Denn Sicherheit kommt von Verantwortung

10 Jahre digitale Aufklärungsarbeit – Perspektiven für die Zukunft

MIT 35 BEITRÄGEN VON FÜHRENDEN EXPERTEN

DsiN Deutschland sicher im Netz

10 JAHRE DSIN

Dieses Buch liefert eine Gesamtschau von Expertenbeiträgen zur Zukunft der digitalen Aufklärungsarbeit für mehr IT-Sicherheit. Weitere Eindrücke zur Debatte ermöglichen die Verweise auf den DsiN-Jahreskongress 2016 vom 27. Oktober 2016 in diesem Buch, unter anderem:

Grundsatzrede **„Denn Sicherheit kommt von Verantwortung“**, Dr. Thomas de Maizière, Bundesminister des Innern und DsiN-Schirmherr

Laudatio **„Du veränderst Deine digitale Welt“**, Klaus Vitt, Staatssekretär im Bundesministerium des Innern

Dinner Speech **„Die digitale Revolution und die Zukunft der Bildung“**, Prof. Dr. Richard David Precht, Philosoph und Publizist

sowie Bürgerforen zu Verbraucherbildung, IT-Sicherheitsdialog und innovativen Trends für IT-Schutz und Vertrauen im digitalen Alltag von Menschen und in Unternehmen.

www.10jahre.dsin.de

Die digitale Fassung dieser Publikation bietet Ihnen neben zusätzlichen Autorenbeiträgen unter anderem auch Bildergalerien und Videoaufnahmen des DsiN-Jahreskongresses 2016.

Weiterführende Links finden Sie unter den angegebenen Webadressen.

Schirmherrschaft

Bundesministerium des Innern

Ihr Leitfaden zum Buch: Digitale Aufklärung 2.0

Die Sensibilisierung und Motivation von Menschen, das Internet sicher zu nutzen, erfordert ein vielfältiges Engagement aller beteiligten Akteure der Digitalisierung. Mit „Digitaler Aufklärung 2.0“ verfolgt Deutschland sicher im Netz das Ziel mit Hilfe von drei Faktoren, die den Kapiteln dieses Buches zugrunde liegen: Aufklärung nach Zielgruppen, Vernetzung von Initiativen und Sicherheit im Dialog.

Kapitel 1

Menschen sicher erreichen – zielgruppenorientierte Aufklärungsarbeit

Defizite im sicheren Umgang mit der Digitalisierung sind bei Nutzern wie auch Unternehmen unterschiedlich ausgeprägt. Eine erfolgreiche Aufklärungsarbeit muss auf diese unterschiedlichen Bedürfnisse eingehen und individuelle Lösungen anbieten, um eine Verhaltensänderung zu bewirken. Der DsiN-Sicherheitsindex differenziert hier nach vier Verbrauchertypen: den Fatalisten, den Gutgläubigen, den Außenstehenden und souveränen Nutzern.

Ab Seite 10

Kapitel 2

Gemeinsam stark für IT-Sicherheit – Initiativen bündeln und vernetzen

Es gibt vielfältige Initiativen und Informationen für IT-Sicherheit von zahlreichen Organisationen. Um die Schlagkraft einzelner Aktionen zu erhöhen und die Koordination untereinander zu stärken, sollte die Zusammenarbeit gebündelt und zentralisiert auf geeigneten Plattformen erfolgen. Für Verbraucher und kleinere Unternehmen werden passende Angebote so leichter auffindbar.

Ab Seite 34

Kapitel 3

Gemeinsamen Dialog fördern – Technologie, Regulierung, Aufklärung

Erst das Zusammenspiel von technologischer Innovation und Regulierungs- sowie Aufklärungsmaßnahmen für Verbraucher ermöglicht es, digitalen Schutz und IT-Sicherheit herzustellen und aufrechtzuerhalten. Denn nur im gemeinsamen Dialog können ergänzende Lösungen mit allen Beteiligten gefunden und gefördert und Insellösungen vermieden werden.

Ab Seite 66

Zum 10-jährigen Jubiläum lädt DsiN alle Akteure ein, die Sensibilisierung von Menschen – beruflich und privat – für einen sicheren Umgang mit dem Internet gemeinsam zu verstärken.

www.dsin.de

www.10jahre.dsin.de

DsiN dankt dem DsiN-Mitglied SAP Deutschland für die großzügige Unterstützung zur Erstellung der Publikation.

Hinweis der Redaktion:
Die Schreibweise der personenbezogenen Hauptwörter wurde von uns nicht angeglichen, sondern in der Form belassen, die die jeweilige Autorin bzw. der jeweilige Autor gewählt hat. Wird das generische Maskulinum verwendet, mögen Leserinnen sich bitte gleichermaßen angesprochen fühlen.

Impressum

Eine Publikation zum 10-jährigen Jubiläum von Deutschland sicher im Netz e.V.

HERAUSGEBER:
Deutschland sicher im Netz e.V.
Albrechtstraße 10b
10117 Berlin
T. 030 27576 310
F. 030 27576 51310

www.10jahre.dsin.de
www.sicher-im-netz.de
info@sicher-im-netz.de

Verantwortlich und Gesamtkonzept:
Dr. Michael Littger

Konzeption und Redaktion:
Dr. Michael Littger
Anita Möllering
Joachim Schulte

VERLAG:
TEMPUS CORPORATE GmbH –
Ein Unternehmen des ZEIT Verlags
Büro Berlin:
Askanischer Platz 3, 10963 Berlin

Büro Hamburg:
Buceriusstraße,
Eingang Speersort 1,
20095 Hamburg
www.tempuscorporate.zeitverlag.de

Geschäftsführung:
Ulrike Teschke, Jan Hawerkamp

Projektleitung:
Yvonne Baumgärtel, Maria Einhorn

Grafik:
Susanne Kluge

Illustration:
Xenia Fink

Korrektorat:
Julia Kühn

Herstellung:
Dirk Woschei

Druck:
G. Peschke Druckerei GmbH

Stand: Oktober 2016

Manifest der Vielfalt

Editorial

Zum 10-jährigen Jubiläum von Deutschland sicher im Netz zeigen 41 Autorinnen und Autoren ihre Sicht auf die Zukunft der digitalen Aufklärungsarbeit. Ein Geburtstagsgeschenk, das zum Gründungsgeist von DsiN passt. Denn die Vielfalt der Stimmen und Engagements ist unsere Basis, um möglichst viele Menschen über den sicheren Umgang mit der Digitalisierung aufzuklären.

Mit erfrischender Offenheit zeigen die Autoren Herausforderungen aus der Praxis der Aufklärungsarbeit – und liefern Lösungsvorschläge. Gemeinsam gründen die Beiträge in der Überzeugung, dass digitale Aufklärungsarbeit zentral ist für IT-Sicherheit. Und dass die damit verbundene Mühe, Kreativität und Geduld in der täglichen Arbeit am Ende zu mehr Sicherheit und Vertrauen führen.

Das Buch ist damit auch ein kraftvolles Statement für die Vitalität digitaler Aufklärung, die davon lebt, dass alle Akteure einen aktiven Beitrag erbringen – heute und in Zukunft. Die drei Kapitel orientieren sich an den drei Erfordernissen der Digitalen Aufklärung 2.0: der Aufklärungsarbeit nach Zielgruppen, der Bündelung von Initiativen und dem Dialog aller Akteure.

Allen Beteiligten gilt unser Dank am heutigen Tag des Jahreskongresses. Wir freuen uns auf anregende Debatten, die wir mit dieser Publikation und der digitalen Fassung unter www.10jahre.dsin.de nachhaltig gestalten wollen.

Berlin, 27. Oktober 2016

Dr. Michael Littger
ist Geschäftsführer von Deutschland sicher im Netz e.V.

Inhalt

Grußwort

von Dr. Thomas de Maizière

Vor zehn Jahren – im Jahr 2006 – war YouTube noch ein Unternehmen, das aus weniger als 70 Mitarbeitern bestand. Im gleichen Jahr wurde es durch die Übernahme von Google zu einem der teuersten Zukäufe in der Geschichte des Internets. 2006 gab es zwar noch keine modernen Smartphones, aber durch Meldungen wie diese konnte jeder erkennen, dass die Digitalisierung immer mehr an Fahrt aufnehmen würde und damit auch die Bedeutung von Sicherheit und Vertrauen im Internet. Es war daher richtig, dass wir vor zehn Jahren Deutschland sicher im Netz gegründet haben.

Von der Gründung gingen drei Botschaften aus, die heute aktueller sind als je zuvor:

Erstens: Sicherheit, digitalen Schutz und Vertrauen können Staat und Unternehmen nur gemeinsam herstellen. Wir müssen zusammenarbeiten, unsere Kompetenzen bündeln und uns koordinieren.

Zweitens: Digitalisierung endet nicht bei Staat und Unternehmen, sondern braucht auch eine Gesellschaft, die sie positiv begleitet. Das ist nicht immer leicht – gerade wegen der vielen Veränderungen, die die Digitalisierung mit sich bringt. Deswegen braucht es viele, die mitmachen: von Pädagogen bis zu Sicherheitsexperten und von Bürger- bis zu Unternehmerorganisationen.

Drittens: Eine sichere Digitalisierung erfordert das Zusammenspiel von Gesetzgebung, Technik und Aufklärung. Die Rahmenbedingungen setzt der Staat – zum Beispiel mit dem IT-Sicherheitsgesetz. Technische Fragen werden im Kreis von Experten geklärt. Aufklärung betrifft aber alle. Sie ist ein Gemeinschaftswerk.

Heute ist diesen drei Botschaften eine weitere wichtige Botschaft hinzuzufügen: Keiner sollte von den Bürgern verlangen, beim Thema Sicherheit zu IT-Experten werden zu müssen. Die Einhaltung von IT-Sicherheitsstandards muss für jeden nachvollziehbar sein. IT-Produkte und -Dienstleistungen sollten schon in der Planungs- bzw. Entwicklungsphase standardmäßig sicher gestaltet werden, das heißt „security by design“ beinhalten, sowie mit sicheren Voreinstellungen bereitgestellt werden, also „security by default“ gewährleisten. Das ist eine der Aufgaben für heute und die kommenden Jahre.

Viele Akteure in der IT-Sicherheit haben sich Deutschland sicher im Netz angeschlossen, und der Verein ist so über die vergangenen zehn Jahre um viele Unterstützer und Partner gewachsen. Das haben wir den Mitgliedern und dem Engagement von Vorstand und Geschäftsführung zu verdanken. Die Bilanz der Projekte ist beeindruckend und setzt Maßstäbe für die nächsten zehn Jahre. Ich freue mich über die Entwicklung und wünsche mir, dass sich weitere Partner und Unternehmen diesem Engagement anschließen werden.

Ich übersende meine herzlichen Glückwünsche zu zehn Jahren Deutschland sicher im Netz und wünsche alles Gute für die Zukunft des Vereins. Es liegen zehn starke Jahre hinter Deutschland sicher im Netz. Weitere werden folgen – da bin ich sicher!

Ihr

Dr. Thomas de Maizière, MdB

www.10jahre.dsin.de

Schauen Sie, was der Bundesminister des Innern in seiner Grundsatzrede „Denn Sicherheit kommt von Verantwortung“ zum DsiN-Jahreskongress am 27. Oktober 2016 in Berlin sagte.

Dr. Thomas de Maizière ist Bundesminister des Innern und Schirmherr von Deutschland sicher im Netz e.V.

Denn Sicherheit kommt von Verantwortung

von Dr. Thomas Kremer

Noch nie war das Thema IT-Sicherheit so wichtig wie heute. Wir stecken mitten in der Digitalisierung unserer Gesellschaft: Menschen, Maschinen und Geräte werden miteinander vernetzt. Damit wird unser Leben in vielen Bereichen jetzt schon einfacher und sicherer. Das Smartphone meldet, wenn in der Wohnung eingebrochen wird. Intelligente Städte zeigen über Apps, wo ein Parkplatz frei ist, das Auto wird in naher Zukunft von selbst fahren und schwere Verkehrsunfälle werden zurückgehen.

In dem Maße, wie die Digitalisierung unserer Gesellschaft voranschreitet, wachsen aber auch Gefahren, die mit der Nutzung digitaler Geräte einhergehen. Die Verbreitung von Botnetzen, Denial-of-Service-Angriffen, Schadprogrammen, Spam, Phishing-Mails und ähnlichen Angriffen auf Endgeräte sind allgegenwärtig. Und auch der aktuelle DsiN-Sicherheitsindex 2016 hat gezeigt: Die Verbraucher fühlen sich jedes Jahr stärker verunsichert. Obwohl bei den meisten Verbrauchern das Risikobewusstsein gewachsen ist, kümmern sich weniger Nutzer um die Umsetzung sicherheitsrelevanter Vorsichtsmaßnahmen. Aufklärungsarbeit in Sachen IT-Sicherheit war noch nie so wichtig wie heute.

Der sichere Umgang mit digitalen Diensten ist wesentlich für den Erfolg der Digitalisierung. Dabei fängt IT-Sicherheit bei jedem Einzelnen an, zum Beispiel durch regelmäßige Updates seiner Programme, den Einsatz aktueller Virenscanner und die sichere Speicherung von Daten – und das nicht nur am Computer, sondern auch auf dem Smartphone. Noch wichtiger ist allerdings ein steigendes Sicherheitsbewusstsein. Denn das sicherste Programm kann nicht verhindern, dass User unachtsam auf E-Mail-Anhänge klicken, sich auf dubiosen Seiten aufhalten oder fremde USB-Sticks in den Rechner stecken.

IT-Nutzer denken und handeln sehr unterschiedlich. Der DsiN-Sicherheitsindex unterscheidet vier Verbrauchertypen: fatalistische Nutzer, außenstehende Nutzer, gutgläubige Nutzer und souveräne Nutzer. IT-Sicherheit funktioniert nur über gezielte Aufklärungsarbeit, die die Zielgruppe und deren Kenntnisstand berücksichtigt. DsiN leistet hierzu mit seinen unterschiedlichen Aufklärungsangeboten für eine Vielzahl von Zielgruppen einen wichtigen Beitrag.

Aufklärungsarbeit benötigt zudem einen langen Atem. Verbraucher werden bei Hilfestellungen in Sachen IT-Sicherheit kritischer. Anbieter von Aufklärungsangeboten müssen ihre Glaubwürdigkeit unter Beweis stellen, um als neutrale Anbieter akzeptiert zu werden. Verbraucher wie auch kleine und mittelständische Unternehmen müssen Zeit haben, das Angebot des Hilfeanbieters kennen zu lernen und Vertrauen aufzubauen. Auch bringen nur kurzfristig angelegte Aufklärungsinitiativen wenig Erfolg. Erst über einen längeren Zeitraum stellen sich Veränderungen im Nutzungsverhalten ein. Mit Angeboten wie dem Jugendwettbewerb myDigitalWorld, IT-Sicherheits-Workshops für Entscheider im Mittelstand, digitalen Stammtischen für Senioren sowie der Initiative Digitale Nachbarschaft zur Information ehrenamtlich engagierter Menschen ist DsiN auf einem guten Weg. Das zeigt auch das positive Feedback zur Sicherheitsbarometer-App (kurz: SiBa), die über aktuelle Bedrohungen im Netz informiert.

Damit Bürger aufgeklärt, bewusst und sorgfältig handeln können, bedarf es einer nachhaltigen und an den Bedürfnissen einzelner Nutzergruppen orientierten Aufklärungsarbeit. DsiN agiert mit langfristig angelegten Projekten, um nachhaltig Veränderungen zu bewirken. Dabei ist Aufklärungsarbeit immer wieder Pionierarbeit. Denn die Digitalisierung schreitet voran und neue Produkte kommen immer schneller auf den Markt. Für eine bedarfsorientierte Aufklärungsarbeit ist die Zusammenarbeit aller Beteiligten gefragt. Nur wenn Politik, Gesellschaft, Unternehmen, Wissenschaft und Verbraucher gemeinsam an einem Strang ziehen, kann Aufklärungsarbeit in Sachen IT-Sicherheit funktionieren.

Die Gründung des Vereins Deutschland sicher im Netz als eine objektive, produktneutrale, herstellerunabhängige und gemeinnützige Vermittlungsstelle vor zehn Jahren war ein wichtiger Meilenstein bei der Bündelung von Aufklärungsangeboten zum Thema IT-Sicherheit in Deutschland. Wenn es DsiN heute nicht bereits gäbe, müsste der Verein neu erfunden werden.

Mit dieser Festschrift zum 10-jährigen Jubiläum möchten wir Ihnen zeigen, wie DsiN Menschen erreicht und wie Mitglieder, Förderer und Unterstützer sich die Zukunft der digitalen Aufklärungsarbeit für Verbraucher und kleine und mittelständische Unternehmen vorstellen.

www.10jahre.dsin.de

Schauen Sie, was der DsiN-Vorstandsvorsitzende in seiner Eröffnungsrede auf dem Jahreskongress zum 10-jährigen Jubiläum von Deutschland sicher im Netz sagte.

Dr. Thomas Kremer
ist Vorstand für Datenschutz, Recht und Compliance bei der Deutsche Telekom AG und seit 2015 Vorstandsvorsitzender von Deutschland sicher im Netz e.V.

Menschen sicher erreichen – zielgruppenorientierte Aufklärungsarbeit

Aufklärungsmaßnahmen nach dem Gießkannenprinzip erzielen wenig Wirkung. Um Menschen zu erreichen und ihr Sicherheitsverhalten zu verbessern, müssen ihre individuellen Bedürfnisse besser berücksichtigt werden. Dafür gibt es viele spannende Ansätze, die sich lohnen: Denn ein sorgsamer Umgang mit dem Internet würde über 90 Prozent aller Cyberangriffe abwehren. Und erst im sicheren Internet kann sich das ganze Spektrum digitaler Möglichkeiten voll entfalten.

One size doesn't fit all!

Verbraucher sind verschieden, deshalb gelingt Aufklärung nur, wenn sie an individuelle Bedürfnisse angepasst ist.

von Heiko Maas

Zehn Jahre können in der Geschichte eines Vereins eine kurze oder eine lange Zeit sein. Für die großen Fußballvereine sind sie eher eine kurze Zeit, denn sie wurden meist um 1900 gegründet und sind damit über hundert Jahre alt. Für einen Verein, der sich mit der Sicherheit im Internet befasst, sind im Zeitalter der Digitalisierung dagegen schon zehn Jahre eine lange Zeit. Erinnern wir uns an das Jahr 2006: In jenem Jahr wurde Twitter gegründet und MySpace war mit gerade einmal 75 Millionen Nutzern das größte soziale Netzwerk; Facebook fing an, den Hochschul-Campus zu verlassen und Handys wurden ausschließlich zum Telefonieren genutzt, denn Smartphones gab es noch nicht. Trotzdem – auch damals hat Sicherheit im Internet schon viele Menschen bewegt. Deshalb war die Gründung des Vereins Deutschland sicher im Netz im Jahr 2006 ein richtiger Schritt. Seither ist DsiN immer auf der Höhe der Zeit und hat Verbraucherinnen und Verbraucher zuverlässig bei Sicherheitsfragen im Internet unterstützt. Dafür danke ich dem Verein und seinem Team und deshalb gratuliere ich herzlich zu diesem Jubiläum.

Was mir an der Arbeit von Deutschland sicher im Netz besonders gefällt, ist der klare Blick für die unterschiedlichen Bedürfnisse und Ansprüche der Verbraucher. Dies spiegelt sich im DsiN-Sicherheitsindex wider, wo zwischen vier Verbrauchertypen unterschieden wird: Der „außenstehende Nutzer" kennt sich mit den Schutzmaßnahmen nicht so gut aus, ist häufig älter und in der Mehrzahl weiblich. Der „gutgläubige Nutzer" hat wenig Gespür für die Gefahr und ergreift deshalb keine Schutzmaßnahmen. Der „fatalistische Nutzer" ist meist jünger, fühlt sich zwar bedroht, aber unterlässt Schutzmaßnahmen, obwohl er sie kennt. Der „souveräne Nutzer" schließlich ist das Ideal: Er kennt sich mit Schutzmaßnahmen gut aus und wendet diese auch an.

Ich sehe hier deutliche Parallelen zum Ansatz der Bundesregierung, der Verbraucherpolitik ein differenziertes und damit realistisches Verbraucherleitbild zugrunde zu legen. Statt das Ideal eines mündigen Verbrauchers zu beschwören, akzeptieren wir, dass Menschen verschieden sind und in unterschiedlichen Situationen verschieden handeln. Verbraucherwissenschaftler differenzieren dementsprechend zwischen „verletzlichen", „vertrauenden" und „verantwortungsvollen" Verbrauchern, wobei ein und dieselbe Person je nach Situation mal der einen und mal der anderen Kategorie angehören kann.

Aus dieser Verschiedenheit ergeben sich Konsequenzen für eine moderne Verbraucherpolitik: Wenn Verbraucher besonders verletzlich sind, weil es ihnen etwa an Sachkunde oder Erfahrungen fehlt oder weil es um sehr schwierige Materien oder weitreichende Entscheidungen geht, dann brauchen wir passgenaue Informationen. Deshalb orientieren sich die Informationsprojekte unseres Ministeriums an der Situation der Verbraucherinnen und Verbraucher; deshalb haben wir differenzierte Angebote, zum Beispiel zugunsten von Älteren, Migranten und Menschen in besonderen sozialen Lebenslagen.

Für einen Verein, der sich mit der Sicherheit im Internet befasst, sind im Zeitalter der Digitalisierung zehn Jahre eine lange Zeit.

Auch Deutschland sicher im Netz unterscheidet bei seiner Aufklärungsarbeit nach Nutzergruppen. Die Angebotspalette ist breit und reicht von Informationsmaterialien und Tutorials über Wissenschecks, das Sicherheitsbarometer als App bis hin zu Wettbewerben für verschiedene Altersgruppen. Besonders hervorheben möchte ich den Digital-Kompass, den DsiN gemeinsam mit der Bundesarbeitsgemeinschaft der Senioren-Organisationen (BAGSO) betreibt, um Seniorinnen und Senioren bei der aktiven und sicheren Teilhabe am Internet zu unterstützen. Ehrenamtliche Helferinnen und Helfer erhalten Lehr- und Übungsmaterialien, Präsentationsvorlagen und die Möglichkeit, sich mit Gleichgesinnten deutschlandweit auszutauschen. Experten berichten ihnen aus erster Hand zu aktuellen Themen rund ums Internet. Das Bundesministerium der Justiz und für Verbraucherschutz fördert dieses Projekt, und Staatssekretär Gerd Billen hat die Schirmherrschaft für den Seniorenwettbewerb „Der goldene Internetpreis" übernommen.

Dies ist nur ein Beispiel für eine differenzierte, zielgruppenorientierte Aufklärungsarbeit. Es gibt viele weitere. Ich wünsche DsiN auch für die nächsten zehn Jahre eine erfolgreiche Aufklärungsarbeit und viele interessierte Nutzerinnen und Nutzer. Ich bin gespannt, welche Innovationen die Digitalwirtschaft bis zum Jahr 2026 noch für uns parat hat. Eines wird aber unverändert bleiben: Das Bedürfnis der Menschen nach Sicherheit im Netz. Deshalb bleibt die Arbeit von DsiN auch in Zukunft so wichtig!

Heiko Maas
ist Bundesminister der Justiz und für Verbraucherschutz

„Passiert schon nichts!“

Ein Mann stürzt vom Hochhaus. Als er das dritte Stockwerk passiert, denkt er: „Puh, bis jetzt ist alles gut gegangen!“ Der makabre Witz transportiert eine lebensbejahende Botschaft: Bitte nicht warten, bis es zum Schlimmsten kommt. Ein guter Tipp, gerade für den Umgang mit IT-Sicherheit.

Warum kümmern sich Menschen und Unternehmen oft erst um ihre IT-Sicherheit, wenn es zu spät ist?

Dr. Frank Keller
Geschäftsführer PayPal Deutschland, Österreich und Schweiz
Der Gedanke „Bis jetzt ist noch nie etwas passiert“ trügt leider nicht selten im Zusammenhang mit IT-Sicherheit. Die jüngere Generation geht oft zu sorglos mit neuen Technologien um und auch ältere Menschen werden schnell zu einem leichten Ziel von Angreifern im Netz. Zwar wissen alle um die Gefahren, scheuen aber den damit verbundenen Aufwand – und beschäftigen sich erst damit, wenn es zu spät ist. Für Unternehmen, die im Netz agieren, heißt das: Sie müssen sichere Produkte und Dienstleistungen anbieten, die sich zugleich komfortabel nutzen lassen. Wenn sie beide Aspekte – wirksamen Schutz und einfache Handhabung – miteinander kombinieren, gewinnen sie das Interesse der Verbraucher. Auch deshalb haben wir bei PayPal eines der komplexesten Betrugspräventionssysteme weltweit entwickelt. Es nimmt mit jeder Transaktion, die über unser System läuft, an Intelligenz zu – stets mit dem Ziel, Betrügern einen Schritt voraus zu sein.

Dr. Ulrike Struwe
Geschäftsführerin Kompetenzzentrum Technik-Diversity-Chancengleichheit
„Wer sollte ausgerechnet an meinen Daten Interesse haben?” Diese Frage höre ich oft. Interesse am Schutz der eigenen Daten ist zwar vorhanden, aber die meisten Verbraucher wissen wenig über die Gefahren im Internet. Dasselbe gilt für die Schutzschilder wie Verschlüsselung, Antivirenprogramme oder Sicherheitskopien. Informationen darüber gibt es zwar zuhauf, doch befinden sich Verbraucher in einer Holschuld: Wer sucht, wird fündig. Wer nicht sucht, bleibt ungeschützt. Das betrifft die Jüngeren vor allem in sozialen Netzen und bei Ortungsdiensten, die Älteren im sicheren Umgang mit E-Mails, Einkäufen und Bankgeschäften über das Internet. Würde mit jedem Kauf eines Computers, Notebooks oder Smartphones ein DsiN-Handbuch – gedruckt und digital – ausgegeben, das praxisnah Risikoszenarien und die entsprechende Vorsorge darstellt, bekäme das Thema einen ganz anderen Stellenwert.

Prof. Dr. Sachar Paulus
Experte für IT-Sicherheit an der Hochschule Mannheim und im Beirat von Deutschland sicher im Netz e.V.
Jedes Jahr unterrichte ich Internetsicherheit in Schulen. Begeisterung schwappt mir entgegen, wenn ich elektronische Geräte auspacke und neue, interaktive Spiele zeige. Wenn es dann um die Regeln geht, wie man sich sicher im Internet und in der Welt der Apps bewegt, hören mir die Kids kaum noch zu. Senioren interessiert eher, ob Online-Banking sicher ist, wie sie eine Reise im Internet sicher buchen oder wie man sich gegen Online-Betrüger wehrt. Auch hier gilt: Bei den Regeln zum sicheren Verhalten hört kaum noch jemand zu. Dafür gibt es eine psychologische Erklärung: Das Erläutern von technischen Sachverhalten wird wohlwollend aufgenommen, das Vermitteln von Regeln und Verhaltensweisen hingegen eher als bevormundend verstanden. Als Eingriff in die persönliche Freiheit werden sie abgelehnt. Tipps sind erwünscht – aber nur, solange sie als Vorschlag und Alternative daherkommen.

