitarbeiterinnen und Mitarbeiter der HSH Nordbank AG nunmehr auch die Umgebung unserer portfoliomanagement auf ihren Rechnern haben“, bekräftigt Kirsten Walsemann, Leiterin der IT. „Wechselnde Besetzungen und eine begrenzte Zahl an Clients als Zielbild – diese Herausforderung galt es gemeinsam anzugehen.“ Die Lösung: virtuelle Clients – simulierte virtuelle Arbeitsumgebungen, auf die jederzeit von jedem Ort mit ein paar Klicks zugegriffen werden

Bankwesen

kann. Dieses Prinzip – mit dem eigenen Laptop oder Smartphone auf eine vorhandene technische Infrastruktur zuzugreifen – nennt man Bring your own device (BYOD). Es ermöglicht, von beliebigen mobilen Endgeräten aus in Netzwerken von Unternehmen, Schulen, Universitäten und Bibliotheken zu arbeiten.

Zugang übers Internet

Mitarbeiter der hsh portfoliomanagement AöR arbeiten über das Landesnetz Hamburg. Der Zugang mithilfe der virtuellen Clients allerdings erfolgt über das Internet. Diesem Prozess vorgeschaltet ist das Citrix Netscaler Gateway, über das sich die Nutzer mittels Zwei-Faktor-Authentifizierung validieren müssen. Es folgt die Einwahl zum Rechenzentrum über die Citrix-Software XenDesktop. Die Server des Rechenzentrums stellen dem Nutzer dann die Virtual-Desktop-Infrastruktur (VDI) zur Verfügung, auf der für jeden Benutzer das Betriebssystem und benötigte Programme abgebildet sind. Der Nutzer kann auf der Stelle im gewohnten Setting arbeiten, die Daten liegen zu jeder Zeit im Rechenzentrum.

Dr. Karl-Hermann Witte, Vorstand der hsh portfoliomanagement AöR, resümiert: „Nicht nur mit der Gründung unserer Gesellschaft, sondern auch mit unseren Anforderungen an Dataport haben wir sicherlich Neuland betreten. Dass sich eine

Mitarbeiter der hsh portfoliomanagement AöR können von überall auf das Unternehmensnetzwerk zugreifen.

erfolgreiche Zusammenarbeit entwickeln muss, ist selbstverständlich. Die Erfolgsfaktoren sind dabei eine offene Kommunikation und das Verständnis für die Arbeitsabläufe in den beiden Gesellschaften. Gemessen daran können wir nach fast zwei Jahren der Zusammenarbeit sagen: Wir sind erfolgreich unterwegs.“

Vom Pilotprojekt zum Standard

Was in der Privatwirtschaft bereits verbreitet ist, trifft zunehmend auch auf den öffentlichen Dienst zu: Es wird agiler gearbeitet, die Einbindung von externen Endgeräten in vorhandene Netzwerke kann ein wichtiges Kriterium für die Zusammenarbeit sein. Die Anwendung des Prinzips BYOD lässt sich im Rahmen der öffentlichen Verwaltung hervorragend über virtuelle Clients sicherstellen. Nach erfolgreichem Abschluss des Pilotprojektes für die hsh portfoliomanagement AöR nutzt Dataport nun die Erfahrungen aus dem Projekt, um für die Lösung eine marktfähige Produktreife zu erlangen, denn sie soll künftig auch anderen Auftraggebern angeboten werden.

//Andrea Brücken

HINTERGRUND

Die hsh portfoliomanagement AöR steht in Trägerschaft der Länder Schleswig-Holstein und Hamburg. Ihre Aufgabe ist die gewinnorientierte Abwicklung eines Portfolios notleidender Schiffskredite der HSH Nordbank mit einem Forderungsvolumen in Höhe von 4,1 Milliarden, das mit Ablauf des 30. Juni 2016 an die Anstalt übertragen wurde. Weitere Informationen zur hsh portfoliomanagement AöR finden Sie unter www.hshpm.de.