Von Nutzern lernen

Aufklärung darf keine Einbahnstraße sein

von Thomas Krüger

Der Großteil aller Zwölf- bis Dreizehnjährigen in Deutschland (86 Prozent) besitzt laut JIM-Studie 2015 ein Smartphone – die Mehrheit davon (62 Prozent) verfügt dazu über ein All-Inclusive-Paket mit Internet-Flatrate. Unsere Kinder bewegen sich damit wie selbstverständlich und weitgehend unabhängig von der Hilfe oder gar Kontrolle ihrer Eltern in den sozialen Netzwerken. Sie nutzen ihr Smartphone als Werkzeug, beispielsweise um Bilder von sich zu machen und auf verschiedenen Plattformen online zu stellen – oder sie vertreiben sich die Zeit mit digitalen Spielen.

Was wäre, wenn unsere Kinder auf das gehört hätten, was Pädagoginnen und Pädagogen noch vor wenigen Jahren ihren Eltern geraten haben? Dass Smartphones nichts für Kinder seien, weil sie ihre persönlichen Daten aufzeichnen („ausspähen"), weil sie sie auswerten („überwachen") und damit immer neue Nutzungsweisen eröffnen („kontrollieren")? Was wäre, wenn sie auf ihre Eltern gehört hätten, die das Smartphone allenfalls als Telefon akzeptiert haben, das sie anrufen können, wenn sie sich um ihre Kinder Sorgen machen? Was wäre, wenn sie auf ihre Schulleiterinnen und Schulleiter gehört hätten, die das Smartphone – bis heute – gerne verteufeln und zum Teil radikal aus dem Schulalltag verbannen, indem sie die Benutzung auf dem Schulgelände verbieten? Wie froh müssen wir sein, dass uns unsere Kinder nicht für voll genommen haben. Dass sie mutig auf das Neue zugegangen sind, dass sie alte Werte über Bord geworfen und neue Werte kultiviert haben.

Wer sich Neues aneignen will, muss oft etwas anderes aufgeben. Dieses Prinzip der „Schöpferischen Zerstörung" ist im Prozess der Digitalisierung besonders sichtbar. Um Informationen zu teilen, muss ich diese preisgeben. Wer dagegen nicht möchte, dass andere Menschen Dinge über ihn wissen, der kann sich nicht sinnvoll an sozialen Netzwerken wie Twitter oder Facebook beteiligen. Ob es nur um das Wetter geht, um Eindrücke aus dem Urlaub oder um die Meinung zum aktuellen Zeitgeschehen – wer nicht spricht, wird nicht gehört.

„Sicher im Netz" setzt voraus, „im Netz" zu sein – Medienaskese kann also nicht unser Ziel sein. Sicherheitsbemühungen müssen auf die tatsächlichen Nutzungsweisen abgestimmt sein und dürfen diese nicht erschweren. Sonst surfen die User um sie herum. Ein Netzwerk wie Deutschland sicher im Netz ergibt also nur dann Sinn, wenn es die gewünschten Nutzungsweisen nicht behindert, sondern unterstützt. Sicherheitsregeln werden immer dann ignoriert, wenn sie zu kompliziert werden. Daten werden nicht mehr händisch gesichert, Passwörter auf zahlreichen Plattformen wiederverwendet, Trivialpasswörter gesetzt – und Smartphones nicht verschlüsselt. Was nützen all die Sicherheitsvorkehrungen, wenn sie in Wahrheit Sicherheitsbehinderungen sind, weil sie niemand gerne – und nur ein geringer Teil überhaupt – nutzt?

FATALISTISCHE UNBEDARFTHEIT

Es geht also nicht nur um die Vermittlung von Wissen an die Nutzerinnen und Nutzer. Insbesondere die Jüngeren unter ihnen sind bereits erstaunlich nutzungskompetent. Wenn sie trotzdem einen Hang zur fatalistischen Unbedarftheit entwickelt haben, dann auch, weil wir ihnen keine alltagstauglichen Sicherheitsmechanismen zur Verfügung gestellt haben. Hand aufs Herz: Haben Sie Passwörter mehrmals vergeben? Oder wissen Sie, was Ihre Smartphone-Apps und Nutzerkonten alles an Daten über Sie sammeln und was mit diesen Daten geschieht?

Eben. Weil niemand so recht versteht, wie sein E-Mail-Programm Nachrichten verschlüsselt, und dies ohnehin nur dann Sinn ergibt, wenn es die meisten anderen auch machen, verschlüsseln Sie Ihre Mails nicht. Weil jeder noch so kleine Online-Shop und jede Online-Community von Ihnen ein Passwort verlangen, können Sie sich die schiere Menge an mitunter kryptischen Zeichenfolgen nicht mehr merken. Sie sind zwar dereinst mit guten Vorsätzen gestartet, haben jedoch letztlich aufgegeben, für jede Seite ein individuelles Passwort zu vergeben. Ich darf Ihnen verraten: Sie sind nicht allein. Sie könnten außerdem jedem erklären, was Datenschutz bedeutet. Auf Ihrem Smartphone allerdings läuft ein Betriebssystem von Google oder Apple. Sie füttern mit Ihrem Gerät die riesigen Datenschätze der beiden Weltmarktführer. Sie tun dies und wissen darum. Aber die Websuche ist eben so furchtbar praktisch, alle Apps sind automatisch auf dem neuesten Stand und die Navigation weiß besser Bescheid über den Stau um die Ecke als der Verkehrsfunk im Radio.

Für das Projekt Sicherheit im Netz bedeutet das, dass wir alle die Denkrichtung ändern müssen. Produkte wie Google Maps und die Sprachsuche sind so nutzerfreundlich, weil deren Anbieter irgendwann angefangen haben,

MYDIGITALWORLD

Der Jugendwettbewerb myDigitalWorld in Kooperation mit der Bundeszentrale für politische Bildung fordert junge Menschen der acht bis elften Schulklasse auf, zu zeigen, wie sie ihre digitale Welt sicherer machen. DsiN führt den Wettbewerb mit Förderung des Bundesministeriums des Innern sowie Deutsche Telekom, Google und Ericsson als Paten durch. Den Gewinnern winken Klassenfahrten sowie Geld- und Sachpreise. Einreichungen sind bis zum 12. Dezember 2016 möglich:

www.mydigitalworld.org

den Informationsfluss umzukehren: nicht mehr vom Produkt zu den Nutzenden, sondern von den Nutzenden zum Produkt. Eben weil die Art, wie diese Werkzeuge verwendet werden, ausgewertet wird, eben weil ihre Anbieter merken, wenn es irgendwo hapert, eben weil die Nutzenden diese Werkzeuge beständig mit Wissen füttern, eben darum sind diese Anwendungen so erfolgreich. Was wäre, wenn wir diese Umkehrung auf unsere Vermittlungsbestrebungen übertragen würden? Wenn es nicht mehr um „Vermittlung“ oder gar „Aufklärung“ ginge, sondern darum, die geballte Expertise aller anzuzapfen?

NUTZEREXPERTISE ERFRAGEN

Kürzlich hat die Bundeszentrale für politische Bildung (bpb) wieder ein „BarCamp“ ausgerichtet. Das Besondere an so einer „Un-Konferenz“ ist, dass sie ohne zuvor eingeladene Redner und PowerPoint-Präsentationen auskommt. Beim BarCamp werden alle Teilnehmerinnen und Teilnehmer dazu angeregt, eigene Themenvorschläge ad hoc einzubringen. Diese werden gesammelt, und wenn sich genug Interessierte finden, werden dazu Diskussions- und Arbeitsrunden veranstaltet. In einem solchen Format würden insbesondere jene Stimmen hörbar, die bislang als „fatalistisch“ oder „gutgläubig“ gelten. Sie könnten Hürden aufdecken und Ansätze liefern, wie diese zu beseitigen wären. Und es spräche nichts dagegen, sich danach gleich ans Werk zu machen. Denn wenn mit den Nutzerinnen und Nutzern die eigentlichen Fachleute einmal zusammengekommen sind, warum laden wir sie dann nicht noch auf einige weitere Tage ein, um konkrete Lösungen zu erarbeiten?

Um die Kluft zwischen Sicherheitsanspruch und Nutzungswirklichkeit zu überwinden, müssen nicht nur die Verbraucher, sondern wir alle selbstkritisch sein. Denn wer kann schon die ganze digitale Welt erklären? Was wir hingegen können, ist die Menschen dort abholen, wo sie stehen, nämlich in ständiger Nutzung. Wir können sie für Sicherheit im Netz sensibilisieren, um dann gemeinsam beiderseitige Bildungsprozesse zu gestalten. Dabei dürfen wir nicht unsere Werte vorgeben, sondern müssen diese gemeinsam aushandeln.

Ich bin der Überzeugung, dass jeder Mensch bestimmte Expertisen aufweist und etwas zu erzählen hat. Durch die Kooperation des bpb-Schülerwettbewerbs mit „myDigitalWorld“ motivieren wir Schülerinnen und Schüler, ihre Nutzungsgewohnheiten zu reflektieren und auch ihr „digitales Ich“ besser kennen zu lernen. Ich bin gespannt darauf, was sie dabei entdecken und berichten. Auch wenn wir nicht allem zustimmen werden, so lohnt es sich doch sicher, zuzuhören. Zeit, damit zu beginnen.

www.10jahre.dsin.de

Schauen Sie, was Klaus Vitt, Staatssekretär im Bundesministerium des Innern, in seiner Laudatio zum Jugendwettbewerb myDigitalWorld sagte, der 2016 mit dem Schülerwettbewerb der Bundeszentrale für politische Bildung kooperiert.

Thomas Krüger
ist Präsident der Bundeszentrale für politische Bildung (bpb)

IT-Sicherheit für alle – Ideen, Inhalte, Initiativen

von Dr. Wieland Holfelder

Wie können wir den sicheren Umgang mit digitalen Diensten für alle Bürger fördern? Mit dieser Schlüsselfrage beschäftigen wir uns bei Deutschland sicher im Netz (DsiN) inzwischen seit zehn Jahren. Wir sind uns darin einig, dass sowohl Bewusstsein als auch Kenntnisse nur durch neue, zielgruppenspezifische Ansätze vermittelt werden können. Genau wie die Online-Angebote, deren Komfort wir alle so zu schätzen wissen, müssen auch unsere Initiativen passgenau auf die Bedürfnisse der jeweiligen Nutzergruppen zugeschnitten sein.

Drei Beispiele sollen exemplarisch zeigen, wie ein doch manchmal recht sperriges Thema wie IT-Sicherheit mit frischen Ideen an verschiedene Zielgruppen vermittelt werden kann:

BOTTOM-UP: BERUFSSCHÜLER FÜR IT-SICHERHEIT

Ein gutes Beispiel für unseren Ansatz, Zielgruppen mit passenden Angeboten anzusprechen, ist das Projekt „Bottom-Up“. Die Idee: Multiplikatoren zum Thema IT-Sicherheit zu identifizieren und diese mit einem intelligenten Programm zu aktivieren. Eine wichtige Zielgruppe sind hier Berufsschülerinnen und Berufsschüler. Diese jungen Menschen sind die ersten ihrer jeweiligen Jahrgänge, die im Rahmen der Ausbildung den betrieblichen Arbeitsalltag kennen lernen. Häufig arbeiten sie in kleinen und mittelgroßen Unternehmen, in denen Ressourcen für IT-Sicherheit knapp bemessen sind. Durch Unterrichtseinheiten, die im Rahmen von „Bottom-Up“ verfügbar sind, können sich Auszubildende auch aus kleineren Betrieben ein Basiswissen zu praktischer IT-Sicherheit aneignen und in ihre Ausbildungsbetriebe mitnehmen. „Hallo Chef, um Ihr Smartphone abzusichern, sollten Sie sich schleunigst mindestens einen Entsperrcode zulegen!“ Solche praktischen und überaus wichtigen Beispiele erlernen Auszubildende bei „Bottom-Up“, Auszubildende, die ihre Kenntnisse praktisch anwenden. Wir freuen uns, dass dieses Projekt auch vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird.

DIGITALE NACHBARSCHAFT

Auch diese Initiative unterstützt bundesweit Multiplikatoren, die Vereinen und engagierten Bürgern in Deutschland Hilfestellung beim

sicheren Umgang mit dem Internet geben. Das Vorhaben reagiert auf die wachsende Digitalisierung in ehrenamtlichen Organisationen, denen meist nur rudimentäre Kompetenzen und Maßnahmen in IT-Sicherheit und Datenschutz gegenüberstehen. Die Initiative schult über die nächsten Jahre mehr als eine Million Bürger in grundlegenden Fragestellungen der IT-Sicherheit. Für eine breitenwirksame Vermittlung werden ehrenamtlich engagierte Bürger und Vereinsmitarbeiter als IT-Trainer, sogenannte „Scouts“, zur Weitervermittlung von digitalem Sicherheitswissen befähigt. Eine zentrale Anlaufstelle im Internet bündelt alle Aktivitäten und Materialien des Projekts in einer digitalen Lernplattform.

Auf dem Lehrplan stehen relevante Themen für den Vereins- und Lebensalltag von Anwendern: Vom erfolgreichen Auftritt in sozialen Medien, über sichere digitale Mitgliederverwaltung und Buchführung, bis hin zu Crowdfunding werden Koordinatoren und Funktionsträger geschult. Ehrenamtliche erlernen unter anderem digitale verschlüsselte Kommunikation und den sicheren Umgang mit Bezahlung und Datenschutz im Internet.

Scouts, die sich bei der „Digitalen Nachbarschaft“ ausbilden lassen, profitieren gleich dreifach: Sie leisten mit ihrem Engagement nicht nur einen zentralen Beitrag zur digitalen Transformation ihrer ehrenamtlichen Organisation, sondern erhalten auch ein offizielles Weiterbildungszertifikat, mit dem sie die erlangten Qualifikationen beruflich nutzen können. Außerdem werden sie Teil einer bundesweiten Community und profitieren dauerhaft von aktuellem Wissen und Aktionen rund um das Thema Sicherheit im Internet. Das Projekt wird vom Bundesministerium des Innern gefördert, und auch Google unterstützt es von Anfang an.

DER GOLDENE INTERNETPREIS

Bereits jeder zweite über 60-Jährige ist regelmäßig im Internet unterwegs. Der Goldene Internetpreis prämiert Menschen dieser Altersgruppe, die das Internet selbst kompetent nutzen sowie auch solche, die andere dabei begleiten, in die Onlinewelt einzusteigen. Ein Sonderpreis zeichnet außerdem besondere Projekte aus, die mit mehreren Generationen verwirklicht werden. Dabeisein ist einfach. Teilnehmen kann, wer über 60 Jahre alt und online aktiv ist. Egal, ob als Nutzer von Internetplattformen, Kommunikations- und Organisationstools oder Apps – jeder, der die vielfältigen Möglichkeiten des Internets im Alltag oder für gesellschaftliches Engagement nutzt, ist ein möglicher Gewinner beim Goldenen Internetpreis. Häufig sind es interessante persönliche Geschichten und (Aha-)Erlebnisse, die Teilnehmer mit dem Internet verbinden. Und wer andere beim Erlernen und Erleben der Möglichkeiten des Internets begleitet, ist bei dem Wettbewerb ohnehin goldrichtig.

> Häufig sind es persönliche Geschichten, die Teilnehmer mit dem Internet verbinden.

Vorbild für andere sein und zeigen, wie vielfältig und nützlich das Internet sein kann – für Menschen jeden Alters: Dafür soll der Goldene Internetpreis Beispiele finden und würdigen. Und für das überaus ehrenwerte „Problem“, das die Engagierten im Lande häufig auch bescheidene Leute sind, gibt es eine Lösung: Freunde, Bekannte und Familienmitglieder können die über 60-jährigen „Digitalprofis“ ebenfalls nominieren.

Der Goldene Internetpreis hat in der Vergangenheit schon tolle Beispiele für die Online-Begeisterung der über 60-Jährigen zutage gefördert. Da diese Bevölkerungsgruppe in Zukunft weiter wachsen wird, bleibt DsiN am Ball. Ansporn für weiterhin gute Arbeit haben wir: die Schirmherrschaft durch das Bundesministerium der Justiz und für Verbraucherschutz.

Darüber hinaus unterstützt Google, das ich im Vorstand von DsiN vertreten darf, den Verein bei weiteren zielgruppenspezifischen Aktivitäten. Es ist dabei von Vorteil, dass das Unternehmen selbst in Deutschland an den Themen Datenschutz und -sicherheit arbeitet. Von hier aus werden Produkte zum Schutz der Privatsphäre weltweit entwickelt. Erst im Frühjahr 2016 wurde unser neues Entwicklungszentrum in München eröffnet und bezogen. (Dass unsere neuen Räumlichkeiten ausgerechnet nahe der Münchener Hackerbrücke liegen, ist für uns Computerexperten natürlich ein netter Zufall.)

Ein kurzer Blick in unsere bayerische „Datenschutzwerkstatt“: Hier wird der Web-Browser Chrome in Sachen „Datenschutz“ betreut. Ein bekanntes Beispiel ist der Password Manager, mit dem man sich diverse (hoffentlich stets unterschiedliche!) Passwörter auf verschiedenen Webseiten merken kann.

Auch der Dienst MyAccount (Mein Konto) wurde in München entworfen und programmiert. Eine zentrale Anlaufstelle, über die Nutzer schnell und komfortabel Daten verwalten und Datenschutzeinstellungen vornehmen können inklusive eines Privatsphäre- und Sicherheitschecks. 2015 wurde MyAccount für alle Nutzer weltweit eingeführt und binnen eines Jahres von über einer Milliarde Menschen weltweit genutzt.

Der überwiegende Teil unserer Mitarbeiterinnen und Mitarbeiter am Münchener Standort, den ich leiten darf, sind Software-Ingenieure. Sie kommen aus über 30 Ländern. Hier zeigt sich, dass Deutschland längst zu einem Zentrum für Know-how in Sachen IT-Sicherheit geworden ist.

Ich bin fest davon überzeugt: Wenn wir alle gemeinsam – Unternehmen, Initiativen wie DsiN und öffentliche Stellen – auch in Zukunft unseren Teil beitragen, werden wir die Nutzung des Internets gemeinsam immer sicherer machen. Liebes DsiN, herzlichen Glückwunsch und auf gute und vor allem sichere weitere zehn Jahre!

„Bottum-Up“ als ein Beispiel für zielgruppenspezifische Aufklärungsarbeit an Berufsschulen ist im Internet unter www.dsin-berufsschulen.de abrufbar. Die Heimatseiten der „Digitalen Nachbarschaft“ sind unter www.digitale-nachbarschaft.de erreichbar.

Dr. Wieland Holfelder
ist Engineering Director & Site Lead der Google Germany GmbH und im Vorstand von Deutschland sicher im Netz e.V.

Unsichere Schule 2.0? Digitale Sicherheit als Bildungsherausforderung

von Martin Drechsler und Björn Schreiber

Die Nutzung neuer digitaler Medien nimmt unaufhaltsam Einfluss auf alle Bereiche des menschlichen Zusammenlebens: Der Begriff der digitalisierten Netzwerkgesellschaft beschreibt eindrücklich die damit verbundenen Veränderungen von Kultur, Wirtschaft, Institutionen und des zivilgesellschaftlichen Lebens. Neue Technologien wie das Internet der Dinge, Künstliche Intelligenz oder Augmented Reality zeigen dabei völlig neue Möglichkeiten auf, die Prozesse der Enthierarchisierung, Globalisierung und Hybridisierung von Räumen weiter vorantreiben werden. Das eröffnet uns viele Chancen, ist aber auch mit Unsicherheiten und Herausforderungen verbunden.

Der Begriff der Sicherheit beschreibt in diesem Zusammenhang nicht nur die Nutzung technischer Maßnahmen zum Schutz vor Cyberangriffen oder die Sensibilisierung für die Preisgabe persönlicher Daten, sondern wird ergänzt durch ein individuelles Gefühl, das vor allem auf persönlichen Dispositionen und Einstellungen sowie den eigenen Nutzungspräferenzen und -fähigkeiten beruht (siehe hierzu DsiN-Sicherheitsindex 2016). Umso wichtiger ist eine ganzheitliche Thematisierung von Sicherheit im digitalen Raum, die bereits mit der ersten Nutzung von Angeboten beginnen sollte.

IT-SICHERHEIT FÄNGT IN DER SCHULE AN

Der Lernraum Schule nimmt bezüglich Sicherheitsaspekten und Herausforderungen digitaler Medien eine zentrale Rolle ein. Gerade weil digitale Medien eine fundamentale Bedeutung in der Sozialisation von Kindern und Jugendlichen haben und zudem alle gesellschaftlichen Bereiche durchdringen, muss sie die Schule sowohl auf einer inhaltlichen als auch auf einer methodisch-didaktischen Ebene einbinden und diskutieren. Dies erfordert jedoch eine ganzheitliche Betrachtung von kindlichen und jugendlichen Nutzungspräferenzen. Es ist daher wenig hilfreich, stets nur mit einem erhobenen Zeigefinger und dem Aufmalen digitaler Schreckensszenarien Schüler*innen sensibilisieren zu wollen.

Ganz im Gegenteil: Zunehmend fühlen sich Jugendliche in der Schule bezüglich digitaler Medien nur wenig ernst genommen und erwarten neben einer Fokussierung auf Sicherheitsaspekte ebenso Anreize und Begleitung bei einer produktiven und partizipationsorientierten Mediennutzung (siehe hierzu SINUS-Jugendstudie 2016). Gleichzeitig zeigen gerade aktuelle Thematiken wie z. B. Hate Speech, Vorratsdatenspeicherung oder Algorithmen völlig neue Diskussionslinien und Dispute auf, die die Autorität und den Wissensvorsprung der Erwachsenenwelt in Fragen eines sicheren und kompetenten Umgangs mit digitalen Medien erschüttern. Jugendliche nehmen digitales Fehlverhalten und Konflikte sehr wohl wahr und suchen nach persönlichen Formen des Umgangs, aber auch der Abgrenzung.

KRITISCHE UND PRAXISNAHE MEDIENBILDUNG IST UNVERZICHTBAR

Es zeigt sich also, dass die Sensibilisierung für das sichere Handeln im digitalen Raum aus einem Zusammenspiel von handlungsorientierter Medienbildung – die Reflexion, Kritik, technische Kompetenzen und gestalterische Fähigkeiten umfasst –, einem vertiefenden technischen Wissen und einem Diskussionsprozess um gesellschaftliche Werte und Normen bestehen muss. Dabei geht es, insbesondere vor dem Hintergrund eines intelligenten Risikomanagements, darum, Jugendlichen Befähigungs- und Bewältigungsstrategien zu vermitteln, damit sie auch für zukünftige, heute noch nicht einmal absehbare Herausforderungen gewappnet sind.

Dass dies hohe Anforderungen an den Lernraum Schule stellt, scheint klar. Auch deshalb ist neben einer Implementierung in Schulprogrammen, Rahmenlehrplänen, Aus-, Fort- und Weiterbildungen, geeigneten Materialien und technischen Voraussetzungen die Öffnung des Lernraums Schule für außerschulische Bildungsinstitutionen, NGOs und Initiativen sinnvoll. Sie können ein Innovationsmotor sein und Fachwissen sowie sozial- und medienpädagogische Vermittlungsansätze mitbringen und Schulen intensiv beraten. Das Projekt „Medien in die Schule“ (www.medien-in-die-schule.de) der Partner FSM, FSF, Google Deutschland und der Unterstützer DsiN, Telefonica Deutschland, Auerbachstiftung, Amadeu Antonio Stiftung und der Technologiestiftung Berlin zeigt zahlreiche Ansätze auf, wie Sicherheit im digitalen Raum sinnvoll und vor allem ohne Bevormundung prozess- und produktionsorientiert vermittelt werden kann.

www.10jahre.dsin.de

Im Bürgerforum 1 des DsiN-Jahreskongresses sprechen der Präsident des Berufsschullehrerverbandes BLBS, OStD Eugen Straubinger, und MdB Saskia Esken gemeinsam mit Martin Drechsler und weiteren Experten über Verbraucherbildung durch Digitale Aufklärung 2.0.

Martin Drechsler
ist Geschäftsführer der Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM) und im Vorstand von Deutschland sicher im Netz e.V.

Björn Schreiber
ist Referent für Medienbildung der FSM

Wie ich zur SiBa-App kam – und dort geblieben bin

DsiN-Geschäftsführer Dr. Michael Littger befragt die SiBa-Nutzer Axel Vedder und Georg Klysch über ihre Erfahrungen mit der App

Seit November 2015 informiert die App des DsiN-Sicherheitsbarometers (kurz SiBa-App) über aktuelle Risiken und Bedrohungen im digitalen Alltag. Der Geschäftsführer von DsiN, Dr. Michael Littger, unterhält sich mit zwei von 35.000 aktiven Nutzern über ihre Erfahrungen mit der App: Axel Vedder und Georg Klysch

Dr. Michael Littger: **Wie sind Sie zum Sicherheitsbarometer von DsiN gekommen?**

Axel Vedder: Ich kann mich leider nicht mehr erinnern.

Georg Klysch: Die App war entweder in der *c't* oder auf golem.de erwähnt worden. Oder vielleicht auf bsi-fuer-buerger.de?

Jetzt mal ganz spontan: Gibt es eine SiBa-Nachricht, an die Sie sich konkret erinnern?

Georg Klysch: Nicht an eine bestimmte. Aber ganz klar an die drei Gruppen Virenwarnungen, Warnungen vor Trojanern, die Festplatten verschlüsseln, und Meldungen über gehackte Adressdatenbanken.

Axel Vedder: Mir ist die Nachricht in Erinnerung geblieben, dass „PayPal" für Angriffe verwendet wurde.

Haben Ihnen die SiBa-Nachrichten schon mal wirklich weitergeholfen?

Georg Klysch: Nicht im praktischen Fall, da ich meine Systeme überdurchschnittlich gut absichere – aber sicherlich im Zusammenhang mit neuen Trends und der Sensibilisierung für digitale Gefahren. Als Informationsmedium, auch für mein berufliches Umfeld, finde ich die SiBa-App einfach gelungen. Für betroffene User dürften die weiterführenden Links in den Nachrichten von großer Hilfe sein.

Stärkung des Sicherheitgefühls oder Verunsicherung – wie wirken die vielen Meldungen auf Sie?

Georg Klysch: Eingestellt habe ich die Push-Nachrichten auf die beiden höchsten Risiken sowie sämtliche Lebensbereiche. Die Meldungen sind sehr moderat formuliert. Die App beschreitet meiner Meinung nach einen guten Mittelweg: Die Anzahl der Meldungen nervt nicht und die Neugier bleibt bestehen. Auch wird man regelmäßig daran erinnert, die eigene Datensicherheit zu bedenken.

Axel Vedder: Ich empfinde mehr Sicherheit – und Ihre Hinweise lassen sich ja wunderbar filtern. Wenn es zuviel wird, kann man die App auch mal vernachlässigen.

Wer ist denn aus Ihrer Sicht verantwortlich für IT-Sicherheit: Unternehmen, Anwender, Politik oder Behörden?