Gutachten zur Datenschutzgrundverordnung

Einheitlicher Datens
Föderalismus

Die Neugestaltung der Landesdatenschutzgesetze birgt eine außergewöhnlich große Chance für die Bundesländer: Sie können jetzt die Grundlagen dafür legen, dass Daten über Landes- und Zuständigkeitsgrenzen ungehindert fließen. Wie das geht, zeigt ein entsprechendes Gutachten.

Die Bundesländer haben mit der Umsetzung der EU-Datenschutzgrundverordnung (DSGVO) die seltene Gelegenheit, Vorschriften zu vereinheitlichen und damit eine entscheidende Grundlage für die digitale Transformation der öffentlichen Verwaltung zu schaffen.

Das zeigt ein von Dataport in Auftrag gegebenes juristisches Gutachten. Es macht auch deutlich, dass die Bundesländer ihre Landesdatenschutzgesetze vollständig überarbeiten müssen. Denn die EU-Datenschutzgrundverordnung hat nicht zum Ziel, nationales Recht zu ersetzen. Sie sieht eine Reihe von Öffnungsklauseln vor und räumt den Mitgliedstaaten einen Umsetzungsspielraum ein, enthält aber auch klare Regelungsaufträge an nationale Gesetzgeber.

Warum ist das so wichtig? So wie es zurzeit aussieht, entstehen in den verschiedenen Bundesländern gänzlich unabhängig voneinander Landesgesetzgebungen. Deren Diversität, so das Gutachten, kann zu einem entscheidenden Handicap für die digitale Transformation der Verwaltung werden. Ein Handicap, das im Zweifel nur noch durch zentrale, bundeseinheitliche Vorgaben behoben werden kann. Dabei lassen sich die notwendigen Grundlagen auch im föderalen System umsetzen. Dafür braucht es aber einheitliche Gesetzgebungen. Die sind, so das Gutachten, nicht nur ein Hebel für die Digitalisierung, sondern auch für das Schaffen von Synergien durch länderübergreifende Zusammenarbeit, zum Beispiel beim gemeinsamen Einsatz von Verfahren. In Summe lässt sich also sagen: Einheitlicher Datenschutz stärkt den Föderalismus.

Verwaltung ohne Flickenteppich

Eine hohe Diversität bei den Landesgesetzgebungen dagegen würde laut Gutachten zu Dissynergien und damit zu Ineffizienz führen. Im Ergebnis führt das zu höheren Kosten sowie zu einer langsameren und damit nicht am Interesse des Bürgers und der Wirtschaft ausgerichteten Verwaltung. Eine effiziente und hochdigitalisierte Verwaltung benötigt also einen einheitlichen Datenschutz und keinen Flickenteppich an länderspezifischen Regelungen.

Ziel der europäischen Datenschutzgrundverordnung ist nun gerade ein einheitlicher Rechtsrahmen. Für den Datenschutz in der öffentlichen Verwaltung allerdings lässt die DSGVO den Nationalstaaten und den Bundesländern Regelungsspielraum. So gibt die DSGVO zwar die rein materiellen Datenschutzziele bindend vor. Sie dürfen und sollen auf Länderebene nicht infrage gestellt werden. Verfahrensregeln dagegen

EU-DSGVO

Die EU-Datenschutzgrundverordnung ist am 24. Mai 2016 in Kraft getreten und muss ab dem Mai 2018 in jedem Mitgliedsstaat der EU unmittelbar angewendet werden. Sie löst die bisherige europäische Datenschutzrichtlinie vollständig ab.

chutz stärkt den

können gestaltet werden. Eine große Chance für die öffentlichen Verwaltungen. So könnte zum Beispiel übergreifend einheitlich festgelegt werden, unter welchen Voraussetzungen verschiedene Fachverwaltungen Daten austauschen oder gemeinsame Verfahren nutzen dürfen. Eine Frage, die für den Großteil der Digitalisierungsprojekte in der öffentlichen Verwaltung entscheidend ist.

Neue Regelungen mit Bürgernutzen

Die zurzeit noch vorliegenden Regelungen für die Übermittlung von personenbezogenen Daten (Abruf) und die Verarbeitung personenbezogener Daten aus einem Datenbestand (gemeinsames Verfahren) sind überaus heterogen. Sie können jetzt ohne weiteres vereinheitlicht werden.

Einen entsprechenden Formulierungsvorschlag hat Dataport auf Basis des Gutachtens entwickelt:

„Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf (Abrufverfahren) oder mehreren Verantwortlichen gemeinsam die Verarbeitung personenbezogener Daten aus einem Datenbestand (gemeinsames Verfahren) ermöglicht, darf eingerichtet werden, soweit dies unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Person und der Aufgaben der beteiligten Stellen angemessen ist. Die beteiligten Stellen treffen als gemeinsam Verantwortliche eine Vereinbarung gemäß Artikel 26 Absatz 1 der Verordnung (EU) 2016/679."

Mithilfe einer solchen einheitlichen Regelung könnte somit nicht nur die organisatorische Zusammenarbeit innerhalb der Verwaltungen und im Interesse der Verwaltung erleichtert werden. Sie würde zudem die übergreifende Zusammenarbeit im Interesse der Bürger ermöglichen. Denn Lebenssachverhalte der Bürger beschränken sich immer weniger auf „Zuständigkeitsräume" von Verwaltungen. So ist es zum Beispiel denkbar, dass ein Bürger seinen Wohnsitz in Bundesland A hat, während der Schulort der Kinder in Bundesland B liegt. Das effiziente Bearbeiten von Anträgen des Bürgers aber darf nicht daran scheitern, dass für Verwaltung A andere datenschutzrechtliche Verfahrensvoraussetzungen gelten als für Verwaltung B.

Das vorliegende Gutachten beschreibt die Notwendigkeit und die Möglichkeiten für die gemeinsame Gestaltung der Landesdatenschutzgesetze. Es enthält zudem eine Reihe von Vorgehensvorschlägen.

//Britta Heinrich

Das Gutachten wurde von dem Kieler Rechtsanwalt Christian Hoffmann erstellt. Es ist auf www.dataport.de abrufbar.

ITIL-Prozessmanager

Keine Änderung ohn

Im laufenden IT-Betrieb sind immer wieder Updates oder Konfigurationsänderungen erforderlich. Um Störungen zu vermeiden, organisieren Prozessmanager die Umsetzung. Uta Litzki ist im Bereich Changemanagement tätig. Sie autorisiert anstehende Veränderungen und behält die Prozesse im Blick.

Let's do IT.

Für einen reibungslosen IT-Betrieb sind klare Prozesse wichtig. ITIL-Prozessmanager geben die Prozesse im Unternehmen vor und arbeiten an deren Entwicklung und Verwaltung. Sie stellen dadurch sicher, dass Dienste jederzeit zur Verfügung stehen. Bei Dataport arbeiten Prozessmanager nach den Vorgaben des technischen Standards, der IT- Infrastructure Library, kurz ITIL. Darin sind Prozesse definiert, die typischerweise im IT-Betrieb von Unternehmen vorkommen. Dazu gehören zum Beispiel die Prozesse Change, Incident, Problem und Servicelevel.

Kontrollierte Veränderung

Ein Change ist eine geplante Änderung an der IT, die kontrolliert abläuft. Dies können Veränderungen an IT-Komponenten, Fachverfahren oder Infrastrukturen sein wie zum Beispiel ein Server-Update. Der Ablauf ist dabei stets gleich. Der Fachbereich erfasst einen Change im IT-Service-Management-Tool (ITSM-Suite) und gibt Details an: Was soll gemacht werden? Welche Auswirkungen hat die geplante Maßnahme? Was muss noch berücksichtigt werden? Prozessmanagerin Uta Litzki prüft bei kritischen Maßnahmen die Angaben, schätzt die Auswirkungen ab und genehmigt die Changes. Danach kann die Organisation und Umsetzung erfolgen. Dieses geplante Vorgehen sorgt für einen stabilen IT-Betrieb.