Georg Klysch: Alle vier! Wollen Sie Beispiele? Anwender posten per Smartphone auf Facebook und teilen somit diesem Anbieter gleich ihre Handynummer mit. Hier müssen Verbraucher aufpassen. Und in Firmen werden E-Mails mit Betriebsgeheimnissen unverschlüsselt verschickt. Das geht nicht! Grundsätzlich gilt aber auch: Digitale Kommunikation ist inzwischen so selbstverständlich, dass die Risiken eines Abgreifens von (Meta-)Daten schon aus dem Bewusstsein verschwinden. Hier müssen alle aufpassen. Es kann auch nicht sein, dass das Handy der Bundeskanzlerin abgehört wird.

Axel Vedder: Ja, auch ich meine, dass IT-Sicherheit eine Aufgabe für alle ist, die am Internet partizipieren.

Schön, dass Sie die SiBa-App nutzen; welche weiteren Angebote für Sicherheit im Netz können Sie empfehlen?

Georg Klysch: Zusatzprogramme für IT-Sicherheit bei Browsern (Add-Ons) wie NoScript für den Firefox. Auch Projekte wie TrutzBox und spezielle Webseiten wie die des Sicherheitsportals des BSI helfen weiter.

Axel Vedder: Und jeder Nutzer sollte über eine aktuelle Firewall verfügen.

Sie haben einen Wunsch frei für digitale Sicherheit: Welchen wählen Sie?

Georg Klysch: Eine Aufklärungsarbeit, die der gutgläubigen Haltung „Meine Daten interessieren doch eh niemanden" entgegenwirkt. Auch einen verantwortungsbewussteren Umgang mit den Daten von anderen. Sollten Informationen und Schulungen nichts nutzen, wäre es Aufgabe des Staates, mittels Standards für Datensicherheit zu sorgen. Diese müssen sich selbstverständlich am Wohl des Bürgers orientieren.

SIBA-APP – SICHERHEITSBAROMETER

Die SiBa-App informiert Nutzer über aktuelle, sicherheitsrelevante Vorfälle im digitalen Alltag. Links verweisen auf konkrete Schutzmaßnahmen sowie auf Tipps, was bei einem Angriff zu tun ist. Themengebiete für Sicherheitsnachrichten sind einstellbar sowie auch die Möglichkeit, aktuelle Meldungen als Pushmeldungen zu beziehen. Jede News kann mit Freunden geteilt werden. Die Gefahrenstufe der Meldungen wird über ein Ampelsystem angezeigt. Das Angebot wird mit dem Bundesministerium für Sicherheit in der Informationstechnik, dem Bundeskriminalamt sowie Branchenverbänden und DsiN-Mitgliedern täglich aktualisiert und ist in allen App-Stores verfügbar.

www.dsin.de/siba

Chefsache: IT-Sicherheit@Mittelstand

von Dr. Martin Wansleben

Die Digitalisierung hat längst in Werkhallen, Fahrzeuge, Läden und Büros Einzug gehalten. Das ist positiv, denn die umfassende Digitalisierung und Vernetzung der betrieblichen Prozesse und der Kundenschnittstelle wird ein wesentlicher Faktor für die künftige Wettbewerbsfähigkeit unserer Unternehmen sein. Das ist auch den allermeisten Geschäftsführern bewusst – wie unsere aktuelle Umfrage zur Digitalisierung bestätigt. Genauso klar ist der Mehrheit: Hier wird es zu Verschiebungen in der Wertschöpfungskette kommen. Viele Unternehmen setzen sich deshalb mit dem Trend der Plattformisierung auseinander. Zahlreiche arbeiten daran, ihren Kunden passgenaue „Smart Services" anzubieten. Insbesondere der industrielle Mittelstand steht vor der Herausforderung, die dabei neu auftretenden Sicherheitsfragen offen anzugehen.

HILFE ZUR SELBSTHILFE IM MITTELSTAND

Die Veranstaltungsreihe IT-Sicherheit@Mittelstand von DsiN und DIHK bietet Entscheidern bundesweit praxisnahe Kurse für digitalen Schutz im Unternehmen. Grundlage sind kostenlose Schulungsmaterialien, die von DsiN entwickelt und in den IHKs vor Ort präsentiert werden: in bis zu acht Workshops jeden Monat. Dabei wird den Teilnehmern eine „Hilfe zur Selbsthilfe" ermöglicht. Der Bundesminister für Wirtschaft und Energie ist Schirmherr.

www.dsin.de/it-sicherheit-mittelstand

INVESTITIONEN IN SICHERHEIT ZAHLEN SICH AUS

Hier gibt es bereits eine hohe Sensibilität: Aus unseren Umfragen und der intensiven Diskussion mit den Unternehmen vor Ort wissen wir, dass bei den Geschäftsführern von großen wie kleinen Unternehmen Fragen der Daten- und Informationssicherheit hohe Priorität haben. Denn diese werden als eine der wichtigsten Hürden auf dem Weg zur Digitalisierung wahrgenommen. Bei der praktischen Umsetzung müssen mitunter noch Schwierigkeiten überwunden werden. Im Zentrum stehen die Fragen nach den wichtigsten Assets des Unternehmens und wie man sie nachhaltig schützen kann – und diese sind vielfach noch nicht abschließend beantwortet.

SICHERHEIT ALS WETTBEWERBS- UND STANDORTVORTEIL

Die Digitalisierung im Betrieb gelingt insbesondere dann, wenn das Thema IT-Sicherheit von Anfang an mitgedacht und sukzessive umgesetzt wird. Hier und da kostet das mehr Zeit und Ressourcen. Die Erfahrung der Unternehmen zeigt aber auch, dass es sich lohnt. Große Gefahren gehen hier insbesondere von veralteten Systemen oder Schadsoftware aus, die über E-Mail und Surfen ins Unternehmen gelangen. Solche Risiken sind häufig schon mit überschaubaren Mitteln zu bewältigen, etwa indem automatische Updates aktiviert und Firewalls installiert werden. Oft hilft auch bereits der gesunde Menschenverstand weiter: vorausgesetzt, die Mitarbeiter sind entsprechend sensibilisiert.

Im Rahmen von Industrie 4.0 wird es zu einer durchgehenden internen und externen Vernetzung kommen. Daten, die im industriellen Fertigungsprozess anfallen, werden systematisch erfasst und verarbeitet. Freilich bedarf es dafür einer anderen Sicherheitsarchitektur. Wichtig ist zu klären, wer nicht an die Daten herankommen darf und wie das gewährleistet wird.

Die Entwicklung und Etablierung von sicheren Industrie-4.0-Lösungen „made in Germany" ist ein Kernthema, an dem wir gemeinsam mit anderen Akteuren aus Wirtschaft, Wissenschaft und Politik arbeiten. Solche Lösungen bieten auch einen erheblichen Wettbewerbsvorteil für deutsche Ausrüster auf den internationalen Märkten.

HILFE BEI DER DIGITALEN TRANSFORMATION DES UNTERNEHMENS

Die IHK-Organisation bietet Unternehmen Unterstützung auf dem Weg zu einer sicheren Digitalisierung ihrer Geschäftsprozesse an. Denn wir wissen – auch aus eigener Erfahrung –, dass die Geschäftsführung eines jeden Unternehmens gut beraten ist, Daten- und Informationssicherheit als strategisches Thema mitzudenken. So wird digitaler Schutz ein wichtiges internes Thema, mit dem man auch beim Kunden punkten kann. In Kooperation mit Deutschland sicher im Netz e.V. und weiteren Partnern bieten wir die Veranstaltungsreihe IT-Sicherheit@Mittelstand an. Hier vermitteln wir praktische Tipps für die ersten Schritte hin zu mehr Daten- und Informationssicherheit.

Unser Ziel ist es, mit den Veranstaltungen und darauf aufbauenden Aktivitäten in den Regionen einen wertvollen Beitrag zu leisten, um unsere Unternehmen noch besser auf die Herausforderungen einer digitalisierten Welt vorzubereiten.

Dr. Martin Wansleben
ist Hauptgeschäftsführer des Deutschen Industrie- und Handelskammertages e.V. (DIHK)

Mitarbeiter zu Botschaftern für IT-Sicherheit machen

von Dr. Peter Krug und Stefan Brandl

Viren, Trojaner, Ransomware – es gehen viele Schreckgespenster um in der modernen, digital vernetzten Welt. Doch können Angriffe von Außen im Prinzip nur dann fruchten, wenn es auch intern ein Problem gibt. Das kann etwa ein Leck in der technischen Sicherheitsinfrastruktur sein. Viel häufiger allerdings sitzt das Problem leider vor den Bildschirmen. Alle relevanten Untersuchungen belegen auch, dass die eigenen Mitarbeiter die häufigste Gefahrenquelle sind, wenn es um Sicherheitsprobleme geht. Dabei steckt oftmals nicht einmal kriminelle Energie oder die Absicht dahinter, dem Unternehmen Schaden zuzufügen. Vielmehr ist es die Sorglosigkeit im Umgang mit den technischen Hilfsmitteln, die Angriffsfläche bietet.

Die größten Gefahren lauern stets an den Stellen, wo sich Routine einschleicht und man nicht mehr so genau hinsieht. Damit kommt dem Sicherheitsbewusstsein der Mitarbeiter eine enorm wichtige Bedeutung zu. Und dass es darum besser bestellt sein könnte, zeigt nicht zuletzt der DsiN-Sicherheitsmonitor. Rund ein Drittel der Unternehmen sehen laut den Auswertungen von 2016 immer noch nicht die Notwendigkeit, organisatorische Rahmenbedingungen wie Richtlinien, Sicherheitskonzepte, geregelte Verantwortlichkeiten und ähnliches für mehr IT-Sicherheit umzusetzen. Noch weniger, nämlich nur gut ein Viertel, bieten ihren Mitarbeitern regelmäßige Informationen und Schulungen zum sicherheitsbewussten Verhalten an.

> Angriffe von Außen fruchten nur dann, wenn es auch intern ein Problem gibt. Und die eigenen Mitarbeiter sind die häufigste Gefahrenquelle.

UNTERNEHMEN ALS INKUBATOREN FÜR SICHERHEITSBEWUSSTSEIN

Was lässt sich dagegen tun? Die Antwort lautet: Aufklärung, Aufklärung, Aufklärung. Neben großen, öffentlichkeitswirksamen Kampagnen sind es gerade die kleinen Dinge, die im Prinzip jedes Unternehmen leisten kann und die hier Erfolg versprechen. Aufmerksamkeit zu erregen ist schon einmal ein Anfang. Aber damit die Sensibilisierung nachhaltig wirkt, darf sich das Thema Sicherheit nicht in einmaligen Belehrungen erschöpfen. Es muss im täglichen Tun ankommen. Die Unternehmen müssen ihre Mitarbeiter dazu bewegen, ihr Verhalten zu ändern.

Ein gutes Beispiel für ein solches gelebtes Sicherheitsbewusstsein ist die DATEV eG. Als Unternehmen mit besonderen Sicherheitsanforderungen sind IT-Sicherheit und Datenschutz sozusagen seit Gründung des Unternehmens vor 50 Jahren Bestandteil der DATEV-DNA. Das schlägt sich in einem umfassenden Datenschutz- und Datensicherheitskonzept nieder. Dabei handelt es sich um einen Mix aus baulichen, organisatorischen und natürlich technischen Vorkehrungen. Aber extrem wichtig ist eben auch der personelle Aspekt.

Schon beim Eintritt in das Unternehmen werden die neuen Mitarbeiter im Rahmen von Einführungstagen, die ihnen das Unternehmen näherbringen, auch besonders für die Gefahren beim Umgang mit Informationen und beim Einsatz von IT-Systemen sensibilisiert. Zusätzlich werden Angestellte bei jedem Gang durch das Unternehmen beispielsweise durch Plakate mit verschiedenen Sicherheitsaspekten konfrontiert, sodass die Thematik permanent präsent ist. Regelmäßige Schulungen und virtuelle Trainings frischen immer wieder die sicherheitsspezifischen Kenntnisse auf und halten das Thema im Bewusstsein.

SCHUTZ DURCH VERMEIDEN VON ANWENDERFEHLERN

Inhaltlich gibt es zwei Hauptebenen, die den Mitarbeitern in Fleisch und Blut übergehen müssen. Zum einen geht es darum, die technischen Systeme sauber zu halten. Dazu gehören grundlegende Verhaltensregeln – etwa

DSIN-SICHERHEITSMONITOR MITTELSTAND

Der „DsiN-Sicherheitsmonitor Mittelstand“ erhebt seit 2011 die Sicherheitslage bei mittelständischen Unternehmen anhand einer Onlinebefragung. Seit Start haben sich über 7.000 Unternehmen an der Umfrage beteiligt. Die Studie zeigt die Entwicklung der Sensibilisierung und Schutzmaßnahmen in unterschiedlichen Unternehmensfeldern. Auffällig ist eine steigende Digitalisierung bei eher stagnierenden Schutzmaßnahmen. Die aktuelle Erhebung 2016 wurde am 18. Oktober 2016 auf einer Sitzung der Cybersicherheitsallianz zur it-sa Sicherheitsmesse in Nürnberg vorgestellt.

www.dsin.de/downloads/dsin-sicherheitsmonitor-mittelstand

dass ein unbekannter Dateianhang beziehungsweise Internet-Link in einer E-Mail nicht einfach angeklickt werden sollte oder dass ein gefundener USB-Stick keinesfalls mit dem Firmennetz verbunden werden darf. Und dass man auch E-Mails aus vermeintlich bekannten Quellen eine gesunde Portion Misstrauen entgegenbringen sollte.

Um ihre Mitarbeiter für diese Gefahren zu sensibilisieren, können Unternehmen unter anderem auf den Leitfaden „Verhaltensregeln zur Informationssicherheit“ zurückgreifen, den Deutschland sicher im Netz gemeinsam mit DATEV veröffentlicht hat. Die zentralen Aspekte der IT-Sicherheit werden darin aus der Sicht von Mitarbeitern thematisiert. Sie betreffen Fragen zur E-Mail-Sicherheit, die Vermeidung von Passwort- und Datendiebstahl sowie Methoden des Social Engineering.

Damit die Sensibilisierung nachhaltig wirkt, darf sich das Thema Sicherheit nicht in einmaligen Belehrungen erschöpfen.

MITARBEITER GEGEN SOCIAL ENGINEERING WAPPNEN

Mit Social Engineering haben wir auch bereits die zweite elementare Angriffsebene erreicht, die nicht auf die Technik, sondern auf den Mitarbeiter als soziales Wesen zielt. Unter Social Engineering werden in der IT-Sicherheit Angriffsmethoden zusammengefasst, bei denen Kriminelle versuchen, durch Manipulation von Personen an sensible Informationen von Unternehmen oder Privatpersonen zu gelangen. Ein Beispiel für eine solche Vorgehensweise ist der sogenannte Enkel-Trick, mit dem junge Betrüger ältere Menschen zur Überweisung von Geldsummen bewegen, indem sie sich als ihre Enkel ausgeben, die in einer finanziellen Notlage stecken. Um hier Aufmerksamkeit zu schaffen, haben DATEV und DsiN einen weiteren Leitfaden entwickelt: „Verhaltensregeln zum Thema Social Engineering“.

Am Beispiel einiger besonders gefährdeter Lebens- und Arbeitsbereiche macht die Broschüre Unternehmer und ihre Mitarbeiter auf konkrete Risiken durch Social-Engineering-Attacken im Arbeitsalltag aufmerksam und gibt einen kompakten und allgemeinverständlichen Überblick. Klare Verhaltensregeln am Ende jedes Kapitels sowie Hinweise zu weiterführenden Informationen unterstützen bei der Umsetzung des Gelernten. Zusätzlich enthält der Leitfaden einen Testfragebogen, mit dem die Mitarbeiter selbst überprüfen können, wie anfällig sie noch für Social Engineering sind. Darüber hinaus soll ein Erinnerungs-Kalender mit integrierter Karte dabei helfen, im beruflichen Alltag stets achtsam zu bleiben.

ALLES EINE FRAGE DER UNTERNEHMENSKULTUR

Die Gefahren sind also prinzipiell bekannt. Informationen und Rüstzeug gibt es ebenfalls genug. Wenn viele Unternehmer und Geschäftsführer der IT-Sicherheit einen hohen Stellenwert zuerkennen würden und diesen damit auch ihren Mitarbeitern nahebrächten, würden die Angestellten ganz automatisch zu einem gigantischen Netzwerk an Sicherheitsbotschaftern, die auch in ihrem privaten Umfeld Positives bewirken. Ob dies gelingt, ist eine Frage der Unternehmenskultur. Aus der Praxis bei DATEV lässt sich erkennen, dass dieses Modell funktioniert. Bleibt zu hoffen, dass sich viele Unternehmen dazu bewegen lassen, es in die Tat umzusetzen.

DSIN-LEITFÄDEN FÜR MITARBEITER

Aufklärungsmaßnahmen zur Informationssicherheit werden gerade in kleineren Betrieben vernachlässigt. Dies ist auch ein Ergebnis des DsiN-Sicherheitsmonitors. Zu den größten Schwachstellen gehören unzureichende Kenntnisse der Mitarbeiter. Die Leitfäden von DsiN und DATEV geben Praxisbeispiele zu konkreten Risiken und Gefahren. Sie vermitteln einen verständlichen Überblick zum Thema Informationssicherheit und helfen, Eigenverantwortung in diesem Bereich zu fördern. Die Reihe umfasst zahlreiche Ausgaben mit den Schwerpunkten E-Mail-Sicherheit, Social Engineering und Verschlüsselung.

www.dsin.de/downloads/verhaltensregeln-zum-social-engineering

Dr. Peter Krug
ist Vorstandsmitglied der DATEV eG und im Beirat von Deutschland sicher im Netz e.V.

Stefan Brandl
ist Referent für Sicherheitsthemen bei der DATEV eG

Standortfaktor IT-Sicherheit

von Ulrich Hamann

Arbeit, Kapital, Boden: Diese drei Produktionsfaktoren brauchte ein Land laut klassischer Volkswirtschaftslehre für die Erzeugung von Waren und Dienstleistungen. Je mehr, umso besser und umso höher das Bruttoinlandsprodukt. Die digitale Transformation der Wirtschaft sorgt jedoch für einen Paradigmenwechsel in der Nationalökonomie. In der vernetzten, digitalen Welt verliert der Boden an Bedeutung – vom Standort für Server-Farmen vielleicht abgesehen. Statt dessen wird die Generierung und Nutzung von Daten immer wichtiger. Kurz gesagt: Big Data statt Big Buildings.

Wenn jedoch der Umgang mit Daten zusehends die Dynamik einer Volkswirtschaft beeinflusst, dann gewinnen auch die Daten- und die IT-Sicherheit immer mehr an wirtschaftlicher Bedeutung. Wenn Unternehmen die Chancen des digitalen Wandels nutzen wollen, brauchen sie nachhaltigen Schutz für ihre Werte: für alle Infrastrukturen, Kommunikationswege und Daten. Nur wenn die Anwender darauf vertrauen können, dass ihre Daten weitestgehend geschützt sind, werden sie die Möglichkeiten digitaler Angebote ausschöpfen.

Entsprechend wirken sich IT-Sicherheitsbedenken bereits auf das gesamtwirtschaftliche Wachstum in Deutschland aus. Das zeigt eine aktuelle repräsentative Umfrage im Auftrag der Bundesdruckerei. Befragt wurden rund 550 IT-Sicherheitsverantwortliche deutscher Unternehmen. Zwei Drittel rechnen mit steigenden IT-Sicherheitsrisiken durch die Digitalisierung. Das hat Folgen: Jedem fünften Unternehmen geht nach eigener Einschätzung aktuell Umsatz verloren, da es die Digitalisierung aus Angst vor IT-Sicherheitsvorfällen nicht schnell genug vorantreibt; für ein zusätzliches Drittel ist diese Aussage immerhin teilweise zutreffend. Mit anderen Worten: Aus Angst vor Cyberattacken und Datenverlust transformiert jedes zweite Unternehmen seine Prozesse, Produkte und Services behutsamer als möglich und schlägt daher einen langsameren Wachstumspfad ein.

> In der vernetzten, digitalen Welt verliert Boden an Bedeutung – vom Standort für Server-Farmen vielleicht abgesehen.

Egal, ob diese Bedenken im Einzelfall berechtigt, übertrieben oder vorgeschoben sind: Sie verzögern die notwendige Digitalisierung der deutschen Wirtschaft und haben entsprechende volkswirtschaftliche Folgen für die Wirtschaftsleistung von heute und morgen. Besonders betroffen ist laut Umfrage das Rückgrat der deutschen Wirtschaft, der Maschinen- und Anlagenbau, sowie die ITK- und Elektronikbranche.

Der Trend zur vernetzten Industrie 4.0 stellt also gerade viele innovative Unternehmen vor die vermeintliche Entscheidung: entweder schnelle Digitalisierung und Vernetzung samt höheren Sicherheitsrisiken oder langsame digitale Transformation samt Umsatzverzicht. Dieses Digitalisierungsdilemma gilt auch für die anderen Teile der Volkswirtschaft: Bürger und Behörden. Hier führt der kluge IT-Einsatz zu mehr Effizienz und Bequemlichkeit sowie weniger Kosten und Zeitaufwand.

IT-Sicherheit wird also zum Standortfaktor der digitalen Welt. Wollen wir unseren internationalen Spitzenplatz verteidigen, so müssen Anbieter und Anwender von Hardware, Software und digitalen Dienstleistungen sowie die öffentliche Hand ihrer jeweiligen Verantwortung gerecht werden. Zusammenarbeit tut Not. Und für eine derartige Zusammenarbeit sind Initiativen wie „Deutschland sicher im Netz“ ein schönes Beispiel. Der Fokus, vor allem Privatnutzer sowie kleinere und mittlere Unternehmen (KMU) fit zu machen für den sicheren Umgang mit dem Internet, ist richtig und wichtig: Laut unserer Umfrage fühlen sich derzeit nur acht Prozent der KMU voll und ganz gerüstet für die digitale Transformation!

www.10jahre.dsin.de

Hier finden Sie – grafisch aufbereitet – die Zahlen zu den Umsatzverlusten bei Unternehmen durch Cyberrisiken sowie ein Interview mit Herrn Hamann zum Standortfaktor IT-Sicherheit.

Ulrich Hamann
ist Vorsitzender der Geschäftsführung der Bundesdruckerei

IT-SICHERHEITSMONITOR-CHECK

Seit 2011 betreibt DsiN einen kostenfreien Online-Sicherheitscheck. Die Abfrage zu sicherheitsrelevanten Themen sensibilisiert Mitarbeiter im Unternehmen und gibt wertvolle Tipps für die Sicherheit im Betrieb. Die Erhebung ist Grundlage des DsiN-Sicherheitsmonitors.

www.it-sicherheit-in-der-wirtschaft.de

Die Sensibilisierung, Befähigung und Motivation von Menschen für IT-Sicherheit ist eine Herkulesaufgabe – und von niemandem allein zu schaffen. Es ist gut, dass sich viele unterschiedliche Initiativen diesem Thema angenommen haben. Damit einzelne Aktionen nicht verpuffen, hilft eine gegenseitige Vernetzung. Sie kann über Plattformen wie Deutschland sicher im Netz erfolgen, wo starke Akteure zusammenwirken für ein koordiniertes Vorgehen.

Gemeinsam stark für IT-Sicherheit – Initiativen bündeln und vernetzen

Jetzt Stärken bündeln für ein sicheres digitales Leben

von Hartmut Thomsen

Wir skypen mit Geschäftspartnern in Singapur und verschicken Konstruktionszeichnungen als Mail-Anhang nach Brasilien. In unserer Freizeit chatten wir über WhatsApp und laden Fotos auf Instagram hoch. Kein Zweifel: Das Internet ist fester Bestandteil unseres Alltags, ja unseres gesamten Lebens geworden.

Doch die vernetzte Welt hat auch ihre Schattenseiten. Ein Klick auf einen gefährlichen E-Mail-Anhang, ein Besuch auf der falschen Website, ein veraltetes Virenschutzprogramm: Schnell wird deutlich, dass viele Gefahren im Netz lauern. Stets muss damit gerechnet werden, dass Kriminelle die vielfältigen Möglichkeiten nutzen, um sich zu bereichern oder Schaden anzurichten. Ob Bots in Firmennetzwerken wertvolles Wissen ausspionieren oder Nutzer durch Ransomware erpresst werden: Sicherheit ist und bleibt ein hochaktuelles Thema – für Privatpersonen ebenso wie für Unternehmen, die sich um die Integrität ihrer Daten sorgen.

Das gilt umso mehr, je umfassender und komplexer die Vernetzung wird. Heute sind nicht mehr nur Computer miteinander verbunden, sondern zunehmend auch Maschinen, Häuser, Lifestyle-Accessoires und Gebrauchsgegenstände aller Art. Mit der Virtual-Reality-Technologie ist schließlich auch unsere Sicht auf das „echte“ Leben unmittelbar betroffen. Damit sind Energieversorger, Anbieter im Gesundheits- und Verkehrswesen oder Behörden längst nicht mehr die einzigen Akteure, bei denen Vorfälle systemrelevant werden können.

> Gemeinsam ist man stärker. Das ist auch der Kerngedanke von Deutschland sicher im Netz.

Genau wie im öffentlichen Raum möchten wir uns natürlich auch im Netz sicher und ohne Sorge bewegen können. Hier gilt, was in anderer Hinsicht längst zum Allgemeinwissen gehört: Gemeinsam ist man stärker. Das ist auch der Kerngedanke von Deutschland sicher im Netz. Die Initiative hat sich zur Aufgabe gemacht, umfassend über die Gefahren im Internet aufzuklären. Mehr noch: Wir wollen dafür sorgen, dass sowohl Unternehmen als auch jeder einzelne Bürger bestmöglich auf die digitale Zukunft vorbereitet sind – und zwar auf die damit verbundenen Chancen und Risiken gleichermaßen. Dabei geht es nicht um einen Rundum-Schutz als Garantie für maximale Sorglosigkeit. Wir möchten dazu beitragen, dass sämtliche Nutzer in der Lage sind, verantwortungsvoll mit den Risiken der Digitalisierung umzugehen. Und vor allem möchten wir ihnen die dazu notwendigen Instrumente an die Hand geben.

VIELFÄLTIGE PROJEKTE UND INITIATIVEN

Das ist eine anspruchsvolle und fordernde Aufgabe, die nur von einem Netzwerk engagierter Menschen und Organisationen bewältigt werden kann. Glücklicherweise gibt es überall in Deutschland Projekte, Initiativen und Unternehmen, die sich den Herausforderungen der Digitalisierung stellen. Die Motive mögen unterschiedlicher Natur sein. Einige tun es, weil es sie in ihrem Kern betrifft. Andere, weil sie gesellschaftliche Verantwortung übernehmen wollen. Ganz gleich jedoch, warum und wie: Wichtig ist, dass es sie gibt.

Viele Instrumente machen aber noch kein Orchester. Denn wenn jeder nur seine eigenen Projekte umsetzt, werden die einzelnen Stimmen verhallen – oder schlimmer noch: Sie werden Teil einer großen Kakophonie, die niemand hören möchte. Ein konzertiertes Vorgehen hat dagegen viele Vorteile. Alle Beteiligten können von gemeinsamen Erfahrungen profitieren und ihre Expertise und Stärken einbringen. Auf diese Weise sprechen alle mit einer Stimme. Das nutzt dem großen Ganzen ebenso wie dem Einzelnen.