Risiko bewerten, Störungen minimieren

Es gibt zwei Arten von Changes. Die vorautorisierten Changes überspringen die Phase der Genehmigung und können nach Erfassung direkt umgesetzt werden. Genehmigungspflichtige Changes zur zentralen Infrastruktur werden hingegen im

ITIL-Prozessmanagerin Uta Litzki sorgt für den reibungslosen Ablauf der Prozesse im Changemanagement.

e Change

Jeder Change muss genehmigt und der Zeitpunkt für Wartungsfenster geplant werden.

Uta Litzki klärt in Absprache mit Kollegen unklare Details zu geplanten Veränderungen.

wöchentlichen Change Advisory Board (CAB) besprochen und bewertet. Uta Litzki leitet das Gremium, an dem das Betriebsmanagement sowie die entsprechenden Abteilungs- und Gruppenleiter teilnehmen. Changes mit höchster Risikostufe werden in einem gesonderten CAB besprochen, an dem auch die Bereichsleiter und Bereichsleiterinnen teilnehmen. Durch die sorgfältige Risikobewertung werden änderungsbedingte Störungen minimiert.

Prozessmanagement von der Pike auf

Uta Litzki ist gelernte Fachinformatikerin für Systemintegration. Ihre Ausbildung hat sie 2003 im Landesamt für Informationstechnik begonnen, aus dem Dataport 2004 nach einem Zusammenschluss mit anderen Institutionen hervorging. Nach einer Station im Prozessmanagement war ihr zukünftiger Arbeitsbereich schnell gefunden. Die ITIL-Zertifizierung absolvierte sie 2006 und arbeitete sieben Jahre als Prozesskoordinatorin. Weitere drei Jahre unterstützte sie im Prozessmanagement bei der Zusammenführung der Rechenzentren an einem neuen Standort. Sie entwickelte und überwachte die Betriebsprozesse sowie deren Zusammenspiel mit den ITIL-Prozessen. Seit 2017 ist sie als ITIL-Prozessmanagerin für den Changemanagement-Prozess verantwortlich. „Das war immer das, wo ich hinwollte." Als Prozessmanagerin ist sie zwar erst seit einem Jahr dabei, aber sie weiß schon jetzt: „Da gibt es viel zu tun, und da will ich weiter machen." Im Prozessmanagement geht es auch um die kontinuierliche Weiterentwicklung der Prozesse. Hieran arbeitet Uta Litzki gemeinsam mit anderen Mitarbeiterm vom Betrieb und den Prozesskoordinatoren. Sie schätzt den Austausch und die Vielseitigkeit ihrer Tätigkeit: „Für mich ist es wichtig, über den Tellerrand zu blicken, sich abzustimmen und zu wissen, was in jedem Bereich abläuft." *//Tanja Vengušt*

ITIL-PROZESSMANAGER BEI DATAPORT

Technisches Verständnis und Kommunikationsstärke sind bei Dataport Grundvoraussetzungen für die Arbeit als ITIL-Prozessmanager. Außerdem benötigt man Erfahrungen in der Prozesskoordination sowie Kenntnisse der ITIL-Prozesse. Die Zertifizierung kann bei Dataport absolviert werden. Bewerber sollten ein Studium im Bereich Informatik oder eine Ausbildung als Fachinformatiker mit mehrjähriger Berufserfahrung vorweisen können.
Für mehr Infos zur Bewerbung besuchen Sie uns auf www.dataport.de.

E-Mail-Sicherheit

Erst denken – dann klicken

Die vermeintliche Rechnung des Energieversorgers, der Link auf eine verpasste Nachricht oder ein Super-Schnäppchen – die Zahl der E-Mails, mit denen Schadsoftware verbreitet wird, steigt rasant. Doch mit etwas Besonnenheit lassen sich viele Risiken für den eigenen Computer eindämmen.