Nun heißt dies nicht, dass wir als DsiN immer und überall mitreden müssen. Vielmehr schaffen wir eine Plattform zum Austausch über Herausforderungen und Lösungsansätze, zum Knüpfen und zum Ausbau von Kontakten sowie zur Koordination gemeinsamer Aktivitäten. Wir schaffen eine Plattform, die gleichermaßen Drehkreuz für Informationen, Knotenpunkt der Kommunikation und Wissensressource ist.

AKTIONSBUND DIGITALE SICHERHEIT

In Deutschland gibt es zahlreiche gute Initiativen zum sicheren Umgang mit dem Netz. Um Verbrauchern den Zugang zu erleichtern, müssen sie besser miteinander vernetzt werden. Dies hat sich der Aktionsbund Digitale Sicherheit zur Aufgabe gemacht: Er bringt Initiativen und Veranstaltungen von gemeinnützigen Organisationen zusammen. Ein Aktionsfinder führt Internetnutzer zu den Aufklärungsangeboten, die ihren Bedürfnissen, Wissensniveaus und ihrer lokalen Umgebung entsprechen. Seit dem Start haben sich über 40 Initiativen aus den Bereichen Prävention und Aufklärung, Wissenschaft und Bildung sowie gemeinnützige Verbände in der Plattform zusammengeschlossen.

www.aktionsbund.org

DIGITALE AUFKLÄRUNG IN DER PRAXIS

Gerade bei innovativen Diensten kann effiziente Aufklärung nur im Verbund erfolgen. Ein anschauliches Beispiel hierfür findet sich im Bereich Gesundheit. Die ersten Krankenkassen führen Tarife ein, die sich nach dem Verhalten der Kunden bemessen. Viele der für eine solche Einschätzung notwendigen Daten werden über Fitnessarmbänder übermittelt. Das wirft natürlich Fragen im Hinblick auf den Datenschutz auf. Wichtige Aspekte wie die Anonymisierung von Patientendaten oder die Speicherung von Daten in der Cloud müssen erörtert werden. Auch hier sind wir gemeinsam stärker, denn es geht um die Vernetzung der beteiligten Akteure: Krankenkassen treten in den Dialog mit Ärzte- und Patientenverbänden sowie Sicherheitsexperten und Anbietern aus der Wirtschaft. Erst wenn der Diskurs sichtbar und transparent wird, kann ein stimmiges Gesamtbild entstehen, das der Sache dient und Ängste von Nutzern beseitigt.

> In einer Welt, in der das Entwicklungstempo fast schon täglich zunimmt, kann niemand alles wissen.

Ähnlich verhält es sich mit dem „Aktionsbund Digitale Sicherheit“. In diesem Bund haben sich bisher rund 40 Organisationen und Verbände zusammengeschlossen, die Schutz, Sicherheit und Vertrauen für Menschen im Internet durch konkrete Hilfestellungen unterstützen möchten. Der Aktionsbund zeigt exemplarisch, wie ein effektives gemeinsames Wirken funktionieren kann: Die Aufklärungsarbeit passiert vor Ort und wird unter dem weitgespannten Dach von DsiN gebündelt. Auf diese Weise geht kein Wissen verloren und keine Botschaft scheitert an einer zu geringen Reichweite, sondern kann durch kontinuierlichen Austausch systematisch verbreitet werden.

VERTRAUEN IST UNSER KAPITAL

Die Wirkmächtigkeit einer Initiative wie DsiN steht und fällt mit ihrer Glaubwürdigkeit und Integrität. Als Verein, in dem gut zwei Dutzend renommierte Mitglieder ihre Expertise konzentrieren, sind wir ehrenamtlich tätig. Die Schirmherrschaft von Bundesinnenminister Dr. Thomas de Maizière trägt zweifelsohne auch einen erheblichen Teil dazu bei.

In einer Welt, in der das Entwicklungstempo fast schon täglich zunimmt, kann niemand alles wissen. Deshalb steht DsiN in ständigem Austausch mit den unterschiedlichsten Institutionen, wie etwa dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Initiative IT-Sicherheit in der Wirtschaft des Bundesministeriums für Wirtschaft und Energie sowie der Gesellschaft für Informatik e.V. (GI). Auch Forschungseinrichtungen wie das Fraunhofer-Institut für Offene Kommunikationssysteme und Stiftungen wie „Digitale Chancen“ sind unsere Dialogpartner. Damit ein fortlaufender Erfahrungsaustausch gut funktioniert, sind persönliche Treffen unabdingbar – mit den Jahreskongressen und den DsiNsights Breakfasts bieten wir dafür die passenden Gelegenheiten. Und – ohne unbescheiden wirken zu wollen – es gibt auch einige Erfolge zu vermelden. Als Beispiele für gelungene Kooperationen seien hier die Handlungsversprechen „Einfach Verschlüsseln“ (gemeinsam mit dem Kompetenzzentrum Öffentliche IT) und unser DsiN-Sicherheitsbarometer (kurz: SiBa-App, mit Partnern wie dem BSI, dem Bundeskriminalamt, dem Banken- und Versicherungsverband sowie Unternehmen) erwähnt.

Ist dies nur ein Tropfen auf den heißen Stein? Vielleicht. Aber in jedem Fall der Auftakt zu einer nachhaltigen Zusammenarbeit auf den unterschiedlichsten Ebenen. Wie ein Verbund, bei dem die einzelnen Komponenten perfekt ineinandergreifen und damit ein umso stabileres Gesamtkonstrukt bilden, wollen wir weiterhin unser übergeordnetes Ziel verfolgen, ein Ziel, das unser Name bereits formuliert: Deutschland sicher im Netz. Je mehr Unternehmen, Organisationen und Initiativen sich hier einbringen, desto mehr können wir erreichen.

Wir haben gute Argumente: eine umfassende Vernetzung sowie ausgearbeitete und leicht zugängliche Angebote. Und wir registrieren: Immer mehr Menschen und Betriebe hören uns zu. Sie haben verstanden, dass zu einem souveränen Leben in einer digitalisierten Welt gehört, die Risiken zu kennen und sich wirksam vor ihnen zu schützen.

DSIN-JAHRESKONGRESS

Schutz, Sicherheit und Vertrauen in der digitalen Gesellschaft erfordert den kontinuierlichen Austausch zwischen allen Akteuren der Digitalisierung. Zentral dafür sind persönliche Begegnungen – vor Ort mit Bürgern sowie auch zwischen den Experten und Entscheidern. Mit dem DsiN-Jahreskongress ermöglicht der Verein jedes Jahr ein hochrangiges Zusammentreffen von Wirtschaft, Politik und Wissenschaft. Besonderes Augenmerk gilt auch hier der Einbindung von Bürgerinnen und Bürgern. Ihre Bedürfnisse und Fragen sind für die Arbeit von DsiN entscheidend, um Sicherheit und Vertrauen gleichermaßen aufzubauen und zu verstärken.

www.dsin.de

Hartmut Thomsen
ist Geschäftsführer von SAP Deutschland und Stellvertretender Vorstandsvorsitzender von Deutschland sicher im Netz e.V.

Mit Sicherheit Menschen erreichen

von Holger Münch

Online einen Urlaub buchen, Überweisungen tätigen, Nachrichten aus aller Welt lesen: Das Internet hat unser Leben an vielen Stellen bereichert und vereinfacht. Es eröffnet neue Möglichkeiten der Kommunikation und des Wissenszugangs, neue Geschäftsmodelle und gibt neue Impulse für Forschung und Entwicklung. Digitalisierung und Vernetzung sind aber auch in der Kriminalität angekommen.

Terrororganisationen nutzen das Internet für ihre Propaganda, Cyberangriffe auf kritische Infrastrukturen und Cyberspionage sind eine Bedrohung für Staat, Wirtschaft und Gesellschaft. Kinderpornografie, „Phishing“ persönlicher Zugangsdaten zu Bankkonten oder Onlineshops, Handel mit illegalen Waren, Verbreitung von Schadsoftware und Betrugshandlungen finden im und über das Internet statt. Kriminellen eröffnen sich hier neue Chancen und Tatgelegenheiten.

2015 wurden über 45.000 Cybercrime-Fälle von der Polizei erfasst. Doch polizeiliche Statistiken bilden nur einen kleinen Ausschnitt der tatsächlichen Dimension von Cybercrime ab. Das Dunkelfeld ist groß. Taten werden in vielen Fällen nicht bemerkt oder nicht angezeigt.

DIE SIBA-APP – DAS SICHERHEITSBAROMETER

Das BKA ist Partner der SiBa-App, mit der Bürgerinnen und Bürger sowie Mitarbeiterinnen und Mitarbeiter in Unternehmen aktuelle Nachrichten zu neuen sicherheitsrelevanten Vorfällen erhalten. Hilfreich sind nicht nur die präventiven Maßnahmen, die passend zum Vorfall empfohlen werden. Besonders wichtig für Betroffene können die Maßnahmen zur Reaktion bei einem Sicherheitsvorfall sein. Die Vielfalt der Empfehlungen wird durch Verweise auf die unterschiedlichen Partner gewährleistet.

www.dsin.de/siba

VEREINTES VORGEHEN GEGEN INTERNETKRIMINALITÄT

Wesentlich für die erfolgreiche Bekämpfung der Cybercrime ist die Zusammenarbeit zwischen den Sicherheitsbehörden und mit Kooperationspartnern aus verschiedensten Bereichen, um unsere Kommunikation, unsere sozialen Zusammenhänge und unser wirtschaftliches Leben gegen Gefahren zu schützen. Im Verein Deutschland sicher im Netz wird die Kompetenz von Behörden, Politik, Wirtschaft und Wissenschaft zusammengeführt. Ziel ist es, Verbraucher/innen und Unternehmen vor Gefahren im Internet zu warnen und zu kompetenten Internetnutzern zu machen.

Das Internet ist kein strafverfolgungsfreier Raum. Die Polizei kann Cybercrime jedoch nur wirksam bekämpfen, wenn sie von entsprechenden Straftaten erfährt. Daher ist es wichtig, dass Betroffene Anzeige erstatten. Nur so kann die Polizei Spuren und Beweise sichern und Kriminelle überführen. Da es sich häufig um „flüchtige Daten“ handelt, ist zudem schnelles Handeln geboten.

AUCH VERBRAUCHER GEFORDERT

Neben der Suche nach den Tätern ist es wichtig, dass alle Nutzer/innen wachsam und verantwortungsvoll im Internet unterwegs sind. Virenschutzprogramme und Sicherheitsupdates der Softwarehersteller mögen lästig erscheinen, sind aber notwendig. Es ist bequem, Dienstleistungen über das Internet abzuwickeln, aber die Preisgabe persönlicher Daten darf nicht leichtfertig geschehen, denn allzu einfach können diese von Kriminellen abgefangen und missbräuchlich genutzt werden. Auch die zunehmende Vermischung der Nutzung von Endgeräten sowohl für private als auch berufliche Zwecke birgt die Gefahr von Sicherheitslücken.

Es ist die Eigenverantwortung von Unternehmen, Behörden und jedes Einzelnen gefragt, die Risiken, die mit der Nutzung moderner Kommunikationsmittel und der zunehmenden globalen Vernetzung einhergehen, zu kennen und sich entsprechend dagegen zu schützen.

DIGITALE NACHBARSCHAFT FÜR VEREINE

Ehrenamtliches Engagement wird in Deutschland großgeschrieben. Über 30 Millionen Bürgerinnen und Bürger engagieren sich neben dem Beruf für gemeinnützige Anliegen – zunehmend auch digital. Die IT-Schutzkompetenzen sind dabei oftmals nur unzureichend ausgeprägt. Kriminelle können hier daher noch leicht zuschlagen. Für einen sicheren Umgang mit Daten und Informationen bietet die „Digitale Nachbarschaft“ Grundkurse für digitale Sicherheit im Ehrenamt und zur Weitergabe an Bürgerinnen und Bürger.

www.digitale-nachbarschaft.de

Holger Münch
ist Präsident des Bundeskriminalamtes (BKA) und im Beirat von Deutschland sicher im Netz e.V.

Nur nicht den Kopf in den Sand stecken

IT-Sicherheit ist für jeden machbar

Avira-Geschäftsführer Travis Witteveen stellt sich den Fragen des DsiN-Vorstandsvorsitzenden Dr. Thomas Kremer

Travis Witteveen, CEO des Antivirensoftware-Herstellers Avira, will Berührungsängste mit IT-Sicherheitsvorkehrungen abbauen, weil ein Vogel-Strauß-Verhalten hier früher oder später zu Problemen führt. Dem DsiN-Vorsitzenden Dr. Thomas Kremer erklärt er, welche IT-Schutzvorrichtungen er für sinnvoll hält.

Dr. Thomas Kremer: **Was würden Sie sagen: Ist das Internet heute sicherer als früher?**

Travis Witteveen: Das lässt sich schwer beantworten. Egal ob im Unternehmen oder privat: Wir haben es heute mit einer schier unerschöpflichen Zahl von IT-Systemen und Geräten mit unterschiedlichen Programmiersprachen, Methoden und Anwendungen zu tun. Gleichzeitig steigt die Anzahl an Angriffsvektoren und Schadsoftware ständig an. Damit erhöhen sich die Einfallstore und Angriffsmöglichkeiten für Cyberkriminelle enorm. Auch wenn wir mit neuen Geräten und Anwendungen das Internet immer einfacher, schneller und günstiger nutzen können, machen sie uns aber auch anfälliger für Bedrohungen aus dem Netz.

Wie gut sind Unternehmen heute gegen Cyberangriffe geschützt?

Unternehmen stehen zunehmend häufiger im Fadenkreuz von Cyberangriffen. Damit droht stets auch ein Daten- und Reputationsverlust. Im Grunde genommen sollten sich Unternehmen bereits als „gehackt" betrachten und die Investitionen in ihre IT-Sicherheit entsprechend anpassen. Es reicht dabei nicht, nur in Technologie zur Abwehr von Cyberangriffen zu investieren. Diese muss durch Reporting- und Kontrollsysteme sowie umfassende Mitarbeiterschulungen ergänzt werden. Privatanwender sollten darauf achten, dass sie zumindest grundlegende Sicherheitsvorkehrungen treffen: Einsatz einer Antiviren-Software, sichere Passwörter und zusätzliche Anwendungen zum Schutz der Privatsphäre im Internet. Wenn diese Sicherheitsvorkehrungen eingehalten werden, lassen sich private Geräte leichter schützen als Firmennetzwerke.

Kann es eine wasserdichte Lösung in Sachen Cybersicherheit geben?

Cyberkriminelle sind clever und schnell. Wenn wir uns hundert Möglichkeiten überlegen, wie sie in ein System eindringen könnten, finden sie eventuell einen Zugang, den wir nicht bedacht haben. Hundertprozentige Sicherheit würde dazu führen, dass Systeme oder Dienste nicht mehr nutzbar wären. Sicherheit sollte immer eine austarierte Investition in Effizienz und Effektivität sein.

Aus einer Reihe von Umfragen wissen wir: Viele Verbraucher glauben, dass sie „eh nichts ändern können". – Ist diese fatalistische Haltung für Sie nachvollziehbar?

IT-Sicherheit ist ein Thema, bei dem sich viele Verbraucher überfordert fühlen. Deshalb tun sie oft einfach gar nichts, um sich gegen Gefahren im Internet zu schützen. Dieses Vogel-Strauß-Verhalten bringt jedoch früher oder später Probleme mit sich. Verbraucher sollten daher zumindest die bereits angesprochenen Sicherheitsvorkehrungen beachten und bei Anwendungen zum Schutz ihrer Privatsphäre und Identität sowie gegen Schadsoftware auf einen erfahrenen Anbieter mit guten Testergebnissen vertrauen.

IT-Sicherheit ist mit nur wenigen „Klicks" erreichbar, trotzdem verzichten viele darauf. Wie motivieren Sie Menschen im Unternehmen und zu sicherem Verhalten?

Wer zumindest einen Basisschutz gegen Online-Bedrohungen einsetzt, macht es für Cyberkriminelle schwieriger und kostenintensiver, erfolgreich anzugreifen. Es geht also darum, Verbraucher zu motivieren, den ersten Schritt zu machen, um wenigstens ein Minimum an IT-Sicherheit auf ihren Systemen und Geräten zu gewährleisten. So können sie ein kostenloses Antivirenprogramm auf ihren Geräten installieren, das einen Basisschutz gegen Schadsoftware garantiert. Mit einer VPN-Anwendung (Virtual Private Network) lassen sich zudem Daten ganz einfach gegen Datendiebe schützen, etwa bei der Nutzung von öffentlichen WLANs. Wir sehen es als unsere Aufgabe, dem Anwender zu zeigen, wie er damit sein digitales Leben unbeschwert und sicher leben kann. Insgesamt ist hier aber noch immer viel Aufklärungsarbeit auf Verbraucher- wie auch auf Unternehmensebene zu leisten.

Sie haben zwei Wünsche frei für mehr IT-Sicherheit – welche sind das?

Erstens: Der Kampf für mehr Sicherheit im Internet ist nicht verloren, so lange wir ihn nicht aufgeben. Und das tun wir nicht. Ich wünsche mir daher, dass Anwender – egal ob Unternehmen oder Privatleute – zumindest über einen Basisschutz verfügen, wenn sie das Internet nutzen. Zweitens: Anwender sollten verstehen, dass IT-Sicherheit sie bei der Nutzung des Internets nicht ausbremst, sondern ihnen viel mehr Möglichkeiten bietet, das Internet noch besser, schneller und effektiver zu nutzen.

Travis Witteveen
ist CEO des Softwareherstellers Avira GmbH

Digitalisierung – aber sicher!

von Wilhelm Dresselhaus

Die vierte industrielle Revolution ist eine digitale Revolution. Ihr Hauptkennzeichen ist die weitgehende Digitalisierung praktisch aller Wirtschaftssektoren und Lebensbereiche. Milliarden von Geräten werden im Internet der Dinge – im sogenannten Internet of Things – vernetzt. Die Automatisierung schreitet in Industrie und Alltag weiter voran, reale und virtuelle Welten verschmelzen miteinander und unvorstellbar große Datenmengen („Big Data“) werden als Rohmaterial verarbeitet, um daraus hilfreiche Informationen abzuleiten.

Diese Megatrends bergen viel positives Potenzial. Damit ist nicht nur das Umsatzpotenzial gemeint für Unternehmen im Maschinen- und Anlagenbau, in der Automobilindustrie, der Elektrotechnik und vielen anderen Branchen, sondern auch das Potenzial, unser Leben wirklich besser zu machen: Durch das vernetzte und später automatisierte Fahren können Staus und Unfälle reduziert werden. Lkw, die als „Platoon“ dicht hintereinanderfahren, verbrauchen weniger Treibstoff und belasten die Umwelt in geringerem Maße. In der Medizin können Sensoren, die am Körper getragen werden und wichtige Vitalparameter überwachen, die Gesundheitsversorgung verbessern und sogar als Frühwarnsystem dienen. Es gibt unzählige Beispiele. Im Zentrum aller Anwendungsfälle steht die Vernetzung, und je mehr die Digitalisierung unser Leben durchdringt, desto mehr werden Kommunikationsnetze zur kritischen Infrastruktur, die es zu schützen gilt.

VERNETZTE GERÄTE SIND OFT LEICHT ZU MANIPULIEREN

Sicherheit ist hier zentral. Wie könnten wir uns sonst auf selbstfahrende Autos und Züge verlassen, den Gerätschaften in unserem Smart Home vertrauen oder unsere Gesundheit in die virtuellen Hände vernetzter Geräte legen? Auch bei weniger offensichtlichen Beispielen aus dem Hier und Jetzt zeigt sich, warum die Digitalisierung nur mit Sicherheit funktionieren kann: so etwa bei den Gefahren, die von Botnetzen ausgehen. Mit einem Botnetz bezeichnet man eine Anzahl von automatisierten Computerprogrammen, sogenannte Bots. Diese werden meist ohne Wissen der Inhaber auf Computern und vernetzten Geräten installiert und ferngesteuert für illegale Zwecke, etwa Angriffe auf Computernetze, eingesetzt. Tatsächlich existieren inzwischen bereits Botnetze, die größtenteils aus einfachen IoT-Geräten (Internet of Things) wie Webcams bestehen. Solche vernetzten Geräte verfügen in der Regel nicht über genügend Leistung, um sich mittels Sicherheitssoftware selbst zu schützen. Auch die verwendeten Protokolle sind häufig eher einfach und daher leicht zu manipulieren. So haben Botnetze in der jüngsten Vergangenheit ganze Geräteklassen dazu gebracht, dieselben Passwörter zu verwenden. In der Öffentlichkeit bekannt wurden Fälle, in denen Verkehrssysteme, Autos und Smart-TVs geknackt und manipuliert wurden.

> Um die Chancen der Digitalisierung nutzen zu können, muss den damit verbundenen Gefahren Rechnung getragen werden.

Die Gefahren sind sehr real und müssen ernst genommen werden, denn neben dem tatsächlichen Schaden steht auch das Vertrauen der Verbraucher und Unternehmen in neuartige digitale Dienste auf dem Spiel. Dieses Vertrauen hat erheblichen Einfluss darauf, ob sich ein Angebot auf dem Markt durchsetzen kann oder nicht.

DREI ELEMENTE EINER SICHERHEITSARCHITEKTUR

Um die Chancen der Digitalisierung nutzen zu können, muss auch den damit verbundenen Gefahren Rechnung getragen werden. Eine Sicherheitsarchitektur für das Internet der Dinge sollte deshalb drei Kernelemente beinhalten:

Erstens eine sichere, unveränderliche „Identität“ für jedes Gerät. Mit dieser Identität meldet sich das Gerät im Netz an und kann identifiziert sowie gegebenenfalls einer Geräteklasse zugewiesen werden. Zeigt der Sensor oder die Kamera später eine für diese Geräteklasse unübliche Aktivität, kann schnell eingegriffen werden.

Das zweite Kernelement besteht in einem sicheren Kommunikationskanal für das Gerätemanagement. Dazu gehört ein Authentifizierungsmechanismus, um die Geräteidentität festzustellen. Die Datenübertragung in beide Richtungen muss sichergestellt und geschützt sein – ebenso wie die Integrität der dabei übertragenen Daten. Dabei kommen beispielsweise verschiedene Techniken der Datenverschlüsselung zum Einsatz. Nur die vorgesehenen Adressaten dürfen die Daten erhalten; und zwar ohne,

DER IT-SICHERHEITSBLOG FÜR DEN MITTELSTAND

IT-Sicherheitsvorkehrungen in den Technologien („by design”) sind ein Weg zu mehr IT-Sicherheit. Im Mittelstandsblog von DsiN erhalten Entscheider Informationen zu unterschiedlichen IT-Sicherheitslösungen: Experten schreiben über ihre praktischen Erfahrungen, Sicherheit ganzheitlich im Unternehmen zu implementieren, und geben einfache Tipps. Seit Gründung vor vier Jahren zählte der Blog über 75.000 Leser, die sich über aktuelle Sicherheitsfragen im Unternehmen informieren.

www.dsin-blog.de

dass diese zuvor verändert oder in irgendeiner Weise manipuliert wurden.

Drittens benötigt das Gerät noch eine vertrauenswürdige Softwareumgebung. Das heißt, die Software, mit deren Hilfe das Gerät genutzt und gesteuert wird und die ggf. als Firmware auch auf dem Gerät läuft, muss sicher sein. Auch bei Firmware-Updates muss gewährleistet sein, dass sie ohne Manipulation aufgespielt werden.

ZUSÄTZLICH: SICHERHEITSWÄCHTER IM BETREIBERNETZ

Bei allen Vorsichtsmaßnahmen gibt es dennoch keine hundertprozentige Sicherheit. Längst haben Kriminelle den Nutzen des Internets der Dinge für sich entdeckt und entwickeln entsprechende Schadsoftware. Zudem müssen viele für den Informationsaustausch automatisierte (M2M-)Geräte billig sein, da sich sonst der Einsatz nicht lohnen würde. Aus diesem Grund kommunizieren gerade solche simplen Geräte nach wie vor häufig unverschlüsselt oder sind aufgrund ihrer einfachen Beschaffenheit nicht in der Lage, fortschrittliche Sicherheitsmechanismen zu unterstützen. Um sich vor Manipulation und Missbrauch zu schützen, tun Netzbetreiber deshalb gut daran, auf Netzwerkebene weitere Sicherheitsmaßnahmen zu implementieren. So werden nicht nur bekannte Angriffssignaturen erkannt und unterbunden. Moderne Lösungen sind auch in der Lage, anhand von ungewöhnlichen Aktivitäten im Datenverkehr neue Angriffsmuster zu erkennen. Die betreffenden Geräte werden identifiziert und können, falls nötig, vom Netz genommen werden.

AUFKLÄRUNG UND INFORMATION WICHTIGER BAUSTEIN

Generell kommt dem Netzbetreiber in einer digitalisierten Wirtschaft und Gesellschaft eine immer wichtigere Rolle zu. Während Telekommunikationsnetze früherer Jahre separat und abgeschottet waren, ist dies heute nicht mehr der Fall. Deshalb hat die Sicherheit heute eine immer größere Bedeutung. Netzelemente, die heute mehr und mehr auf Standard-Hardware laufen, Cloudifizierung und Virtualisierung sorgen dafür, dass neue Bedrohungsszenarien entstehen, denen Rechnung getragen werden muss. Nur durch ein umfassendes Sicherheitsmanagement über das gesamte Netz hinweg lassen sich moderne Telekommunikationsnetze wirksam schützen und das Vertrauen der Firmenkunden und Verbraucher gewinnen. Aufklärung und Information sind hier besonders wichtig: Verbraucher sowie kleine und mittelständische Unternehmen ohne eigene Expertise sollten sich beim Hersteller sowie über unabhängige Quellen informieren, welche Sicherheitsmaßnahmen in den Geräten, in der Kommunikation zwischen Geräten und im Netz sinnvoll sind, bevor sie eine entsprechende Anschaffung tätigen.

www.10jahre.dsin.de

Zum Abschluss des DsiN-Jahreskongresses sprechen BSI-Präsident Arne Schönbohm sowie die Bundesbeauftragte für Datenschutz Andrea Voßhoff mit dem Autor dieses Beitrags und weiteren Experten über Perspektiven digitaler Sicherheit für Wirtschaft und Gesellschaft.

Wilhelm Dresselhaus
ist Sprecher der Geschäftsführung der Nokia Solutions and Networks GmbH

Gemeinsam dem Löwen begegnen

von Renate Radon

Allein auf Amerikas Straßen sind 2015 mehr als 35.000 Menschen gestorben. Der tägliche Verkehrstod gehört dort wie anderswo so selbstverständlich zum Alltag, dass er kaum noch eine Randnotiz in der Lokalzeitung wert ist. Doch die fatale Kollision eines Tesla-Fahrers mit einem Lastwagen in Florida sorgte im Sommer 2016 weltweit für Schlagzeilen. Der Grund: Es handelt sich um den ersten tödlichen Unfall eines selbstfahrenden Autos. Der Unglücksfahrer hatte sich auf seinen Autopiloten verlassen, doch das System hat den Lkw nicht als Hindernis identifiziert.