Die Zahl der verschickten E-Mails steigt von Jahr zu Jahr explosionsartig. 2017 wurden jeden Tag weltweit knapp 270 Milliarden Mails durch die Netze übertragen, für 2021 gehen die Prognosen bereits von fast 320 Milliarden Mails am Tag aus. Bei einem großen Teil dieser Nachrichtenflut handelt es sich um unerwünschte Mails (Spam), die im besten Falle lästig, im schlimmsten Falle gefährlich für den eigenen Computer sein können. Der drastische Anstieg des Mailverkehrs kommt nicht von ungefähr: Über keinen anderen Weg können Cyberkriminelle ihre Viren, Würmer, Trojaner und Betrugsattacken so einfach verbreiten wie über E-Mails. Laut dem Jahresbericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat sich die Anzahl der Spam-Mails mit Schadsoftware in Anhängen oder auf verlinkten Seiten seit Ende 2015 um 1.270 Prozent erhöht.

Schwachstelle Unvorsichtigkeit

Die Attacke über die E-Mail scheint sich zu lohnen, denn die Angreifer nutzen dabei einen gravierenden Schwachpunkt im Schutz eines Computers vor Viren aus: die Unvorsichtigkeit des Nutzers. Ein gefährlicher Anhang oder Link ist in Eile, vor Schreck oder aus Unwissenheit schnell angeklickt, und das Schadprogramm kann bei unzureichend geschützten Systemen sein Werk beginnen. Dabei ist die Qualität der trügerischen Mails inzwischen beachtlich und von Originalnachrichten zum Beispiel der Telefongesellschaft, der Versicherung oder des Energieversorgers kaum noch zu unterscheiden.

Ping: Sie haben drei neue Nachrichten. Eine davon ist mit Sicherheit Spam. Innerhalb von zwei Jahren hat sich die Anzahl von Spam-Mails um 1.270 Prozent gesteigert.

Misstrauen ist gefragt

Es heißt also: Augen auf und genau hingucken. Wie kann man sich am besten schützen? Angesichts der rasant steigenden Bedrohung ist für E-Mail-Nutzer neben aktuellem technischem Schutz wie Virenscannern und sicheren Systemeinstellungen vor allem Misstrauen gefragt. Mit etwas Besonnenheit und einfachen Plausibilitätsprüfungen lässt sich das Risiko deutlich minimieren.

› Niemals Links oder Anhänge in Mails von unbekannten Absendern öffnen. Sollte es sich um etwas Authentisches handeln, wird sich der Betreffende mit Sicherheit wieder melden.

› Bei Rechnungen und Mahnungen von bekannten Unternehmen genau überlegen: Hat man wirklich einen Vertrag ab-

geschlossen oder etwas bestellt? Hat es zu einer Mahnung überhaupt eine Rechnung gegeben? Im Zweifelsfall lieber über die Internetseite des Unternehmens das eigene Benutzerkonto öffnen und nachschauen, ob es aktuelle Dokumente gibt.

› Dateiformat von Anhängen prüfen: Auch wenn es sich offenbar um ein PDF-Dokument handelt, kann sich dahinter eine ausführbare Datei (*.exe) verbergen.

› Übersetzungen aus anderen Sprachen sind mittlerweile sehr gut. Doch oft finden sich in der Anrede oder im Text noch merkwürdige Formulierungen und Fehler. Ein Indiz für eine Fälschung.

› Bei bekannten Absendern misstrauisch sein: Ist es plausibel, dass mir derjenige einen Anhang oder einen Link schickt? Im Zweifelsfalle per Telefon oder Messenger nachfragen.

› Gewinne und Schnäppchen: Mails mit Links auf angebliche Gewinne, Erbschaften oder Super-Schnäppchen sind immer verdächtig. Niemand Seriöses hat etwas zu verschenken.