Seither ist die Diskussion um Sicherheitsrisiken autonomer Fahrzeuge neu entflammt. Dabei spielt es kaum eine Rolle, dass mehr als 90 Prozent aller Verkehrsunfälle auf menschliches Versagen zurückzuführen sind. Autonomes Fahren dagegen kann den Straßenverkehr deutlich sicherer machen. Das US-Transportministerium geht davon aus, dass 19 von 20 Unfällen in Zukunft verhindert werden können.

Es liegt in der menschlichen Natur, Unbekanntes mehr zu fürchten als Bekanntes, meinen Experten wie der Potsdamer Risikoforscher Ortwin Renn. „Was ich nicht kenne, ist mir unheimlich“, sagte Renn in einem Interview mit dem *Spiegel*. Dass die größte Angst oft sogar dort herrsche, wo die reale Gefahr am geringsten sei, führt er auf die Zeit der Besiedlung der Savanne durch unsere Urahnen zurück. „Es gibt einen Löwen, aber keiner hat mit dieser Sorte von Löwen irgendeine Erfahrung, und schon steigt die Angst ins Unermessliche.“ Das erkläre auch, warum neue Technologien in der

DIGITALER BILDUNGSPAKT

Der Digitale Bildungspakt gründet in der Überzeugung, dass digitale Kompetenzen die Voraussetzung für Teilhabe am gesellschaftlichen Leben und beruflichen Erfolg sind. Der Pakt liefert Denkanstöße und Handlungsempfehlungen zur Digitalisierung im deutschen Bildungswesen und leistet durch konkrete Projekte selbst einen Beitrag zur Umsetzung.

www.digitaler-bildungspakt.de

Bevölkerung oft auf starke Vorbehalte stoßen – es fehle uns schlicht an Erfahrung.

Doch anders als der Löwe in der Savanne sind Technologien nicht einfach da. Wir müssen sie entwickeln und ihre Verbreitung vorantreiben, damit wir sie nutzen können. Und nur indem wir sie nutzen, können wir die notwendigen Erfahrungen sammeln, um Ängste ab- und Vertrauen aufzubauen. Es gehört also durchaus ein wenig Mut dazu: Ohne den hätte die Menschheit schließlich nie den sicheren Urwald verlassen, um in der Savanne Erfahrungen mit Löwen zu sammeln.

DIE ANGST VOR NEUEM UND UNBEKANNTEM ÜBERWINDEN

Beispiel digitale Bildung: In einer Welt, die immer stärker durch digitale Technologien geprägt wird, ist digitale Kompetenz die entscheidende Voraussetzung für Bildung, für beruflichen Erfolg und für die Teilhabe am gesellschaftlichen Leben. Rund 90 Prozent der Berufe werden in naher Zukunft digitale Kompetenzen erfordern. Das Beherrschen digitaler Technologien entscheidet über die Chancen des Einzelnen auf dem Arbeitsmarkt. Gleichzeitig hängt die Zukunft unserer Wirtschaft davon ab, dass sie genügend Fachkräfte mit digitalen Qualifikationen findet. Doch derzeit ist Deutschland laut „International Computer and Information Literacy Study“ (ICILS) in Sachen digitaler Bildung bestenfalls Mittelmaß. So setzen beispielsweise in keinem anderen ICILS-Teilnehmerland Lehrkräfte Computer so selten im Unterricht ein wie in Deutschland. Damit verschenken sie gewaltige Chancen. Denn der Einsatz digitaler Technologien im Unterricht ermöglicht nachweislich lebendigere Lernerfahrungen und nachhaltigere Lernerfolge.

Deshalb hat Microsoft 2016 einen Digitalen Bildungspakt für Deutschland angestoßen, der inzwischen eine Vielzahl von Unternehmern, Wissenschaftlern, Bildungsexperten und Pädagogen, kommunalen Entscheidern und Technologie-Spezialisten vereint. Deutschland sicher im Netz ist auch hier unser Partner. Nur durch gemeinsames, mutiges und verantwortungsvolles Handeln können wir dafür sorgen, dass zukünftige Generationen die Chancen neuer Technologien voll nutzen können.

DIE VERBREITUNG DIGITALER TECHNOLOGIEN VORANTREIBEN

Auch die digitale Transformation unserer Wirtschaft müssen wir jetzt mutig vorantreiben. Denn die Welt da draußen dreht sich immer schneller. Junge Hightech-Unternehmen drängen mit Macht in gewachsene Märkte und stellen die Spielregeln in allen Branchen auf den Kopf. Entscheidend ist es, die digitale Transformation jetzt als Chance und nicht als Bedrohung wahrzunehmen.

AKTIONSBUND DIGITALE SICHERHEIT

Um Verbrauchern den Zugang zu guten Initiativen zu erleichtern, hat sich der Aktionsbund Digitale Sicherheit zur Aufgabe gemacht, Initiativen und Veranstaltungen von gemeinnützigen Organisationen zusammenzubringen: Ein Aktionsfinder führt Internetnutzer direkt zu den Aufklärungsangeboten, die ihren Bedürfnissen, Wissensniveaus und ihrer lokalen Umgebung entsprechen.

www.aktionsbund.org

Beispiel Cloud Computing: Zwar können firmeneigene IT-Infrastrukturen heute kaum noch dieselbe Sicherheit gegen Datenmissbrauch und Datenverlust bieten wie die Cloud. Dennoch verhindern Sicherheitsbedenken nach wie vor, dass Unternehmen konsequent in diese wichtige Basistechnologie investieren. Auch hier müssen wir gemeinsam mit einer umfassenden Aufklärungsarbeit und absoluter Transparenz gegensteuern. Denn das Cloud Computing ist die Voraussetzung für sämtliche Zukunftskonzepte – von dem Internet der Dinge und der Industrie 4.0 über vernetzte Wissensarbeit bis zur intelligenten Auswertung großer Datenmengen. Die Nutzung der Cloud ist deshalb keine Frage des „ob“, sondern allenfalls eine Frage des „wie“.

> Die Nutzung der Cloud ist keine Frage des „ob“, sondern allenfalls eine Frage des „wie“.

Fakt ist: Es liegt in der Verantwortung der IT-Wirtschaft, nutzerfreundliche und sichere Lösungen zu entwickeln und deren Funktionsprinzipien sowie mögliche Risiken transparent zu machen. Außerdem brauchen wir eine Politik, die Rahmenbedingungen vorgibt, unter denen sich neue Technologien so entwickeln können, dass sie der Gesellschaft, der Wirtschaft, der Verwaltung und dem Bürger von möglichst großem Nutzen sind. Aber wir brauchen auch digital mündige User, die Risiken realistisch einschätzen können, Verantwortung für ihr eigenes Handeln übernehmen, neue Technologien kompetent beherrschen und angebotene Sicherheitslösungen auch wirklich anwenden.

Und letztlich müssen alle drei Gruppen an einem Strang ziehen, um gemeinsam mit Mut und Verantwortungsbewusstsein die Verbreitung neuer Technologien voranzutreiben. Darum sind Initiativen wie Deutschland sicher im Netz so wichtig. Seit ihrer Gründung im Jahr 2006 hat DsiN viel erreicht. Mit der fortschreitenden Digitalisierung, der zunehmenden Vernetzung und der steigenden Komplexität unserer Welt wächst auch der Aufklärungsbedarf. Wir müssen weiter sensibilisieren, Basiswissen vermitteln, die Umsetzungsbereitschaft verbessern und Vertrauen aufbauen. Dabei gilt es, mit dem rasanten technologischen Wandel Schritt zu halten. Um das in Zukunft leisten zu können, müssen wir alle Kräfte bündeln und möglichst viele Akteure einbinden. Denn es ist keine Lösung, im Urwald abzuwarten, bis andere Erfahrungen mit dem Löwen gesammelt haben. Diese anderen gewinnen in der Zwischenzeit sonst einen so großen Wissensvorsprung, dass sie kaum noch einzuholen sind. In Zeiten rasant fortschreitender Digitalisierung gilt das mehr denn je. Wir können es uns als Gesellschaft und als Wirtschaftsstandort schlicht nicht leisten, allzu lange zu zögern.

Renate Radon
ist Mitglied der Geschäftsleitung von Microsoft Deutschland und im Vorstand von Deutschland sicher im Netz e.V.

Was erleichtert die digitale Transformation?

Warum Aufklärung nicht unterschätzt werden darf und weiterhin wichtig bleibt

von Torsten Küpper

Die Digitalisierung unterzieht unsere Gesellschaft einer weitreichenden Transformation. Digitale Technologien, vernetzte Produktionsweisen, die digitale Speicherung und Verbreitung von Wissen sowie moderne Logistikketten werden immer selbstverständlichere Bestandteile unseres Alltags.

Um diesen umfassenden gesellschaftlichen Veränderungsprozess im Sinne aller Beteiligten erfolgreich gestalten zu können, müssen alle von der Digitalisierung betroffenen Akteure eingebunden werden. Jedem kommt dabei eine spezifische Rolle zu: Während der Staat die regulatorischen Rahmenbedingungen festlegt, müssen die Informations- und Kommunikationsunternehmen sichere Produkte anbieten. Ähnlich wie im Straßenverkehr müssen jedoch auch die Anwender der Produkte wissen, wie sie am besten – und vor allem gefahrlos – auf der „Datenautobahn“ unterwegs sein können.

DIE DIGITALE MÜNDIGKEIT

Nutzer müssen sich als mündige, aufgeklärte Bürger sicher und selbstständig in der digitalisierten Gesellschaft bewegen können. Nur so kann das wichtige Grundrecht auf informationelle Selbstbestimmung substanziell gewahrt bleiben. Digitale Mündigkeit besteht deshalb aus zwei Komponenten: digitale Kompetenz, also die Fähigkeit zum richtigen Umgang mit dem Internet, und digitale Selbstbestimmung, also die Fähigkeit, bewusst zu entscheiden, in welchem Umfang man sich im Internet bewegen möchte.

> Die Nutzer müssen sich als mündige und aufgeklärte Bürger sicher und selbstständig in der digitalisierten Gesellschaft bewegen können.

Oft schwingt im öffentlichen Diskurs über die Folgen der Digitalisierung die Angst mit, nicht ausreichend selbstbestimmt zu handeln. Dieses erodierende Grundvertrauen kann dazu führen, dass das Potenzial der Digitalisierung zum Nutzen aller Akteure nicht vollständig ausgeschöpft wird. Deshalb muss sowohl die Politik als auch die Wirtschaft die vorhandenen Sorgen ernst nehmen. Manche Unsicherheit kommt sicher auch von mangelnder Kenntnis darüber, wie digitale Technologien funktionieren und wie leicht sich Maßnahmen ergreifen lassen, um beispielsweise besser gegen Internetkriminalität geschützt zu sein.

DAS AKZEPTIEREN INNOVATIVER DIENSTE

Eine stärkere Sensibilisierung und vor allem Befähigung des Nutzers zum sicheren Umgang mit dem Internet ist zugleich Voraussetzung für die langfristige Akzeptanz von innovativen Diensten. Nur wenn diese Akzeptanz gegeben ist, wird die Digitalisierung gelingen. Deshalb müssen sich Politik und Wirtschaft weiterhin nachdrücklich mit diesen Themen befassen. Alle beteiligten Akteure müssen dabei ihren Beitrag zur digitalen Aufklärung leisten.

Huawei sieht sich als Partner der digitalen Aufklärung und ist davon überzeugt, dass die Digitalisierung unsere Gesellschaft und unser Leben positiv verändern wird. Dieses Selbstverständnis steht im Einklang mit den Zielen von Deutschland sicher im Netz und deshalb freut sich Huawei, ein aktives Mitglied zu sein und die Initiative in ihrem Wirken nach Kräften zu unterstützen.

KOMPETENZEN IN SCHULEN TRAINIEREN

So wie die Grundregeln im Fahrradfahren schon früh vermittelt werden, ist auch die Sensibilisierung für Sicherheit und Schutz im Netz bereits im jungen Schulalter sinnvoll: Verhaltensregeln werden hier eingeübt und als selbstverständlich angenommen. Mit einem neuen Projekt für Lehrer schafft DsiN ein niedrigschwelliges Angebot, das bestehende Initiativen zur Steigerung digitaler Kompetenzen für den Einsatz im Unterricht einfach aufbereitet.

info@sicher-im-netz.de

Torsten Küpper
ist Mitglied der Geschäftsleitung beim Telekommunikationsausrüster Huawei

Vergesst die Älteren nicht!

Wie wir die Generation 60plus fürs Netz gewinnen können

von Dr. Barbara Keck

Selbstbewusst, interessiert und souverän: So nutzen viele Ältere bereits das Internet. Der Goldene Internetpreis, den wir seit 2012 gemeinsam mit Deutschland sicher im Netz vergeben, zeigt uns immer wieder tolle Persönlichkeiten, neue Ideen und vielfältige Möglichkeiten sowie aktive Organisationen und vielversprechende Projekte. Mit diesem Wettbewerb und weiteren Initiativen möchten wir als Bundesarbeitsgemeinschaft der Senioren-Organisationen (BAGSO) Mut machen, aufklären und bestehende Barrieren abbauen.

Denn es gibt sie natürlich immer noch – die Seniorinnen und Senioren, die sich nicht trauen, die Internetwelt für sich zu entdecken. Für viele dieser älteren „Nonliner“ gab es bisher kaum oder wenig Berührungspunkte mit dem Internet.

In den Schulen gibt es zum Beispiel viele gute Ansätze, die Medienkompetenz der Kinder zu fördern: durch witzige Filme, Materialien, die zum Austausch anregen, und durch aktive Einbindung der digitalen Welt in den Schulalltag. Auch im Berufsleben haben viele Menschen die Chance, über aktuelle digitale Entwicklungen auf dem Laufenden zu bleiben.

Und im Alter? Hier gibt es Computerclubs und Internetkurse, die mit viel Engagement und Erfolg Ältere im Netz begleiten. Diese Erfahrungsorte sind aber weder flächendeckend noch mit guten Konzepten und Materialien ausgestattet. Hier stehen wir noch ganz am Anfang.

FÜR DIGITALE SENIORENARBEIT

Ältere Generationen haben ein steigendes Interesse am Internet sowie auch das Bedürfnis nach Hilfe bei der Anwendung. Im Projekt Digital-Kompass erhalten Menschen, die ältere Bürger bei digitalen Fragen begleiten, geeignete Materialien sowie die Möglichkeit zur direkten Vernetzung mit Experten in „Digitalen Stammtischen“. Das Projekt wird vom Bundesministerium der Justiz und für Verbraucherschutz gefördert und von DsiN im Verbund mit BAGSO durchgeführt.

www.digital-kompass.de

Gemeinsam mit DsiN haben wir uns im Digital-Kompass zur Aufgabe gemacht, die älteren Multiplikatoren in ihrer Arbeit zu unterstützen. Ziel ist es, ein lebendiges Portal für Lotsen, Trainerinnen und Trainer, Helfer und Engagierte zu schaffen, die Ältere auf dem Weg ins und im Netz begleiten.

Sicher im Netz den Einstieg zu finden und unterwegs zu sein, ist nicht nur eine Frage von Spamfiltern, Firewalls oder Datenschutz. Wer sich sicher im Internet bewegen möchte, muss zunächst sicher ins Netz. Oft wählen Einsteiger den günstigsten Tarif, wundern sich dann aber über zusätzliche Kosten für Überschreitungen und steigen wieder aus. Der Einstieg kann jedoch maßgeblich erleichtert werden durch gute Vorinstallationen und Service-Pakete, die die E-Mail-Adresse anlegen, erste Kontakte ins Adressbuch aufnehmen und gewünschte Apps installieren. Hierfür gibt es gute Angebote. Es lohnt sich, diese bekannt zu machen und die nicht service-verwöhnte Generation 60plus zu ermutigen, solche Einstiegsangebote zu nutzen.

Viele ältere Kunden erwarten auch, dass die Sicherheit gleich mit dem Gerät mitgeliefert wird. Sich selber nach sechs Monaten wieder kümmern zu müssen, ist nicht der Service, den sich diese Zielgruppe wünscht.

Wir fordern eine nutzerfreundlichere Gestaltung von Internet-Plattformen und klarere Informationen. Viele Verkaufsportale sind bereits auf einem guten Weg. Dennoch erleben Nutzer immer wieder Überraschungen. So werden Arzneimittel zu spät oder gar nicht geliefert. Hier brauchen wir eine schnellere Information, was geliefert werden kann, und zwar bevor sich das Rezept auf den Weg macht. Gute Information fördert das Vertrauen und das Sicherheitsgefühl.

Halten wir fest: Sicherheit gewinnt mit zunehmendem Alter an Bedeutung. Und: Ältere Kundinnen und Kunden wünschen sich nutzerfreundliche und kräftesparende Sicherheitslösungen. Hier besteht noch viel Handlungsbedarf! Ältere Menschen können uns dabei den Weg weisen, wenn wir sie besser bei Entwicklungen einbeziehen. Wenn wir mehr Sicherheit schaffen, die keinen hohen Aufwand für den Kunden erfordert, dann werden wir die Seniorinnen und Senioren stärker für die digitalen Chancen gewinnen.

Bisher bewegen sich knapp 49 Prozent der 21 Millionen Menschen über 65 Jahren selbstbewusst, interessiert und souverän im Internet. Wir haben noch viel gemeinsam zu tun!

Schauen Sie doch einmal in der Material-Fundgrube vorbei, wo Sie aktuelle Broschüren und passende Vorlagen für Schulungen und Beratungen finden, oder melden Sie sich einfach zu einem Digitalen Stammtisch an: www.digital-kompass.de

Dr. Barbara Keck
ist Geschäftsführerin der BAGSO Service Gesellschaft

„Wo liegt das Problem?“

Eigentlich ganz einfach, dieses Internet. Wie komplex die Technik dahinter ist, merken User oft erst bei Problemen. Dann brauchen Unternehmen wie Verbraucher vor allem Problemlöser, die sie verschonen mit technischer Komplexität.

Wie können Aufklärungsmaßnahmen das Bewusstsein für IT-Sicherheitsfragen steigern?

Kah-Kin Ho
Senior Director Public Sector bei FireEye
Chief Information Security Officers fällt es oft schwer, der Geschäftsleitung die Brisanz von IT-Sicherheit zu vermitteln – aufgrund ihres vorwiegend technischen Hintergrunds sprechen sie selten dieselbe Sprache. Wenn sie etwa erzählen, was sie im letzten Monat gemacht haben – bei uns wurden unter anderem 423.132 Viren entdeckt und mehr als zwei Millionen Verbindungen blockiert –, reagiert der Vorstand meist nach dem Schema: „Eindrucksvoll, na und?” Sinnvoller ist ein anderer Ansatz. Letztens haben wir zwei Angriffe erkannt und abgewehrt, die von kriminellen Vereinigungen in Osteuropa ausgingen. So konnten wir Umsatzeinbußen und Kosten in Höhe von etwa 70 Millionen Euro verhindern und vereiteln, dass Kreditkartendaten von 10 Millionen Kunden gestohlen wurden. Das ist eine Aussage, mit der Vorstände oder Geschäftsführer etwas anfangen können: Ausgaben in IT-Sicherheit lohnen sich.

Martin Drechsler
Geschäftsführer der FSM – Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.
Wir alle wollen ein Höchstmaß an Sicherheit, sind aber oft nicht bereit, viel dafür zu tun. Informationen über IT-Sicherheit müssen uns fast aufgezwungen und in leicht verdaulichen Häppchen serviert werden. Dabei sollte auf die jeweiligen Bedürfnisse eingegangen werden, und die sind bei Unternehmen anders als bei Familien mit Kindern. Familien brauchen Hinweise auf gute und sichere Angebote und Produkte, damit sie die für sich beste Entscheidung treffen können. Aus Nutzersicht sollten Informationen ansprechend und vor allem verständlich sein. Es ist nicht immer nötig, alle Informationen zu einem Thema gebündelt zu erfahren. Wichtiger sind Hinweise, die sich auf konkrete Situationen beziehen. Die Nutzerfreundlichkeit sollte immer im Vordergrund stehen. Deshalb wäre eine zentrale Anlaufstelle ideal, bei der Nutzer zuverlässig alle für sie notwendigen Informationen finden. Die zweitbeste Option: die bestehenden Plattformen noch besser untereinander zu verlinken.

Prof. Dr. Sachar Paulus
Experte für IT-Sicherheit an der Hochschule Mannheim und im Beirat von Deutschland sicher im Netz e.V.
Gerade im Umfeld der IT-Sicherheit herrscht viel Aufklärungs- und Abstimmungsbedarf, entsprechend viele Vereine und Organisationen gibt es hiefür. Würde sich die Durchschlagskraft erhöhen, wenn gleichartige Initiativen gebündelt würden? Nein. Ich denke, die Vielfalt ist für einen angemessenen Umgang mit der IT-Sicherheit förderlich. Natürlich muss klar sein, welche Organisation wofür steht, wer Partner der Politik ist und wer als Interessensvertreter der Wirtschaft wahrgenommen wird. Gerade Mittelständler haben besondere Fragen, denn sie sind besonders exponiert: Sie sind ebenso interessant für Cyberangreifer wie Großunternehmen, haben aber deutlich weniger Möglichkeiten, sich angemessen vorzubereiten. Drei wirksame Ansatzpunkte sehe ich: einen Beauftragten für IT-Sicherheit, eine Risikoanalyse mithilfe eines externen Experten und möglichst aktuelle Betriebssysteme und Anwendungen.

Vernetztes und automatisiertes Fahren – ein Quantensprung für die Sicherheit

von Dr. Joachim Damasky

Die deutsche Automobilindustrie treibt die Digitalisierung im und um das Auto konsequent voran. Bis zum Jahr 2018 invstieren unsere Hersteller 16 bis 18 Milliarden Euro in das vernetzte und automatisierte Fahren, denn es macht individuelle Mobilität effizienter, komfortabler und sicherer.

VERNETZTES FAHREN – ABER SICHER!

Der DsiN-Sicherheitsindex 2016 zeigt: Die Digitalisierung der Mobilität eröffnet Chancen, aber der Wandel wirft auch neue Fragen auf. Die DsiN-Initiative zum vernetzten Fahren informiert Verbraucher über aktuelle Projekte im Bereich der mobilen Vernetzung und beantwortet Fragen zu Sicherheit und Datenschutz. Sie steht unter der Schirmherrschaft des Bundesministeriums für Verkehr und digitale Infrastruktur.

mobilitaet@sicher-im-netz.de

Intelligente Vernetzung ermöglicht eine effiziente Steuerung des Verkehrsflusses. Fahrzeuge werden miteinander und mit ihrem Umfeld kommunizieren, sie werden sich über die Verkehrslage austauschen, sie werden sich gegenseitig vor Gefahren warnen. Zudem werden Autos künftig in der Lage sein, durch hochautomatisierte Fahrfunktionen den Fahrer in Routinesituationen noch weiter zu entlasten, in kritischen Situationen zu unterstützen oder diese sogar zu vermeiden. Autofahren wird damit noch sicherer.

Die Entwicklung von automatisierten Fahrfunktionen geht Schritt für Schritt voran: von der aktuellen Teilautomatisierung über die Hochautomatisierung ab dem Jahr 2020 zur Vollautomatisierung ab 2025. Dabei verlieren wir das Thema Sicherheit nie aus den Augen. Unsere Hersteller informieren die Kunden genau, was die Systeme schon können und was nicht. Bei den heutigen Angeboten und der derzeitigen Gesetzeslage muss der Fahrer immer die Kontrolle behalten. Das gilt zum Beispiel für Einparkhilfen oder Spurhalteassistenten. In naher Zukunft wird es Parkhäuser geben, wo man mit dem Smartphone einchecken kann und sich das Auto dann selbstständig seinen Parkplatz sucht. Mit Fahrzeugen, die vollautomatisch fahren, ist hingegen in nächster Zeit nicht zu rechnen.

Laut Roland Berger liegen die deutschen Hersteller bei der Entwicklung automatisierter Fahrfunktionen im internationalen Vergleich an der Spitze. Und auch die Verbraucher setzen auf die Automobilindustrie. So hat eine repräsentative Umfrage von TNS Infratest in Deutschland ergeben, dass die Mehrheit einem Automobilhersteller am ehesten zutraut, das erste und gleichzeitig erfolgreichste automatisierte Fahrzeug auf den Markt zu bringen. Voraussetzung dafür, dass sich die Menschen für diese neue Form der Mobilität begeistern, ist die Zuverlässigkeit der Fahrzeuge. Sicherheit hat absoluten Vorrang. Systeme werden erst dann in den Markt gebracht, wenn sie technisch völlig ausgereift und mit redundanten Sicherheits- und Kontrollsystemen ausgestattet sind. Hier arbeiten die deutschen Hersteller mit größtmöglicher Sorgfalt.

Gleiches gilt für den Umgang mit den im Auto anfallenden Daten. Hierauf legen wir besonderes Augenmerk. Um ein Höchstmaß an Sicherheit zu gewährleisten, werden die Datensysteme für die Navigations-, Telematik- und Infotainment-Anwendungen getrennt von den fahrrelevanten Systemen in der Fahrzeugelektronik eingebaut. Sicherheitsrelevante Bereiche im vernetzten Fahrzeug werden zudem durch spezielle Hard- und Softwaresysteme vor unerlaubten Zugriffen geschützt. Das erschwert Hacker-Angriffe.

Durch die zunehmende Vernetzung und Automatisierung fallen viele Daten an, deren datenschutzrechtliche Absicherung geregelt werden muss. Das Auto wird zur mobilen Kommunikationsplattform. Dazu entwickeln die Automobilunternehmen technische Lösungen, die den Datenzugriff für bestimmte Personenkreise erlauben und andere davon ausschließen. Die Mitgliedsunternehmen des VDA haben hierfür gemeinsame Datenschutz-Prinzipien festgelegt. Diese umfassen die drei Kernpunkte Transparenz, Selbstbestimmung und Datensicherheit.

Denn nur wenn der Kunde informiert ist und entscheiden kann, welche Angebote er nutzen möchte, wird er die neuen Technologien und Dienstleistungen annehmen. Anstatt Risikodebatten zu führen, sollten wir Chancen und Herausforderungen des vernetzten und automatisierten Fahrens klar darstellen. Mit leistungsfähigen Produkten und einer eingebauten Sicherheitskultur leistet die deutsche Automobilindustrie hierzu ihren Beitrag.

www.10jahre.dsin.de

Schauen Sie, was Norbert Barthle, der Parlamentarische Staatssekretär des Bundesministeriums für Verkehr und digitale Infrastruktur, im Bürgerforum Wirtschaft des DsiN-Jahreskongresses über die „Vernetzung der Welt“ vorträgt. Auch ein Interview mit dem Autor finden Sie online.

Dr. Joachim Damasky
ist Geschäftsführer des Verbands der Automobilindustrie (VDA) und im Beirat von Deutschland sicher im Netz e.V.

Früh übt sich

IT-Sicherheit in der Berufsschulbildung verankern

von Eugen Straubinger

„Es macht Freude, in einem vom Sturm gepeitschten Schiff zu sein, wenn man sicher ist, dass es nicht untergehen wird“, stellte einst der französische Mathematiker und Physiker Blaise Pascal fest. Übertragen auf unsere IT-gepägte Zeit könnte man sagen: Man hat viel mehr Spaß im Internet, wenn man weiß, wie man sich in seinem privaten wie beruflichen Umfeld vor Datenklau, Viren, Spam, Phishing und anderen negativen Begleiterscheinungen der Digitalisierung schützen kann. Um seine Informationshoheit zu bewahren und nicht in den Stürmen des Netzes unterzugehen, sollte man deshalb bereits frühzeitig eine grundlegende Sensibilität und vor allem Handlungskompetenz in Sachen IT-Sicherheit vermittelt bekommen.

Als Pilotschule führte die Philipp-Matthäus-Hahn-Schule (gewerbliches Schulzentrum des Zollernalbkreises) das Projekt „Bottum-Up: Berufsschüler für IT-Sicherheit“ von Deutschland sicher im Netz durch, bei dem die Jugendlichen einen selbstverständlichen Umgang mit Smartphone und Computer zeigten. Defizite kamen jedoch deutlich zum Vorschein bei sicherheitsrelevanten Aspekten, die teilweise absolutes Neuland für die Schülerinnen und Schüler darstellten.

Diese Lücken lassen sich nur mit einem innovativen System an Bildungs- und Aufklärungsarbeit beseitigen. Beginnend in der Primarstufe muss Grundlagenwissen über IT-Sicherheit vermittelt werden. Die Kinder entwickeln sich in dieser Phase bereits sehr früh zu Multiplikatoren, welche die Informationen sowie die Bedeutung des digitalen Wandels in die eigenen Familien tragen. Darauf aufbauend und anschließend müssen die Schultypen der Sekundarbildung die Thematik nahtlos aufnehmen und weiterführen.

BOTTOM-UP

Im Projekt „Bottom-Up: Berufsschüler für IT-Sicherheit“ werden künftige Mitarbeiter von kleinen und mittelständischen Unternehmen (KMU) in ihrer dualen Ausbildung zu IT-Sicherheitsfragen geschult. Sie erhalten praxisnahes IT-Sicherheitswissen und werden sensibilisiert, das Wissen in den Betrieben einzusetzen und weiterzugeben – für mehr IT-Sicherheit und den Schutz von Daten in KMU. Das Projekt erfolgt mit Förderung des Bundeswirtschaftsministeriums.

www.dsin-berufsschulen.de

Die beruflichen Schulen werden zukünftig eine besondere Schlüsselposition bei der Vermittlung von sicherheitsrelevanten IT-Aspekten einnehmen. An den beruflichen Schulen besteht die einmalige Chance, die künftigen Mitarbeiter und Mitarbeiterinnen insbesondere von kleinen und mittelständischen Unternehmen (KMU) mit einem praxisnahen IT-Sicherheitswissen auszustatten. Diese Schulart befähigt die Schülerinnen und Schüler mit der Stärkung des digitalen Selbstvertrauens, das Wissen in den Betrieben einzusetzen und als Multiplikatoren weiterzugeben.

Die Studie „DsiN-Sicherheitsmonitor Mittelstand 2016“ identifizierte eindeutige Trends und auch Schwachstellen der Digitalisierung bei mittelständischen Unternehmen. Einerseits steigt die Nutzung von Firmennetzwerken und Social Media in den KMU kontinuierlich, andererseits ergreift eine Vielzahl dieser Unternehmen keinerlei Schutzvorkehrungen oder Absicherungen gegen Fremdzugriffe oder andere Bedrohungen aus dem World Wide Web. In Teilbereichen konnte die Studie sogar Stagnationen bzw. Rückläufigkeit bei Vorkehrungen der IT-Sicherheit in Unternehmen belegen.

Der hier dokumentierten Diskrepanz muss mit Nachdruck entgegengewirkt werden, indem Unternehmen, Politik, Schulen und Verbände besser zusammenarbeiten. Die Möglichkeiten und die absolute Notwendigkeit des Datenschutzes müssen letztendlich in einem ausgeprägten Maße in die entsprechenden Lehrpläne der verschiedenen Bildungsgänge Eingang finden.

Nur wenn Vorkehrungen für die IT-Sicherheit mit der schnell voranschreitenden Digitalisierung schritthalten können, ist eine Wachstums- und Wettbewerbsfähigkeit der KMU nachhaltig möglich.

Durch das Zusammenspiel der verschiedensten Maßnahmen (mit besonderer Ausprägung in der Schulbildung) kann zukünftig sichergestellt werden, dass es im privaten und beruflichen Umfeld Spaß und Freude bereitet, in einem Sturm von IT-Bedrohungen zu navigieren und das mit dem Bewusstsein, dass das eigene „Schiff“ weitestgehend sicher ist und man nicht untergehen wird.

www.10jahre.dsin.de

„Die Digitale Revolution und die Zukunft der Bildung“ – schauen Sie sich den zukunftsweisenden Vortrag des Philosophen und Publizisten Richard David Precht zum 10-jährigen Jubiläum von DsiN an.

OStD Eugen Straubinger ist Bundesvorsitzender des Bundesverbands der Lehrerinnen und Lehrer an beruflichen Schulen e.V. (BLBS), Schulleiter der Philipp-Matthäus-Hahn-Schule in Balingen und im Beirat von Deutschland sicher im Netz e.V.

Besserer Schutz für unsere Daten

von Stefan Koetz

Die bestehende Vernetzung von Märkten, Branchen, Industrien und der Gesellschaft wird sich in den kommenden Jahren radikal verändern: Stand bisher die Basisvernetzung per Breitbandinternet auf Infrastrukturebene im Vordergrund, geht es zukünftig um die Vernetzung nahezu aller Dinge zu einem „Internet of Things“. In den kommenden Jahren werden nicht mehr nur Millionen Smartphones und Computer vernetzt sein; mit der massiven Zunahme vernetzter Geräte steigt auch das Datenvolumen, das zukünftig in den Netzen transportiert werden muss. Die integrierte Mobilfunk- und Netztechnologie 5G, die derzeit entwickelt wird, hat den Anspruch, die erhöhten Anforderungen an die Kommunikation in einer vollständig vernetzten Informationsgesellschaft sehr viel umfassender als bisher zu erfüllen. Gleichzeitig wachsen aber auch die Anforderungen an die IT-Sicherheit dieser vernetzten Umwelt.

CLOUD-SCOUT-REPORT

Cloud-Wissen und -Kompetenzen sind entscheidend für eine sichere Nutzung der Cloud. Im DsiN-Sicherheitsmonitor 2016 wurde zudem deutlich, dass das Vertrauen in die Cloud steigt, je stärker eine inhaltliche Auseinandersetzung damit erfolgt. Im DsiN-Cloud-Scout werden Unternehmen zu grundlegenden Kompetenzen befragt und erhalten erste Hinweise für eine ernsthafte Befassung mit dem Thema. Der DsiN-Cloud-Scout-Report 2015 fasst die Ergebnisse erstmals – europaweit – zusammen.

cloudscout.cloudwatchhub.eu

MEHR VERNETZUNG VERLANGT MEHR IT-SICHERHEIT

Unternehmen müssen sich stärker als bisher jederzeit auf die Sicherheit ihrer ITK-Infrastruktur, ihrer Systeme und Algorithmen verlassen können. Telekommunikationsunternehmen kommt in diesem Kontext eine besondere Verantwortung zu. Als Betreiber der so wichtigen Telekommunikationsnetze haben sie die Vertraulichkeit und Sicherheit der ihnen übergebenen Daten zu garantieren. Weil es sich bei den Netzen um eine kritische Infrastruktur handelt, sind sie gemäß des kürzlich in Kraft getretenen IT-Sicherheitsgesetzes verpflichtet, die IT-Sicherheit nach dem Stand der Technik zu gewährleisten und Cyberangriffe zu melden.

Die Datenintegrität sicherzustellen, ist ein wichtiger Eckpfeiler, wenn es um die erfolgreiche Weiterentwicklung unserer Gesellschaft geht.

Die Risiken durch kompromittierte Daten sind jedoch erheblich. Nicht nur, dass vertrauliche Informationen in die falschen Hände geraten können. Vielmehr ist die Funktionalität automatisierter Prozesse innerhalb der Telekommunikationsnetze und damit auch innerhalb der Prozesse der Telekommunikationskunden gefährdet. Laut Analysen haben Unternehmen im Jahr 2015 durchschnittlich 146 Tage gebraucht, um einen sicherheitskritischen Vorfall zu erkennen. Die größte Herausforderung für Unternehmen besteht demnach darin, rechtzeitig zu wissen, dass ein Angriff stattgefunden hat.

SCHADENSBEGRENZENDE MASSNAHMEN IN ECHTZEIT EINLEITEN

Wie können Unternehmen sich selbst und ihre Kunden vor diesen realen Bedrohungen schützen? Bislang konzentrierten sich sämtliche Sicherheitsbestrebungen darauf, durch Verschlüsselung, Zugangskontrolle sowie Firewalls etwaige Zugriffe zu kontrollieren und Verstöße zu verhindern. Diese perimeterzentrische Vorgehensweise ist unvermindert wichtig, birgt jedoch zunehmend Probleme, so zum Beispiel stetig steigende Kosten und wachsende Komplexität bei der Authentifizierung. Auch schränkt diese Vorgehensweise den Zugriff auf die Daten und damit auf den Rohstoff der Zukunft in einer digitalisierten Wirtschaft ein. Daneben besteht weiterhin die Gefahr des beabsichtigten oder unbeabsichtigten Missbrauchs durch Insider.

Datenintegrität – also die Sicherstellung der Unversehrtheit von Daten und dadurch der korrekten Funktionsweise von Systemen – ist deshalb ein wichtiger Eckpfeiler, wenn es um die erfolgreiche Weiterentwicklung unserer Gesellschaft geht. Die Datenintegrität umfasst dabei Maßnahmen, um die unerlaubte Veränderung von geschützten Daten aufzudecken, zu analysieren und die Rückführung auf ihren Ursprungszustand zu gewährleisten. Zur Sicherung der Datenintegrität sind inzwischen Lösungen verfügbar, die mithilfe von Hash-Kryptographie, Blockchains und Calendar Time Stamps Integrität herstellen. Hierdurch werden zwar keine unberechtigten Handlungen direkt verhindert, allerdings ermöglicht es, das Eindringen von Angreifern direkt zu erkennen und damit scha-

densbegrenzende Maßnahmen in Echtzeit einleiten zu können.

SICHERHEIT UND DATENINTEGRITÄT GEHÖREN IN JEDE PRODUKTSTRATEGIE

Der DsiN-Cloud-Scout-Report 2015 hat die zunehmende Bedeutung von Datenintegrität im Zusammenhang mit Cloud-Computing sehr eindeutig herausgearbeitet. Die Bereiche, in denen Datenintegrität von entscheidender Bedeutung ist, sind vielfältig und reichen vom Schutz kritischer Infrastruktur bis hin zur Verifizierung von Software-Updates „over the air“, beispielsweise bei der mobilen Software-Aktualisierung von Fahrzeugen. In Zukunft wird es umso wichtiger sein, Sicherheit und Datenintegrität als unverzichtbare Bestandteile der Unternehmens- und Produktstrategie sowie bei der Entwicklung verbesserter Industrielösungen und der Implementierung von Industrie 4.0 mitzudenken.

In einer vernetzten Wirtschaft reicht es jedoch nicht mehr aus, lediglich die eigenen Daten zu schützen. Unternehmen müssen auch den Daten ihrer Partner vertrauen und sicherstellen können, dass deren Daten und Anwendungen nicht korrumpiert sind. Telekommunikationsunternehmen müssen diese Entwicklung aktiv gestalten und sollten deshalb auf ein hohes Maß an Datenintegrität bei all ihren Dienstleistungen achten, um die Kunden-Frage „Kann ich meinen Daten trauen?“ eindeutig bejahen zu können.

VERNETZTES FAHREN – ABER SICHER!

Mit einfachen Beispielen zeigt DsiN künftig neue Chancen der vernetzten Mobilität – und klärt über aktuelle Fragen der digitalen Sicherheit und des Datenverkehrs auf. Die Initiative steht unter der Schirmherrschaft des Bundesministeriums für Verkehr und digitale Infrastruktur. Kontakt unter:

mobilitaet@sicher-im-netz.de

www.10jahre.dsin.de

Im Bürgerforum zur IT-Sicherheit des DsiN-Jahreskongresses sprechen ENISA-Direktor Prof. Dr. Udo Helmbrecht und MdB Gerold Reichenbach mit dem Autor dieses Beitrags und weiteren Experten über IT-Sicherheit durch das Zusammenspiel von Regulierung, Technologien und Aufklärung.

Stefan Koetz
ist Vorsitzender der Geschäftsführung der Ericsson GmbH

Digitale Selbstverteidigung geht alle an

von Markus Beckedahl

Für viele ist das Internet quasi vom Himmel gefallen. Vor gerade einmal zehn Jahren wurden Smartphones eingeführt – zu einem Zeitpunkt, als nicht wenige noch daran glaubten oder zumindest hofften, dass das Internet als Trend wieder verschwinden würde und sie sich deshalb nicht damit auseinandersetzen müssten. Zehn Jahre später haben fast alle Netz, sei es in Form eines Smartphones oder von immer smarteren Fernsehern.

Jeder weitere eingebaute Computer erhöht aber die Komplexität für Fragen der Sicherheit und Privatsphäre, und oft wissen wir gar nichts darüber. Haben Sie eine Vorstellung davon, was Ihr Smartphone mit der Gesamtheit aller Apps gerade ohne Ihr Wissen nach draußen kommuniziert und ob jemand an Ihrem Mikrofon mitlauscht?

WIR HABEN KEINE AHNUNG, WER ZUGRIFF AUF UNSERE DATEN HAT

Finden Sie es auch praktisch, wenn eine Messenger-App einfach mal Ihr Adressbuch hochlädt und Ihnen anzeigt, wer von Ihren Kontakten bereits den Messenger nutzt? Der Anbieter empfiehlt das, und es ist bequem. Aber haben Sie jeden einzelnen Kontakt um Erlaubnis gefragt, ob Sie seine Kontaktdaten einfach mal dem jeweiligen Anbieter schenken dürfen? Viele wollen das nicht und werden vielleicht erst durch Ihre Unachtsamkeit enttarnt und ihrer Privatsphäre beraubt.

Laden Sie sich immer sofort die neuesten Updates für Betriebssystem, Browser oder Apps herunter, wenn die Meldung kommt – oder klicken Sie gerne auf demnächst, weil ein Neustart gerade nicht passt oder Sie einfach keine Lust

dazu haben? Und lädt Ihr neuer Fernseher oder Ihre intelligente Kaffeemaschine auch noch zwei Jahre nach Kauf neue Sicherheitsupdates automatisch herunter, oder wird der Hersteller aus der Verantwortung gelassen?

MILLIONENLECKS SIND KEINE SELTENHEIT

Keine Überraschung mehr sind die regelmäßigen Meldungen über Datenlecks bei großen Unternehmen. Oft geht es um dreistellige Millionenzahlen an kopierten Accounts, die dann häufig im Anschluss im Netz zu finden sind. Hinweise, dass man schnell die Passwörter ändern sollte, gibt es dann zwar viele. Aber mal ehrlich, wer ändert denn deshalb sein Passwort und merkt sich das neue? Passwortmanager wären hier hilfreich, wenn sie sichere Passwörter vorschlagen und sie sich auch noch merken. Aber wo werde ich darüber aufgeklärt, was ein Passwortmanager ist, und wer sagt mir, welche ihrer Anbieter empfehlenswert im Sinne von vertrauenswürdig sind?

WO BLEIBT DIE AUFKLÄRUNGSKAMPAGNE „GIB ÜBERWACHUNG KEINE CHANCE“?

Von klein auf bekommen wir beigebracht, wie wir uns im Straßenverkehr verhalten sollen. Zuerst von den Eltern, dann im Kindergarten und über die Schule bis zur Fahrschule. Aber wie man sich sicher im Netz verhält, wie man die eigene Privatsphäre in Zeiten kommerzieller und staatlicher Totalüberwachung schützt und auf keine Betrugsversuche reinfällt ist dann Eigenverantwortung. Gut für die, die mit Computern aufgewachsen sind und ein Verständnis dafür entwickelt haben oder einfach nur informierte Freunde besitzen bzw. auf Angebote zur Medienkompetenz in Bibliotheken oder Volkshochschulen zurückgreifen (können). Der Rest bleibt sich momentan selbst überlassen. Und wird damit nicht nur zum potenziellen Opfer, sondern auch zum Sicherheitsrisiko für alle anderen.

TRAINER FÜR INTERNETSICHERHEIT

Die Digitale Nachbarschaft von DsiN bietet ehrenamtlich Engagierten eine kostenlose Ausbildung zum Trainer für Internetsicherheit und Datenschutz. Auch Sicherheitsthemen für das Vereinsleben werden adressiert.

www.Digitale-Nachbarschaft.de

Medienkompetenz wollen alle. Aber wenn es konkret darum geht, dafür Töpfe in Haushalten zu schaffen, ist das Thema nicht mehr interessant genug. Das muss sich ändern. Denn Medienkompetenz bedeutet heute lebenslanges Lernen, weil technische Zyklen alle paar Jahre alles auf den Kopf stellen können. Daran konsequent erinnert zu werden und ständig an die jeweilige aktuelle Technik angepasste Lernmaterialien zur Verfügung zu haben, ist Aufgabe und Herausforderung unserer Gesellschaft. Die Arbeit mit offenen Bildungsmaterialien (kurz: OER, für Open Educational Resources) kann dabei helfen, Synergien zu nutzen. Zu oft kommt es heute noch vor, dass verschiedene Bildungsträger fast dieselben Aufklärungsmaterialien unabhängig voneinander entwickeln. Mehr Zusammenarbeit kann hier helfen, auf Vorhandenem aufzubauen und Neues zu generieren.

Vor allem müssen wir uns mehr anstrengen, um aktuelles Wissen rund um IT-Sicherheit und Eigenverantwortung in die Gesellschaft zu tragen. Nicht nur junge Menschen sollten hier primäre Zielgruppe sein, die bringen sich das notfalls auch alleine bei. Mehr Anstrengung brauchen wir bei der Weiterbildung von Lehrern und anderen Multiplikatoren. Und wer denkt an unsere Eltern? Als ich klein war, reagierte unsere Gesellschaft auf die Bedrohung durch Aids mit Aufklärungskampagnen zur Nutzung von Kondomen. Das war erfolgreich, um die Gefahr einzudämmen. Die Kampagnen laufen immer noch, weil ein ständiges Erinnern notwendig für ein starkes Bewusstsein ist, dass man mit Kondomen nicht nur sich selbst, sondern auch die jeweiligen Partner schützt. Wir brauchen vergleichbare Kampagnen mit einem langen Atem und ausreichend finanziellen Ressourcen zur Sensibilisierung über IT-Sicherheit. Wo bleiben die Aufklärungskampagnen „Gib Überwachung keine Chance – nutze Verschlüsselung“?

Markus Beckedahl ist Gründer und Chefredakteur von netzpolitik.org

Gemeinsamen Dialog fördern – Technologie, Regulierung, Aufklärung

Erst das Zusammenspiel von technologischer Innovation und Regulierungs- sowie Aufklärungsmaßnahmen für Verbraucher ermöglicht es, IT-Sicherheit herzustellen und aufrechtzuerhalten. Der gemeinsame Dialog fördert einander ergänzende Lösungen für digitalen Schutz und Vertrauen und vermeidet Insellösungen.

Nur gemeinsam können wir für IT-Sicherheit sorgen

von Sigmar Gabriel

Die Digitalisierung durchdringt schon heute fast alle Bereiche von Wirtschaft und Gesellschaft. Unbestritten sind die vielfältigen Chancen, die sich durch Informations- und Kommunikationstechnologien sowohl für jeden Einzelnen als auch für den Wirtschaftsstandort Deutschland insgesamt bieten. Die Digitalisierung ist jedoch auch mit Herausforderung verbunden. Das betrifft vor allem das Thema Sicherheit: Jedes Unternehmen – vom kleinen Betrieb über den Mittelständler bis hin zu Großkonzernen – muss sich die Frage stellen: „Wie sicher ist meine IT-Infrastruktur?“ Und: „Wie störanfällig ist sie?“

Technische Lösungen sind nur dann wirksam, wenn sie von Unternehmern und Verbrauchern umgesetzt und angewendet werden.

Eine Studie des Digitalverbands Bitkom e.V. liefert dazu interessante Hintergründe. So war jedes zweite Unternehmen in Deutschland in den vergangenen zwei Jahren bereits Opfer von digitaler Wirtschaftsspionage, Datendiebstahl oder Sabotage. Der daraus resultierende wirtschaftliche Gesamtschaden von jährlich 51 Milliarden Euro macht den Handlungsbedarf deutlich.

Die Etablierung eines umfassenden IT-Sicherheitskonzepts ist jedoch gerade für kleine und mittlere Unternehmen eine wirtschaftliche Hürde. So werden diese Unternehmen zu einem leichten Angriffsziel für Gefahren aus dem Netz. Und technische Lösungen sind auch nur dann wirksam, wenn sie von Verbrauchern und Unternehmern umgesetzt und angewendet werden.

Das bundesweite Projekt IT-Sicherheit@Mittelstand von Deutschland sicher im Netz gemeinsam mit dem Deutschen Industrie- und Handelskammertag (DIHK), für das ich gerne die Schirmherrschaft übernommen habe, unterstützt Unternehmen genau dabei: Es richtet sich explizit an Geschäftsführer und Entscheider in kleinen und mittelständischen Unternehmen und berät diese in IT-Sicherheitsfragen ihrer Unternehmen. Im Zentrum stehen hierbei Aufklärung, Befähigung und praktische Umsetzung von IT-Sicherheitsmaßnahmen.

Denn wir wollen gemeinsam das Internet so sicher wie möglich gestalten. Schließlich schafft Sicherheit das Vertrauen, das die Grundvoraussetzung für wirtschaftlichen Erfolg ist. Dazu wollen wir einen offenen Dialog zwischen Wirtschaft, Wissenschaft, Politik und Verbänden führen und unsere Zusammenarbeit vertiefen.

Ein wichtiges Forum dafür ist der jährliche nationale IT-Gipfel der Bundesregierung unter Koordinierung des Bundesministeriums für Wirtschaft und Energie (BMWi). Vor zehn Jahren wurde hier die Gründung des gemeinnützigen Vereins Deutschland sicher im Netz beschlossen.

Ein gutes Beispiel für den IT-Sicherheitsrahmen sind Aufklärungen von Unternehmensmitarbeitern wie das von Deutschland sicher im Netz durchgeführte Projekt „Bottom-Up“. Es richtet sich gezielt an Berufsschüler und wird durch das BMWi gefördert.

Lassen Sie uns in diesem Sinne zusammen die IT-Sicherheit in der deutschen Wirtschaft weiter nachhaltig verbessern!

MITTELSTAND FIT MACHEN FÜR IT-SICHERHEIT

DsiN und DIHK haben 2015 unter der Schirmherrschaft des Bundeswirtschaftsministers die Workshopreihe IT-Sicherheit@Mittelstand ins Leben gerufen. Entscheider in kleinen und mittleren Unternehmen erfahren in Vorträgen in ihren IHKs, was sie für mehr Sicherheit in ihrem Betrieb konkret unternehmen können. Ziel ist die Vermittlung von „Hilfe zur Selbsthilfe“.

www.dsin.de/it-sicherheit-mittelstand

www.10jahre.dsin.de

Auf dem Bürgerforum zur IT-Sicherheit des DsiN-Jahreskongresses erläutert Staatssekretär Matthias Machnig (BMWi) das Zusammenwirken von Regulierung, Technologie und Aufklärungsarbeit für mehr IT-Sicherheit.

Sigmar Gabriel
ist Bundesminister für Wirtschaft und Energie

Nicht ohne meine IT-Sicherheit

Sicherheitsaspekte in der Ausbildung stärken

von Daniela Strobel

Anstoß für die Idee zur Gründung von it-sa Benefiz war – wie so oft – ein kleines Problem, für das eine große Lösung gesucht wurde. Ein studentischer Admin des SecuMedia Verlags brauchte für seine Diplomarbeit eine Firma, die ihm die Chance gab, eine neue Idee für mehr IT-Sicherheit in ihrem Betrieb zu testen. Unter den Ausstellern der IT-Security-Fachmesse it-sa, die der Verlag damals erstmals in Nürnberg veranstaltete, fand sich rasch ein Unternehmen, das dazu bereit war. Inzwischen ist der ehemalige Student in dieser Firma angestellt und macht dort Karriere. Was einmal funktioniert hat, sollte auch öfter möglich sein: Darum wurde der Verein it-sa Benefiz zunächst als Vermittlungsstelle zwischen Unternehmen und Berufsanfängern gegründet. Er sollte vor allem den Nachwuchs im Berufsfeld IT-Sicherheit fördern.

Das ist inzwischen nötiger denn je. Denn mit der fortschreitenden Digitalisierung potenziert sich der Bedarf an Spezialisten, um Bedrohungen wie Hacking, Spionage, Ransomware und Sabotage abzuwehren. 68,5 Prozent aller Unternehmen erwarten nach einer Studie des Sicherheitsanbieters Kaspersky, dass die Anzahl der Mitarbeiter, die sich ausschließlich IT-Sicherheitsfragen widmen, steigen wird. Doch gerade im Bereich der IT-Sicherheit mangelt es eklatant an Fachkräften. Die Rechnung dafür zahlen die Unternehmen: Denn wer keine IT-Experten findet, muss mitunter Unsummen für die Bewältigung von Cybersicherheitsvorfällen ausgeben. Vom Fachkräftemangel betroffene Firmen sind daher oft bereit, höhere Gehälter für immer weniger verfügbares Personal am Markt zu zahlen.

STUDIERENDE TREFFEN AUF IT-SICHERHEIT

Immer noch können Studierende der Informatik und angrenzender Studienfächer ihren Studiengang abschließen, ohne sich jemals mit Fragen der IT-Sicherheit zu befassen. DsiN macht sich daher für eine Behandlung des Themas in der Ausbildung stark – und lädt immer im Oktober gemeinsam mit it-sa Benefiz Studierende zum kurzweiligen Austausch mit Sicherheitsunternehmen ein.

www.dsin.de/messecampus

Wie also kann dem Mangel abgeholfen werden? IT-Sicherheit wird an immer mehr Hochschulen gelehrt – diese Studienangebote gilt es weiter auszubauen. Genauso wichtig ist es, die Studierenden zu motivieren, IT-Sicherheit nicht nur als Beiwerk für andere Informatikberufe zu betrachten, sondern sie mehr als bisher ins Zentrum ihrer Studien und ihrer beruflichen Pläne zu stellen.

> Mit der fortschreitenden Digitalisierung potenziert sich der Bedarf an Spezialisten, um Bedrohungen und Sabotage abzuwehren.

Durch verpflichtende Praktika könnten Studierende Erfahrungen im IT-Sicherheitsbereich machen, sehen, welch große Relevanz das Thema hat, und sich Berufsperspektiven eröffnen. Unternehmen sollten ihnen diese Möglichkeit bieten – und könnten so potenzielle Mitarbeiter kennen lernen und bei Interesse frühzeitig an sich binden.