› Nicht erschrecken lassen: Abmahnungen oder Schreiben von Rechtsanwälten bekommt man per Post, niemals per E-Mail. Drohungen, dass Benutzerkonten gesperrt werden, dass es „dringenden Handlungsbedarf“ gibt oder Links auf Fotos, auf denen man angeblich zu sehen ist, sollen nur zu unbedachten Klicks verleiten.

› Hinweise von WhatsApp, Dropbox und Co. in englischer Sprache löschen: Mails von diesen großen Onlinediensten erhält man normalerweise auf Deutsch.

› Aufforderungen zur Bestätigung von Nutzerdaten ignorieren: Fordert ein bekanntes Unternehmen einen dazu auf, Nutzerdaten über einen Link zu verifizieren, ist Vorsicht geboten. Kein seriöses Unternehmen geht so vor. Anmeldebestätigungen erhält man nur dann, wenn man sich für einen Newsletter eingetragen hat.

Ein falscher Klick, und der Computer ist infiziert.

› Es empfiehlt sich, mehrere Mailadressen für verschiedene Zwecke zu verwenden. Zum Beispiel eine für Bestellungen, eine für private Korrespondenz, eine für Hobbies. Wenn dann eine Telefonrechnung in der falschen Mailbox eintrudelt, ist die Fälschung offensichtlich.

Für den Nutzer gilt also vor allem die Regel: Erst nachdenken und prüfen – dann klicken. Das ist zwar lästig und kostet Zeit, doch der Aufwand lohnt sich, wenn man den Schaden bedenkt, der durch infizierte Rechner und kompromittierte Benutzerkonten entstehen kann.

// Heiko Scharffenberg

Impressum

Herausgeber:
Dataport
Anstalt des öffentlichen Rechts
Altenholzer Straße 10-14
24161 Altenholz
Telefon (0431) 3295-0
Telefax (0431) 3295-6410
Internet: www.dataport.de
E-Mail: Britta.Heinrich@dataport.de

Redaktion: Britta Heinrich (v.i.S.d.P.)
Andrea Brücken, Kirsten Wohlfahrt

Redaktionsbeirat: Michael Hauschild, Gerd Schramm,
Sabine Wichmann, Olaf Wustrow
Reproduktion: Freie und Hansestadt Hamburg,
Landesbetrieb Geoinformation und Vermessung
Layout: Christina Walter
Auflage: 3.500, Ausgabe: 4 / Dezember 2017

Diese Ausgabe wurde auf 100 % Recyclingpapier gedruckt.

Bildnachweis

Titel: mooshny – stock.adobe.com; S. 2 Alex – stock.adobe.com, stockphoto-graf – stock.adobe.com, Maksim Kabakou; S. 4 Julien Eichinger – stock.adobe.com, adrian_ilie825 – stock.adobe.com; S. 5 vector_master – stock.adobe.com, asrawolf – stock.adobe.com; S. 6 Offenblen.de, Артем Константинов – stock.adobe.com, S. 8 Dmytro Tolokonov – stock.adobe.com; S. 10 iQoncept – stock.adobe.com; S. 11 alphaspirit – stock.adobe.com; S. 12 Wayhome Studio – stock.adobe.com; S. 15 freshidea – stock.adobe.com; S. 16 Auguste Lange – stock.adobe.com; S. 19 JFBRUNEAU – stock.adobe.com; S. 20 Th. Rafalzyk; S. 21 pict rider – stock.adobe.com; S. 22 Stefan Törmer; S. 23 Thomas Schulze; S. 25 madpixblue – stock.adobe.com; S. 26 Jane – stock.adobe.com, goolliver25 – stock.adobe.com; S. 27 Stefan Törmer; S. 29 Rea Papke; S. 30 geschmacksRaum® – stock.adobe.com; S. 32/33 Stefan Törmer; S. 33 avian – stock.adobe.com; S. 34 carballo – stock.adobe.com; S. 35 anyaberkut – stock.adobe.com.

www.dataport.de