Die Bereitschaft der jungen Informatiker ist da: Über 60 Prozent der Studierenden wünschten sich schon vor Jahren mehr Lehrveranstaltungsangebote zum Thema IT-Sicherheit. Zu diesem Resultat kam eine von Deutschland sicher im Netz e.V. (DsiN) bereits 2009 initiierte Studie. DsiN und it-sa Benefiz e.V. nahmen dies zum Anlass, Studierende der Informatik auf die damals noch neue Sicherheitsmesse it-sa in Nürnberg einzuladen: Seitdem kommen – 2016 nun schon zum achten Mal – Omnibusse aus allen Teilen Deutschlands mit Studenten und Professoren zum DsiN-Messe-Campus auf die it-sa, um einen Eindruck von der Faszination des Themas Sicherheit zu erhalten, vor allem aber, um anschließend Gesprächstermine bei Ausstellern wahrzunehmen und Kontakte für Praktika und Karrieren zu knüpfen. Denn nicht nur jede Firma und jede Behörde braucht Cyber-Security-Experten. Die hierauf spezialisierten Unternehmen suchen ebenfalls händeringend qualifizierte Mitarbeiter. Um diesen Bedarf zu decken – auch das eine Erkenntnis des DsiN-MesseCampus –, sind mehr Hochschulangebote und spezialisierte Studiengänge unverzichtbar.

Daniela Strobel
ist Vorstandsvorsitzende von it-sa Benefiz e.V.

Demokratische Spielregeln im Netz?

von Maik Pogoda

Derzeit nutzen 2,58 Milliarden Menschen das Internet und auf diesem basierende Applikationen und Services – und voraussichtlich werden es im Jahr 2019 sogar 3,22 Milliarden Menschen sein. Täglich tauschen sie hier Informationen aus, private ebenso wie geschäftliche. Aber können alle Internetnutzer annehmen, dass diese ausgetauschten Informationen sicher und vor dem Zugriff Unberechtigter geschützt sind und also nicht missbraucht werden? Und können wir weiterhin davon ausgehen, dass in demokratischen Strukturen bei der Nutzung des Internets ähnliche Prinzipien, Mechanismen und Strukturen zugrunde gelegt werden, wie sie den Bürgerinnen und Bürgern in Verfassungen und Grundgesetzen verbrieft werden? Und welche Verantwortung tragen wir – als Verbraucher oder Anbieter – bei der Nutzung des Internets?

DSINSIGHTS-BREAKFAST

Ein guter Start in den Arbeitstag beginnt mit Nahrung für Kopf und Magen – einmal im Jahr lädt DsiN Entscheidungsträger aus Politik, Wirtschaft und Gesellschaft zu einem Informationsfrühstück zum Thema IT-Sicherheit ein. Im Mittelpunkt stehen dabei konkrete Sicherheitstipps zu Schutzmaßnahmen im Büro, wie beispielsweise dem einfachen Verschlüsseln von E-Mails.

Jetzt anmelden unter: www.dsin.de

Orientieren wir uns an dem in Deutschland geltenden Grundgesetz, Artikel 20, und den darin getroffenen Festlegungen zur Gewaltenteilung. Erstmals von Aristoteles und Polybios aufgeworfen, von John Locke benannt und von Montesquieu in heutiger Form formuliert, besteht der Sinn der Gewaltenteilung darin, die Staatsgewalt auf mehrere Staatsorgane zum Zweck der Machtbegrenzung und der Sicherung von Freiheit und Gleichheit zu verteilen, auf Legislative, Exekutive und Judikative. Die Legislative, die gesetzgebende Gewalt, beschließt die Gesetze; die Exekutive, die vollziehende Gewalt, führt die Gesetze aus, und die Judikative, die rechtsprechende Gewalt, überwacht die Einhaltung der geltenden Gesetze. Die einzelnen Säulen der Gewaltenteilung sind aufeinander angewiesen und können ihre Macht nicht allein ausüben. Das Prinzip der Gewaltenteilung wird als wesentlicher und unverzichtbarer Bestandteil einer Demokratie angesehen. So wesentlich und unverzichtbar, dass man es heutzutage in den meisten Verfassungstexten wiederfindet.

> Technologien zum Schutz der digitalen Identität und Souveränität sind bereits heute vorhanden.

Es stellt sich die Frage, ob in einem die Grenzen und Kontinente überschreitenden globalen Netz nicht ähnliche Prinzipien und Mechanismen angewendet werden sollten oder müssen, insbesondere wenn die Nutzung des Internets nahezu alle Bereiche des Lebens durchdringt und als Basis für die vierte Industrielle Revolution angesehen wird. Wenn ja, wer bildet in diesem globalen Netzwerk Legislative, Exekutive und Judikative? Wer erlässt entsprechende, für alle Nutzer des Internets verbindliche Gesetze, wer vollzieht und wer überwacht sie? Was sollte der Anspruch an die entsprechenden Gesetze sein, welche Prinzipien, Werte und Normen werden diesen zugrunde gelegt? Wer entscheidet über die Aufnahme und gegenseitige Anerkennung dieser Prinzipien, Normen und Werte – oder brauchen wir diese Prinzipien im Internet nicht?

Technologien zum Schutz der digitalen Identität und Souveränität sind bereits heute vorhanden und werden ständig weiterentwickelt und verbessert. Jeder Nutzer kann selbst und frei entscheiden, welche Technologien respektive Applikationen er zum Schutz seiner Identität und seiner Daten im Netz verwendet. Doch welche Kriterien spielen bei der Entscheidung eine Rolle? Welche kulturellen, sozialen oder soziologischen Eigenarten gilt es zu berücksichtigen? Wie kommt es beispielsweise, dass die Bürgerinnen und Bürger in einem europäischen Land hinnehmen, bis zu 30-mal am Tag mit Videokameras aufgenommen zu werden, jedoch kein elektronisches Ausweisdokument – den elektronischen Reisepass ausgenommen – akzeptieren wollen? Und warum gibt es bis heute Banknoten, obgleich nahezu überall elektronische Zahlungsmittel verfügbar sind?

Die Beantwortung dieser Fragen wird vermutlich unterschiedlich ausfallen, je nachdem, welche Kriterien berücksichtigt wurden. Aber so verschieden die Antworten auf diese Fragen auch lauten mögen: Der Schutz der Identität und Souveränität – auch und insbesondere in der digitalen Welt – ist ein hohes Gut, gerade in einer Demokratie wie der unseren.

Maik Pogoda
ist Geschäftsführer des IT-Unternehmens OpenLimit SignCubes GmbH

Digitalisierung geht alle an

Aufklärungsarbeit als unabdingbare Voraussetzung erfolgreicher digitaler Transformation

von Prof. Dieter Kempf

Will man sich im Internet durch Eingabe des Suchbegriffs „Digitale Transformation“ über das Thema informieren, so erhält man aktuell 12,4 Millionen Ergebnisse. Gibt man z. B. „Industrie 4.0“ ein, sind es gar 18,5 Millionen. Selbst wenn man unterstellt, dass einige dieser Ergebnisse letztendlich auf die gleiche Fundstelle verweisen, und man natürlich die beiden Suchergebnisse nicht additiv werten darf, so erklärt sich hieraus nur unzulänglich, weshalb zu diesem Themenkreis weitere Aufklärungsarbeit notwendig erscheint.

Dass der Titel dieses Beitrags dennoch seine Berechtigung hat, wird deutlicher, wenn man z. B. das Ergebnis einer Umfrage der Bitkom Research vom Frühjahr 2016 zur Digitalisierung zu Rate zieht. So gehen etwa 64 Prozent der befragten Unternehmen davon aus, dass sich durch Digitalisierung ihr Geschäftsmodell verändert, wobei sich lediglich 27 Prozent als Vorreiter einer derartigen Digitalisierung sehen. 59 Prozent sehen sich eher als Nachzügler und 7 Prozent antworten selbstkritisch, sie hätten den Anschluss an die Digitalisierung verpasst. Für 72 Prozent der befragten Unternehmen liegt in der Digitalisierung des eigenen Unternehmens die zweitwichtigste Herausforderung nach der Fachkräftesicherung.

KEINER ENTKOMMT DER DIGITALISIERUNG

Damit ist längst klar, dass der Begriff „Industrie 4.0“, der stellvertretend für die Digitalisierungseffekte im Bereich der Industrie und der industrienahen Dienstleistungen verwendet wurde, gerade eben nicht bedeutet, dass sich digitale Transformation nur im industrienahen Bereich abspielen wird. Je häufiger digitale Plattformen aus bisherigen Wertschöpfungsketten neuartige Wertschöpfungsnetze bilden, umso mehr werden Unternehmen aller Größen und Branchen, egal ob Industrie, Handwerk oder Freie Berufe, von den unterschiedlichen Facetten der Digitalisierung erfasst werden.

Damit kommt dem Aufbau von Digitalkompetenz bei Mitarbeitern eine erhebliche Bedeutung zu. Bereits jetzt beklagen Unternehmen unterschiedlichster Branchen, dass sie Probleme haben, ausreichend IT-Fachkräfte zu finden. In einer internationalen Vergleichsstudie, in der computer- und informationsbezogene Kompetenzen von zwölf- und dreizehnjährigen Schülerinnen und Schülern aus weltweit 21 Bildungssystemen miteinander verglichen wurden, belegten deutsche Teilnehmer lediglich einen Mittelplatz. Der Aufbau von Digitalkompetenz ist mithin nicht nur die Aufgabe jener Unternehmen, die unmittelbar vor digitalen Herausforderungen stehen. Sie ist vielmehr eine Gemeinschaftsaufgabe von Staat, Unternehmen und individuellen Nutzern.

IT-WISSEN RAUS AUS DER NISCHE

Betrachtet man einen Teilbereich digitaler Kompetenz, nämlich das Wissen um IT-Sicherheitsthemen – genauer: das Wissen um IT-Sicherheit in den Bereichen Sicherheit des IT-Betriebes, Sicherheit digitaler Daten und Schutz personenbezogener Daten –, so wird das Ergebnis eher noch schlechter. Nach einer Untersuchung des Comma Security Institutes aus dem Jahr 2015 war lediglich an 17 von 64 Hochschulen ein Lehrstuhl oder eine auf IT-Sicherheit spezialisierte Professur eingerichtet und nur an fünf Hochschulen gab es spezialisierte Studiengänge für IT- und Cybersicherheit.

In einer immer stärker vernetzten Gesellschaft ist aber gerade der sichere Betrieb digitaler Systeme unabdingbar. Denn wie verwundbar schlecht geschützte Systeme sind, hat nicht zuletzt der „Erfolg“ des Locky-Virus in der ersten Jahreshälfte 2016 gezeigt, dem unter anderem auch Krankenhäuser zum Opfer fielen. Was aktuell offenbar nur die Verwaltungssysteme von Krankenhäusern betroffen hat, mag man sich bei telemedizinischen Anwendungen als Fehlerquelle sicherlich gar nicht erst vorstellen.

Das Wissen um IT-Sicherheit darf jedoch nicht nur eine Art „Vorbehaltsaufgabe“ von Spezialisten sein. Die Durchdringung unseres Alltags mit unterschiedlichsten Formen der Nutzung von IT und elektronischer Kommunikation macht es unabdingbar, dass auch jeder Nutzer über Basiswissen auf diesem Gebiet verfügt. Aufklärungsarbeit ist also angesagt! Der Verein Deutschland sicher im Netz hat sich genau diese Aufklärung seit seiner Gründung im Jahr 2006 zur Kernaufgabe gemacht. Dabei reichen die Aktivitäten von der Anleitung der Verbraucher bei der Gestaltung eines sicheren Passwortes über Hinweise zur vertraulichen E-Mail-Kommunikation bis zu aktuellen Meldungen der Sicherheitsbarometer-App (SiBa) über Risiken und Bedrohungen im Netz.

Eine erfolgreiche Transformation in die digitale Welt der Zukunft wird nur gelingen, wenn wir gemeinsam an der Aufgabe arbeiten, alle Wirtschaftsteilnehmer auf diese Veränderungen vorzubereiten. Dabei gilt es durch Aufklärung die Voraussetzungen für jeden Einzelnen zu schaffen, selbstbestimmt über seine Nutzung neuer Technologien zu entscheiden und selbstbewusst aus dem Angebot leistungsfähiger und vertrauenswürdiger Partner zu wählen. Auch das ist digitale Souveränität!

Prof. Dieter Kempf
war langjähriger Vorstandsvorsitzender von DsiN, Präsident des Branchenverbands Bitkom sowie Vorstandsvorsitzender der DATEV eG und ist als nächster Präsident des BDI nominiert

Gemeinsam überzeugen: Aufklärung durch Zusammenarbeit

von Arne Schönbohm

Kaum ein Bereich des Lebens kommt heutzutage ohne zuverlässige und sichere Kommunikationssysteme aus. Sie sind essenziell für eine funktionierende Wirtschaft und für viele weitere Bereiche unserer eng vernetzten Gesellschaft. Sie schaffen die Voraussetzung für Mobilität, Datenaustausch sowie Kapital-, Waren- und Dienstleistungstransfer. Sie ermöglichen das einfache Telefonieren und lassen uns via Kurznachrichtendienste, soziale Netzwerke oder Instant-Messenger miteinander in Verbindung treten. Sie sorgen aber auch für die Vernetzung von medizinischen Geräten in einem Operationssaal und sind Voraussetzung für die Industrie 4.0 sowie für die Energiewende oder den Betrieb von kritischen Infrastrukturen. Mit der immer stärkeren Verbreitung von Kommunikationssystemen entstehen dabei immer auch neue Abhängigkeiten des Menschen von der einwandfreien Funktionsfähigkeit der Systeme.

UNSER EMPFINDLICHES DIGITALES NERVENSYSTEM

Durch Kommunikationssysteme intelligent vernetzte Wertschöpfungsketten ermöglichen systemische, energie- und ressourcenschonende Produktionsprozesse und neue Lösungen für Mobilität und Logistik. Die Dynamik der Digitalisierung im Produktions- und Dienstleistungssektor ist weiterhin ungebrochen: Bis zum Jahr 2018 werden weltweit voraussichtlich allein 1,3 Millionen Industrieroboter miteinanderkommunizieren und kooperieren. Im Internet der Dinge werden bis 2020 schätzungsweise 50 Milliarden Endgeräte interagieren. Leistungsfähige und sichere Kommunikationssysteme entwickeln sich daher immer mehr zum zentralen Nervensystem für Anwendungsfelder wie Industrie 4.0, Telemedizin und autonomes Fahren.

> Bis zum Jahr 2018 werden weltweit voraussichtlich allein 1,3 Millionen Industrieroboter miteinander kommunizieren und kooperieren.

Gleichzeitig nimmt aber auch die Bedrohung durch Sicherheitslücken in diesen Systemen zu. Die Zahl der IT-Angriffe durch Kriminelle, Spione und Terroristen steigt von Jahr zu Jahr. Die Angriffe werden immer professioneller. Kriminelle Dienstleistungen können immer häufiger über das Internet bezogen werden. IT-Sicherheit ist damit eines der integralen Themen der Informations- und Telekommunikationstechnologie (ITK) geworden. Nicht nur für den Staat und die Wirtschaft, sondern auch und insbesondere für den einzelnen Bürger.

> Während es eine gesellschaftliche Aufgabe früherer Jahrzehnte war, Medienkompetenz zu vermitteln, ist es die vorrangige Aufgabe unserer Zeit, IT-Sicherheitskompetenz zu vermitteln.

NACHHOLBEDARF IN SACHEN DATENSCHUTZ

Mit zunehmender Digitalisierung und Vernetzung unserer Gesellschaft bekommen Aspekte wie Datenschutz und Privacy im Internet eine immer größere Bedeutung. Während es eine gesellschaftliche Aufgabe früherer Jahrzehnte war, Medienkompetenz zu vermitteln, ist es die vorrangige Aufgabe unserer Zeit, IT-Sicherheitskompetenz zu vermitteln. In allen Bereichen und auf allen Ebenen, für alle Altersgruppen und Nutzerprofile. Zahlreiche Aktivitäten geschehen inzwischen online und sowohl berufliche als auch private Kommunikation findet in großem Umfang in digitalen Räumen statt. Viele Menschen nutzen soziale Netzwerke und geben dabei so viele personenbezogene Informationen preis wie nie zuvor. Der Schutz ihrer Daten bestätigt sich somit zunehmend als ein zentrales demokratisches Gut.

Bürgerinnen und Bürger müssen in die Lage versetzt werden, selbstbestimmt und sicher in der digitalen Welt zu agieren und ihre Persönlichkeitsrechte effektiv zu schützen. Sie müssen entsprechende Kompetenzen entwickeln – und ihnen müssen entsprechende Angebote gemacht werden. Nicht zuletzt, weil die „digitale Sorglosigkeit“ ein immer noch weit verbreitetes Phänomen ist. Der Einsatz von Virenscannern und die Installation einer Personal Firewall sind bei Privatnutzern noch nicht in zufriedenstellendem Maße verbreitet, und auch Sicherheitsupdates für das Betriebssystem oder die genutzten Anwenderprogramme werden unregelmäßig eingespielt. Weniger als die Hälfte der privaten Internetuser nutzen dafür die automatischen Update-Funktionen der Betriebssysteme und Anwendungen.

DIE ALLIANZ FÜR CYBER-SICHERHEIT

Diese umfassende „Anleitung zur Prävention“ kann nicht nur eine Aufgabe staatlicher Instanzen sein, sie verlangt ein Zusammenwirken aller Akteure. Mit der Allianz für Cyber-Sicherheit (www.allianz-fuer-cybersicherheit.de), die 2012 mit dem ITK-Branchenverband

Bitkom initiiert wurde, verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland, insbesondere der kleinen und mittelständischen Unternehmen (KMU), gegenüber Cyberangriffen zu stärken. Dies erfolgt unter anderem durch die Bereitstellung praktikabler IT-Sicherheitsempfehlungen für KMU durch das BSI und durch Partner der Allianz. Der Allianz gehören inzwischen mehr als 1.800 Institutionen an, davon knapp 100 Partnerunternehmen und mehr als 40 Multiplikatoren. Hinzu kommt eine intensive Kooperation mit der Wissenschaft. Und damit auch die Bürger die Chancen des Internet sicher nutzen können, hat das BSI mit „BSI für Bürger“(www.bsi-fuer-buerger.de; https://twitter.com/bsi; www.facebook.com/bsi.fuer.buerger) ein entsprechendes Informationsangebot aufgebaut, das sich speziell an Privatanwender richtet, die sich in der vernetzten Welt sicher bewegen wollen. Neben der reinen Information zu unterschiedlichsten IT-Sicherheitsthemen bietet das BSI dort auch konkrete Handlungsempfehlungen etwa zur Verschlüsselung an.

SICHERHEITSKONZEPTE FÜR ALLE BÜRGERINNEN UND BÜRGER

Mit dem Verein Deutschland sicher im Netz steht dem BSI ein weiterer wichtiger Kooperationspartner mit sehr guter Vernetzung und einem umfassenden Sicherheitsverständnis zur Verfügung. Das BSI und DsiN richten sich mit ihren Angeboten an Bürgerinnen und Bürger, Wirtschaft sowie Verwaltung und stellen Hilfsmittel bereit, die speziell auf diese Zielgruppen zugeschnitten sind und ihnen helfen, sich mit der Problematik IT-Sicherheit auseinanderzusetzen. Beide möchten Internetnutzer nicht nur informieren, sensibilisieren und aufklären, sondern auch Schutzmaßnahmen etablieren.

Damit zeigen DsiN und BSI gemeinsam sehr konkret und praktisch, wie eine enge Kooperation der mit IT-Sicherheit befassten Institutionen ermöglicht, das Thema mit all seinen unterschiedlichen Aspekten an unterschiedlichste Zielgruppen kompetent zu adressieren. Als nationale Cyber-Sicherheitsbehörde hat das BSI die Aufgabe, die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft zu gestalten. Mit dem kooperativen Ansatz und zusammen mit der Public-Private-Partnership Deutschland sicher im Netz ist hierzu eine wesentliche Grundlage geschaffen.

www.10jahre.dsin.de

Die Ergebnisse aus den Bürgerforen des DsiN-Jahreskongresses – von Verbraucherbildung und IT-Sicherheitsdialog bis Wirtschaftsinnovationen – finden Sie eindrücklich hier zusammengefasst.

Arne Schönbohm
ist Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und im Beirat von Deutschland sicher im Netz e.V.

IT Security Awareness Raising – a Pan-European Challenge

von Prof. Dr. Udo Helmbrecht

The world is quickly embracing digital in every part of life. E-banking, e-health, e-commerce, e-education, e-everything are all now totally dependent on an open, safe and secure cyberspace. We are witnessing the development and deployment of smart manufacturing, the Internet of Things and computer controlled critical infrastructure. Digital is challenging the delivery of old business models, while at the same time providing opportunities for the new world. We see new challenges to old business models, where for example mobile phone manufacturers and internet search engine companies are moving into smart transport. Europe has to embrace this challenge and take the lead in the digital revolution by delivering disruptive business models, using innovative technologies and services in a safe and secure manner. Europe has to ensure the trust of its citizens and industry to have the necessary confidence to work digital.

> Europe has to ensure the trust of its citizens and industry to have the necessary confidence to work with digital.

At the same time trust in online services makes it a necessity to preserve the secrecy and integrity of electronic communication. It goes well beyond individuals' rights: In a society that is ever more depending on the correct functioning of electronic communication services, technical protection of these services is mandatory, since otherwise criminals will abuse vulnerable services. From a technical standpoint, both confidentiality and integrity may be fulfilled by the same cryptographic mechanisms.

TURN USERS INTO GUARDIANS

Also, more and more citizens and businesses are likely to suffer security breaches. This is due to vulnerabilities in these new and exist-

ing technologies, the move towards 'always on' connections and the continuous and exponential user uptake within Member States. Such security breaches may be IT related, for example through computer viruses or other malicious software, system failure or data corruption, or they may be socially motivated, for example through theft of assets or other incidents caused by staff. It is indicative that all industry sectors have experienced staff-related breaches, though technology companies fared better than most.

In an age ever more reliant on digital information, there is an increasing number of technological weaknesses that can be exploited. Recent incidents have highlighted that a considerable number of endusers are unaware of their exposure to security risks. Given the rising level of breaches seen recently, it is more critical than ever that organizations raise security awareness by turning users into a first line of defense. A significant step towards this is to prepare user posture in cyberspace by disseminating information about the current state of the cyber-threat landscape.

> By promoting education, sharing of good practices and competitions such as the European Cyber Security Challenge, the EU seeks to raise awareness of cyber security among its citizens.

A JOINT EU ADVOCACY CAMPAIGN

The European Cyber Security Month (ECSM) is an EU advocacy campaign that seeks to raise awareness of cyber security among citizens and advocates for changing the behavior of citizens towards cyber-threats by promoting education, sharing of good practices and competitions such as the European Cyber Security Challenge. The European Union Agency for Network and Information Security (ENISA), the European Commission's DG Connect and partners have been deploying the ECSM each October for the last five years.

The Digital Agenda for Europe (DAE), adopted in May 2010, and the related Council conclusions highlighted the shared understanding that trust and security are fundamental preconditions for the wide uptake of information and communications technology (ICT) and therefore for achieving the objectives of the 'smart growth' dimension of the Europe 2020 strategy. The DAE emphasized the need for all stakeholders to join forces in a holistic effort to ensure the security and resilience of ICT infrastructures by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks and cyber-crime.

The ECSM was also foreseen in the EU-US summit final report and in the roadmap produced by the awareness-raising sub-group of the EU–US Working Group on Cyber-Security and Cyber-Crime in December 2011. DsiN (Deutschland sicher im Netz e.V.) is a strong partner implementing the ECSM campaign in Germany alongside the Federal Office for Information Security (BSI).

The campaign concentrates on building together a joint EU advocacy campaign across Member States so as to generate broad awareness about cyber security, which is one of the priorities identified in the EU Cyber Security Strategy, as well as to promote the safer use of the internet for all users and increase the national media interest through the European and global dimension of the project. The campaign includes both the general public, acting as 'EU digital citizens', and specific groups focused on Member States' stakeholders from public and private organizations e.g. IT experts, NIS authorities and educational institutions. Over the course of the month of October, a range of local activities and events are held across Europe to raise the security awareness of specific target groups. These include, among others: workshops, conferences, social media campaigns, quizzes and roadshows.

HIGH LEVEL OF INVOLVEMENT

The main contact point to the Member States is through the National Liaison Officers (NLO) network, partners from public and private organizations, and networks of multipliers. The European Commission, other EU bodies such as the European Economic and Social Committee and Agencies continue to get involved and maintain their participation at a high level. The campaign creates a good environment for European but also international cooperation for cyber security public-private partnerships.

The community building process around the campaign is an important win. An example of international impact is the DsiN-Cloud-Scout initiative. Cloud-Scout is an online tool which provides European small and medium enterprises with tailored information and recommendations on their use of cloud services.

CLOUD-SCOUT FÜR MITTELSTÄNDLER – EUROPAWEIT

Grundwissen im sicheren Umgang mit der Cloud ist Voraussetzung für ihre sichere Anwendung – von der Einführung bis zum Betrieb und möglichen Migration auf einen anderen Anbieter. Der DsiN-Cloud-Scout wurde 2014 für alle Anwender in Europa in acht Landessprachen verfügbar gemacht; im Cloud-Scout-Report werden landestypische Gewohnheiten sichtbar:

cloudscout.cloudwatchhub.eu

Prof. Dr. Udo Helmbrecht
ist Geschäftsführender Direktor der ENISA – Europäische Agentur für Netz- und Informationssicherheit und im Beirat von Deutschland sicher im Netz e.V.

Digitalisierung als Pfad in die zukünftige Gesellschaft

von Susanne Dehmel

Wir leben in einer Zeit, in der unsere kühnsten Kindheitsträume bereits Realität geworden sind. Mehr noch: Unsere Phantasie reicht oft nicht aus, um die technischen Innovationen und Fortschritte der Digitalisierung auch nur innerhalb weniger Jahre vorauszusagen: Die Verknüpfung der realen Welt mit virtuellen Welten, Lieferdrohnen, die im Garten Bücher abstellen, selbstfahrende Autos, ein Blutdruckmessgerät, welches die Werte gleich dem Arzt vorlegt, stromproduzierende Dachschindeln, smarte Städte, der Ausdruck von Ersatzteilen – einfach aus dem eigenen (3D-)Drucker. Dies sind nur ein paar von vielen Beispielen dafür, wie sehr unser Alltag von der Digitalisierung durchdrungen ist, ja sogar erst durch sie ermöglicht wird.

Je mehr wir die Vorzüge unseres digitalen Lebens genießen, desto mehr wird uns bewusst, wie abhängig wir von einer Vielzahl von Technologien und Infrastrukturen sind. Die Informationstechnologie ist als weltumspannendes Netz schon längst zur Achillesferse unseres Lebensstandards geworden. Nur die sichere Anwendung und sichere Nutzung der zur Verfügung stehenden Dienste und Geräte schafft Akzeptanz bei den Verbrauchern und bieten diesen einen verlässlichen Mehrwert.

> Nur die sichere Anwendung und sichere Nutzung der zur Verfügung stehenden Dienste schafft Akzeptanz.

Um Nutzen und Risiken der Digitalisierung auszubalancieren, bedarf es eines dynamischen Prozesses, der die täglich neuen Änderungen in den Technologien und in der Gesellschaft berücksichtigt. Hersteller, Systemarchitekten und Betreiber müssen bereit sein, Datensicherheit und Datenschutz bei der digitalen Transformation stets mitzudenken. Der Branchenverband der deutschen Informations- und Telekommunikationsindustrie Bitkom setzt sich mit einer Vielzahl von Publikationen und Studien dafür ein, das Bewusstsein für IT-Sicherheit in Unternehmen, in der Politik und Öffentlichkeit zu schärfen. Wir sind davon überzeugt, dass vor dem Hintergrund der sich ständig verändernden Risikolage und immer wieder neu entstehender Bedrohungen nur ein zielgerichtetes, gemeinsames und abgestimmtes Vorgehen zur Etablierung hoher Sicherheitsniveaus erfolgreich sein kann. Dafür bedarf es des Dialogs aller Beteiligten aus Politik, Wirtschaft und Gesellschaft.

Auf der anderen Seite muss auch der Anwender in der Lage sein, die Vorzüge der Digitalisierung sicher und selbstbestimmt nutzen zu können. Hier ist Bildung und Aufklärung ein wesentlicher Faktor für nachhaltige IT-Sicherheit. Dabei geht es nicht darum, jeden Bürger zu einem Informatikstudium zu verpflichten, sondern niedrigschwellige Informationsangebote zu schaffen und Hilfe zur Selbsthilfe anzubieten, wo es nötig ist. Der von Bitkom mitgegründete Verein Deutschland sicher im Netz leistet genau an dieser Stelle einen wertvollen Beitrag und ist ein wichtiger Partner, der die Verbandsaktivitäten mit Blick auf die Verbraucher ergänzt. Neben der Vielzahl von Projekten, die wir seit vielen Jahren gerne unterstützen, bildet auch der jährlich veranstaltete Kongress eine Plattform, die Kommunikation, Austausch und Begegnung – ganz physisch und real, aber digital begleitet – ermöglicht.

Wie wird sich die Digitalisierung innerhalb der nächsten zehn Jahre entwickeln? Welche Erfordernisse stellen sich, um die IT-Sicherheit auch in der neuen Dekade zu gewährleisten? Antworten auf diese Fragen lassen sich heute nur erahnen und schon jetzt wissen wir: Auch das Entwicklungstempo der Digitalisierung in den kommenden Jahren wird wieder unsere Vorstellungskraft überschreiten. Klar aber ist: Wir werden uns – gemeinsam mit DsiN – weiterhin tatkräftig engagieren, um den für das Vertrauen in die Digitalisierung notwendigen Dialog zwischen allen Beteiligten weiter zu führen und zu fördern.

HUB CONFERENCE

Die hub conference ist die zentrale deutschsprachige Digitalkonferenz mit internationalem Publikum. Jedes Jahr treffen hier Global Player und Start-ups, CEOs, Wissenschaftler und Politiker zusammen und diskutieren aktuelle Trends im Netz.

Die nächste hub conference in Partnerschaft mit DsiN findet am 22.11.2016 in Berlin statt:

www.hub.berlin

www.10jahre.dsin.de

Hier finden Sie das Grußwort von Bitkom-Präsident Thorsten Dirks zum 10-jährigen DsiN-Jubiläum sowie die Jubiläumsrede auf dem Kongress.

Susanne Dehmel
ist Miglied der Geschäftsleitung des Digitalverbands Bitkom e.V.

Deutschland wird WLAN-Hotspot-Land – und IT-Kompetenz nötiger denn je

von Ralf Koenzen

Die WLAN-Störerhaftung ist Geschichte. Seit dem Sommer 2016 können Unternehmen, Bürger und Institutionen ihre WLAN-Netze mit anderen teilen, ohne für deren Tun zu haften.

HILFE ZUR SELBSTHILFE IM MITTELSTAND

Die Veranstaltungsreihe IT-Sicherheit@Mittelstand von DsiN und DIHK bietet Entscheidern bundesweit praxisnahe Kurse für digitalen Schutz im Unternehmen. Grundlage sind kostenlose Schulungsmaterialien, die von DsiN entwickelt und in den IHKs vor Ort präsentiert werden: in bis zu acht Workshops jeden Monat. Dabei wird den Teilnehmern eine „Hilfe zur Selbsthilfe" ermöglicht. Der Bundesminister für Wirtschaft und Energie ist Schirmherr.

www.dsin.de/it-sicherheit-mittelstand

Mit dieser rechtlichen Neuregelung wird digitale Aufklärungsarbeit wichtiger denn je. Denn naiv genutzt bergen offene Netze erhebliche Cyberrisiken. Erst im souveränen Umgang können ihre Potenziale voll ausgeschöpft werden.

Mit dem Wegfall der WLAN-Störerhaftung hat die Politik eines ihrer digitalen Kernversprechen umgesetzt. Die Gesetzesänderung stellt WLAN-Betreiber – ob Privatperson, Unternehmen oder Gastronom – mit klassischen Providern gleich. Damit haften sie nicht mehr für Urheberrechtsverstöße durch fremde User in ihren Netzen.

Ganz bewusst hat der Gesetzgeber darauf verzichtet, den Betreibern freier WLANs Schutzmaßnahmen für ihre Netze vorzuschreiben. Ob und in welcher Weise sie Maßnahmen zum eigenen Schutz oder zum Schutz ihrer Nutzer ergreifen, bleibt ihnen selbst überlassen.

Diese neue WLAN-Freiheit ist ein großartiger Fortschritt. Sie wird die Digitalisierung hierzulande weiter vorantreiben. Doch sie verlangt auch eine ganz neue IT-Kompetenz – bei Usern wie Betreibern. Sie verlangt bewusstes Handeln im Netz und den souveränen Einsatz von IT-Sicherheitskonzepten. Sie braucht digitale Bildung.

Nur so kann es gelingen, dass WLAN-Anbieter nicht allzu sorglos ihre Netze öffnen, sondern im Vorfeld Konzepte entwickeln, wie sie öffentliche und interne Datenströme sicher trennen und ihre eigenen Netze effektiv schützen können. Nur so schaffen wir es, dass User öffentliche Netze umsichtig nutzen, ihre Endgeräte richtig konfigurieren und Verschlüsselung sowie virtuelle private Netzwerke (VPN) bewusst für ihre persönliche Sicherheit einsetzen.

Seit nunmehr zehn Jahren nimmt Deutschland sicher im Netz Schüler, Verbraucher und Unternehmen an die Hand, um sie in genau solchen Fragen zu bilden. Das Engagement für digitale Aufklärung und Wissensvermittlung außerhalb von Schule und Lehre hat einen enormen Stellenwert. Es macht Angebote für alle Gesellschaftsschichten und Altersklassen, für Privatpersonen und den klassischen deutschen Mittelstand. Viele dieser Zielgruppen wären über traditionelle Wege in Schulen und Universitäten nicht erreichbar.

Wie wichtig dieses Engagement ist, belegt einmal mehr der diesjährige DsiN-Sicherheitsindex. Er zeigt auf, dass das Sicherheitsverhalten der deutschen Verbraucher im Netz deutlich hinter ihren Schutzkenntnissen zurückbleibt.

Genau hier liegt die große Herausforderung der Zukunft. Wir müssen Wege finden, die Menschen zum Handeln zu motivieren. Dazu brauchen wir Produkte, die per se ein hohes Maß an Sicherheit aufweisen, also „secure by design" sind. Und wir brauchen den persönlichen Dialog zwischen Experten und Nutzern, wie Plattformen wie DsiN ihn ermöglichen. Mit Formaten und Angeboten wie der Digitalen Nachbarschaft oder IT-Sicherheit@Mittelstand sind wichtige Schritte getan, die es auszubauen gilt.

DSIN-SICHERHEITSINDEX

Die Aufklärungsarbeit erfordert Maßnahmen, die auf die konkreten Bedürfnisse der Verbrauchertypen – Fatalisten, Gutgläubige, Außenstehende und Souveräne – abgestimmt sind. Der DsiN-Sicherheitsindex gibt Auskunft über ihre digitale Bedrohungslage – und zeigt Anknüpfungspunkte, um die Sicherheitspraxis der jeweiligen Zielgruppe zu verbessern.

www.dsin.de/sicherheitsindex

Ralf Koenzen
ist Geschäftsführender Gründungsgesellschafter der Lancom Systems GmbH

Wem helfen Gesetze, die keiner versteht?

Europäischer Datenschutz muss noch transparenter werden

von Andrea Voßhoff

Deutschland ist dafür bekannt, dass seine Bürgerinnen und Bürger ein besonders hohes Datenschutzbewusstsein haben und demnach die Risiken der allgegenwärtigen Datenverarbeitung, der Vernetzung und Profilbildung besonders kritisch sehen. Wie etwa das Eurobarometer Datenschutz der Europäischen Kommission zeigt, sind die Deutschen gegenüber neuen Technologien überwiegend kritischer und skeptischer, was die Einhaltung des Datenschutzes betrifft, als die meisten anderen Europäer.

Aber ist damit alles bestens? Bedeutet dies, dass die Menschen in Deutschland selbstbewusst die Angebote und Dienste des Internets nutzen? Wissen sie deshalb tatsächlich, was genau mit ihren Daten im Netz passiert, wie man sich vor Missbrauch, Datendiebstahl und anderen Risiken wirksam schützen kann?

Ich denke, die Realität sieht ganz anders aus. Häufig wird beklagt – das zeigen auch die in meinem Hause eingehenden Anfragen und Beschwerden –, dass die rechtlichen Bestimmungen zum Datenschutz sehr kompliziert und unverständlich seien. Betrachtet man beispielsweise mit § 28 des Bundesdatenschutzgesetzes die zentrale Vorschrift für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Privatunternehmen, so ist dieser Befund auch nicht verwunderlich. Noch schwieriger ist es für den Einzelnen, die technischen Abläufe bei der allumfassenden Datenverarbeitung insbesondere im Internet wenigstens so weit nachzuvollziehen, wie es für eine aufgeklärte und selbstbewusste Inanspruchnahme der informationellen Selbstbestimmung notwendig wäre.

EUROPAWEITE KOOPERATION

Ich denke, diesen Befund können die Datenschutzaufsichtsbehörden in Bund und Ländern, aber auch in Europa nicht einfach so hinnehmen. Das tun sie auch nicht, denn es gibt inzwischen viele Initiativen, die die Aufsichtsbehörden auch gemeinsam ins Leben gerufen haben. Ich denke etwa an das von den Datenschutzbehörden in Bund und Ländern und vom Kanton Zürich betriebene Portal www.youngdata.de, das sich vor allem an Kinder und Jugendliche richtet.

Dabei dürfen wir aber nicht stehen bleiben. Die kürzlich verabschiedete und ab 25. Mai 2018 geltende Europäische Datenschutz-Grundverordnung (DSGVO) bietet ausdrücklich einen rechtlichen Rahmen für die Aufklärungsarbeit. So findet sich in dem langen Aufgabenkatalog, den der europäische Gesetzgeber den Aufsichtsbehörden in Artikel 57 DSGVO mit auf den Weg gegeben hat, gleich an zweiter Stelle die Aufgabe, „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung [zu] sensibilisieren und sie darüber auf[zu]klären“. Besondere Beachtung sollen dabei spezifische Maßnahmen für Kinder finden.

EUROPÄISCHE INFORMATIONS-STANDARDS

Dies ist ein klarer Auftrag, der nun von den Aufsichtsbehörden weiter mit Leben erfüllt werden muss. Dabei muss es mehr denn je auch darauf ankommen, dass Aufsichtsbehörden ihre Aktivitäten bündeln und dabei nicht an den Grenzen unseres Landes haltmachen. Die Datenschutz-Grundverordnung bietet vielmehr die Möglichkeit und gibt uns auch den Auftrag, hier europaweit zu kooperieren. Ebenso wenig wie die Verarbeitung personenbezogener Daten an nationalen Grenzen haltmacht, darf die Kontrolle der Einhaltung des Datenschutzes und damit auch die Aufklärungsarbeit sich allein auf nationaler Ebene bewegen.

Als ganz konkretes Mittel einer besseren Aufklärung und Information bietet die Datenschutz-Grundverordnung beispielsweise die Möglichkeit, die zahlreichen Informationen, die dem Einzelnen hinsichtlich der Verarbeitung seiner personenbezogenen Daten bereitzustellen sind, mit standardisierten Bildsymbolen (Icons) zu kombinieren. Damit soll nach Art. 12 Abs. 7 der DSGVO in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form ein aussagekräftiger Überblick über die beabsichtigte Verarbeitung vermittelt werden. Die Verordnung überträgt der Europäischen Kommission die Befugnis, Standards für derartige Icons europaweit festzulegen. Hier ist es an den künftig im Europäischen Datenschutzausschuss zusammengeschlossenen europäischen Datenschutzbehörden, die Kommission bei der Erstellung solcher Standards sachgerecht zu beraten.

Dies ist nur ein Beispiel, wie die Datenschutzbehörden ihrerseits zu mehr Bewusstsein, Transparenz und Wissen im Datenschutz beitragen können. Es wird künftig auch verstärkt darauf ankommen, den Menschen technische Möglichkeiten zum Selbstschutz aufzuzeigen, damit sie sich sicher im Netz bewegen können. Bei alldem darf natürlich nicht vergessen werden, dass es zunächst Sache der Unternehmen und Behörden ist, die datenschutzrechtlichen Regelungen einzuhalten und ihrerseits durch zusätzliche Maßnahmen, z. B. durch Zertifizierungen oder Codes of Conduct, für eine faire und transparente Datenverarbeitung zu sorgen.

Andrea Voßhoff
ist Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und im Beirat von Deutschland sicher im Netz e.V.

„Bits kennen keine Grenzen“

„Nicht mein Problem“ – das sagt sich leicht. Hersteller wünschen sich aufgeklärte Verbraucher, die wiederum fordern Hilfe vom Staat und der sieht sich versucht, die Hersteller in die Pflicht zu nehmen. Dabei wollen alle dasselbe: Sicherheit im Netz.

Franz König
Schriftführer im Verein zur Förderung der Seniorenarbeit in Lohmar e.V.
Jeder trägt seinen Teil zur IT-Sicherheit bei. Die Hersteller sind verantwortlich dafür, dass ihre Hard- und Software so genutzt werden kann, dass beim Einsatz keine sicherheitsrelevanten Probleme auftreten. Die Nutzer müssen sensibilisiert und geschult werden, damit sie keine Sicherheitsrisiken eingehen. Und der Staat muss entsprechende Rahmenbedingungen schaffen. Entscheidend geht es hierbei darum, dass die IT-Sicherheit für den Nutzer durchschaubar bleibt. Die Grenzen verlaufen dort, wo der Normalanwender die Zusammenhänge nicht mehr verstehen kann. Anwender müssen auf einen Blick erkennen können, ob ihre eingesetzte Hard- und Software sicher ist, und sie müssen Hilfen erhalten, wie sie den aktuellen Stand verbessern können. Eine Art Armaturenbrett, das die entsprechenden Informationen liefert, könnte im Betriebssystem oder in einer zusätzlichen Software verankert sein.

Dirk Heitepriem
Director Governmental Relations EMEA bei BlackBerry
Wir alle nutzen die Vorteile des Internets, doch wird immer deutlicher, welche Gefahren es auch birgt. Eine natürliche Reaktion ist es, nach einem wachsamen Staat zu rufen, der uns vor diesen Gefahren schützt. Aber ist wirklich der Staat für unsere Sicherheit im Netz verantwortlich? Dieses Netz ist global ausgerichtet, ein Staat allein kann kaum einen umfassenden Schutz per Gesetz schaffen – außer er blockiert weite Teile des Internets komplett. Schon deshalb sind wir alle dazu aufgerufen, für den größtmöglichen Schutz zu sorgen. Der Staat, indem er Rahmenbedingungen und Spielräume für multinationale Lösungen schafft und neue technologische Möglichkeiten fördert. Und die Hersteller, indem sie sich in jedem einzelnen Entwicklungsschritt auf Sicherheit fokussieren und die Nutzbarkeit vereinfachen. Denn jede Technologie ist immer nur so gut, wie sie für den Anwender nutz- und verstehbar ist.

Prof. Dr. Sachar Paulus
Experte für IT-Sicherheit an der Hochschule Mannheim und im Beirat von Deutschland sicher im Netz e.V.
IT-Sicherheit ist ein globales Problem – einfach deshalb, weil die Bits im Internet nicht vor Grenzen haltmachen. Doch „grenzenlos“ darf nicht „unkontrolliert“ bedeuten. Cyberkriminalität ist nur zu bekämpfen, wenn sie aufgedeckt und verfolgt wird und zu entsprechenden Konsequenzen führt. Es gibt noch einen anderen Punkt: Im World Wide Web prallen unterschiedliche Kulturen aufeinander, was zu widersprüchlichen Rechtsauffassungen führt, etwa in Datenschutzfragen. Meiner Ansicht nach sollten juristische Querelen am Ort des Nutzers ausgetragen werden und nicht, wie heute so oft, am Ort des Diensteanbieters. Nächster Schritt: Die juristischen Folgen müssen international durchsetzbar sein. Dafür sind Abstimmungen zwischen Staaten erforderlich – mehr aber nicht: Eine staatliche Vorgabe von konkreten Sicherheitsmaßnahmen kann nicht funktionieren, Staaten sollten immer nur den Rahmen bilden.

Hersteller, Staat oder Anwender: Wer trägt Verantwortung für IT-Sicherheit?

Neulich, im Neuland

von Richard Gutjahr

Wir schreiben das Jahr 2027. Identitätsdiebe treiben im Darknet ihr Unwesen. Polizei und Justiz sind überfordert. Anwälte gibt es nicht mehr, Richter auch nicht. Aufzeichnungen aus dem persönlichen Blog des Datenjägers Richard Gutjahr.

Es war kurz vor Mitternacht, als es an der Tür klopfte. Der Umriss, der sich durch den Bodyscan meiner Holo-Linsen abzeichnete, ließ auf eine mittelgroße Frau schließen, zierlich, um die 30, mit einem Faible für extravagante Kopfbedeckungen. „Mein Name ist Greta", stellte sich die Dame vor. „Ich brauche Ihre Hilfe."

Greta nahm Platz. Die Art, wie sie sich bewegte, wie sie ihre Beine übereinanderschlug, hatte etwas Katzenhaftes. Ihre Gesichtszüge waren markant, aber feminin. Blasse Haut, roter Lippenstift. Sie roch nach Seife und Chanel No. 5. Vor allem aber roch sie nach Ärger.

Für gewöhnlich mache ich einen großen Bogen um diesen Typ Frau. Dann wiederum: Was blieb mir übrig? Mein bedingungsloses Grundeinkommen war aufgebraucht, genau wie mein Hyperspeed-Datenvolumen, und der Monat hatte noch 22 lähmende Tage.

Greta begann zu erzählen. Von dem Tag, an dem sie gehackt wurde. Der Tag, an dem sie aufhörte, zu existieren. Wir schreiben das Jahr 2027. Organisierte Banden treiben ihr Unwesen im Netz, sie entführen Menschen, genauer gesagt, deren Daten. Ob Bankkonto, Versicherungspolice oder Geburtsurkunde; wer es mit diesen Gaunern zu tun bekommt und kein Lösegeld zahlt, wird sprichwörtlich von der Festplatte gelöscht, ausradiert aus dem Leben.

ID-Napping stand natürlich unter Strafe. Aber wer hielt sich noch an Gesetze? Anwälte waren schon vor Jahren abgeschafft worden. Eigentlich ein Grund zur Freude, das Problem: die Richter ebenfalls. Weil die Gerichte aufgrund der ausufernden Cyberkriminalität kollabierten, wurden Computersysteme eingerichtet, die in der Lage waren, auf Basis von Ermittlungsdaten und komplexen Algorithmen binnen Sekunden ein Urteil zu fällen.

Nicht immer waren diese maschinell errechneten Urteile gerecht. Aber was war schon gerecht? Und: Es war die einzige Möglichkeit, überhaupt noch irgendeine Form von Gerichtswesen aufrechtzuerhalten. Wem ein Urteil nicht passte (und wer über das nötige Kleingeld verfügte), der konnte den Bundes-Verfassungsrechner in Karlsruhe anrufen. Doch für Fälle wie den von Greta war ein solcher Weg nicht vorgesehen.

Identitäts-Entführungsopfer konnten nicht zur Polizei gehen. Für die Behörden existierten diese Personen nicht. Ohne korrespondierenden Eintrag im Melderegister liefen selbst biometrische Daten wie Iris-Scans oder Fingerabdrücke ins Leere. Für NONs, so nannte man diese Nicht-Existenzen, gab es nur noch eine letzte Anlaufstelle: Leute wie mich.

Habe ich mich überhaupt schon vorgestellt? Mein Name ist Gutjahr. Richard Gutjahr. Freunde nennen mich Dick. Feinde auch. Im Analog-Zeitalter war ich mal Journalist. Das war, bevor der Robo-Journalismus in die Redaktionen Einzug hielt. Wir Reporter verloren damals alle unseren Job. Zugegeben, um die meisten von uns war es nicht schade.

Heute bin ich ID-Jäger. Das sind Menschen, die sich auf das Aufspüren von persönlichen Daten im Netz spezialisiert haben. Obwohl wir Identitätsjäger nicht gerade den besten Ruf genießen, braucht man uns. Wir helfen, vermisste Daten im Darknet zu lokalisieren und wiederzubeschaffen, egal wie. Bezahlt werden wir nur, wenn es uns gelingt, den Klienten vollständig zu rekonfigurieren. 30 Prozent seines Net-Values, plus Spesen.

Am nächsten Morgen wurde ich von Klara, meiner digitalen Assistentin, geweckt. Die Knochen taten weh und mein Schädel brummte. Es war einer dieser Tage, an denen man nicht einmal seine Drohne vor die Tür schicken würde. Die Innenstadt von Frankfurt war in eine dicke Schicht von Sahara-Sand gehüllt. Die Luft war staubig und brannte in der Kehle. Zeit für einen Drink.

Bei Harry's Bar um die Ecke hatte ich noch Kredit. Es war Sonntagmittag, die Straßen menschenleer. Ein Tesla Twohundred näherte sich. „Hau ab!",

signalisierte ich dem Bordcomputer und das Fahrzeug zog vorüber. Billiger, chinesischer Schrott, designed in California. Ich dachte zurück an die Zeit, als Automobile noch in Deutschland gebaut wurden. Damals durften wir noch selbst lenken und mit 220 Sachen über die Autobahn heizen. Verrückt.

Gretas Daten wiederzubeschaffen war ein Kinderspiel. Harry hatte Connections, sprichwörtlich. Durch seinen Keller verliefen die Kabel zum DE-CIX, einem der größten Knotenpunkte des Internets. Gegen eine kleine Schutzgebühr ließ mich Harry an sein Terminal. Wer konnte ahnen, dass exakt von hier aus einer der größten Daten-GAUs in der Geschichte des Digitalzeitalters ausgehen sollte? Die Stunde Zero, der Moment, der die weltweite Datenwende einläutete. Aber das ist eine andere Geschichte und soll ein anderes Mal erzählt werden.

Richard Gutjahr
ist Moderator, Journalist
und Blogger

DsiN-10-Jahresrückblick

2015

DsiN startet drei Förderprojekte des Bundes, um über zwei Millionen Menschen anzusprechen: Berufsschüler sowie Ehrenamtliche und ältere Generationen stehen im Fokus. Zum 9. IT-Gipfel erscheint die SiBa-App, die in der ersten Woche 25.000-mal heruntergeladen wird. Mit IT-Sicherheit@Mittelstand geht eine bundesweite Workshopreihe mit IHKs an den Start. Die Mitarbeiterzahl von DsiN verdoppelt sich innerhalb von zwölf Monaten.
Dr. Thomas Kremer (Deutsche Telekom) wird zum DsiN-Vorstandsvorsitzenden gewählt.

2016

DsiN begrüßt sein 25. Mitglied und feiert 10-jähriges Bestehen mit dem Bundesminister des Innern und zahlreichen Partnern. Für Jugendliche findet myDigitalWorld erstmals in Kooperation mit dem Schülerwettbewerb der Bundeszentrale für politische Bildung statt. Daneben startet DsiN ein Projekt für Lehrer bis zur 8. Jahrgangsstufe.
Ministerialdirigent Peter Batt übernimmt den Vorsitz im DsiN-Beirat und folgt Martin Schallbruch.

2014

Die Digitale Agenda der Bundesregierung betraut DsiN mit verstärkter Aufklärungsarbeit für die IT-Sicherheit der Bürgerinnen und Bürger sowie KMU. Die Reihe der DsiN-Sichheitsleitfäden wird erweitert. Gemeinsam mit TNS Infratest startet der DsiN-Sicherheitsindex, ein Gradmesser der digitalen Sicherheitslage. Im neuen DsiN-Webportal werden erstmals 300.000 Besucher registriert. DsiN initiiert mit DsiN-Jahreskongress, DsiNsights-Breakfast und DsiN-Partnerabend drei neue Veranstaltungsformate.

2013

DsiN unterstützt Mittelständler bei sicherheitsrelevanten Fragen in der Cloud mit dem DsiN-Cloud-Scout. Ein Jahr später (2014) wird der Scout auf EU-Ebene in acht Landessprachen verfügbar gemacht.
Dr. Michael Littger folgt als Geschäftsführer von DsiN auf Heike Troue.

2012

Mit dem Wettbewerb „Wir zeigen es Euch – Die schönen Seiten des Internets“ spricht DsiN gezielt die Generation 60+ an. Und leistet mit der Passwort-Wechsel-App ein weiteres Angebot zur Passwortsicherheit für Verbraucher.
Dr. Christian Illek (Microsoft) folgt Ralph Haupter als DsiN-Vorstandsvorsitzender.

2011

Steuerberater und Wirtschaftsprüfer werden fortan bundesweit für zwei Jahre über IT-Sicherheit und Datenschutz im Betrieb aufgeklärt – insgesamt über 2.000 Berufsträger.
Der DsiN-Blog für den Mittelstand geht an den Start.
Ralph Haupter (Microsoft) wird Vorstandsvorsitzender von DsiN.

2010

DsiN adressiert junge Menschen mit dem Wettbewerb „Digitale Identitäten 2020“. Für den Mittelstand startet DsiN den Online-Sicherheitscheck für Geschäftsführer und IT-Enscheider, der seitdem die Grundlage des DsiN-Sicherheitsmonitors zur Sicherheitslage im Mittelstand ist.

2009

Mit insgesamt vier Aufklärungsfilmen zur IT-Sicherheit erreicht DsiN gemeinsam mit dem ZDF sowie der RTL Gruppe eine bundesweite Aufmerksamkeit für das Thema. Erstmals findet auf der Fachmesse it-sa in Nürnberg der DsiN-MesseCampus statt: DsiN fordert, dass Lehrpläne innerhalb der Informatikausbildung zu mindestens 10 Prozent die Vermittlung von IT-Sicherheit vorsehen.

2008

Das Sicherheitsbarometer mit Meldungen zu Sicherheitsvorfällen startet – sieben Jahre später wird es im Rahmen einer App grundlegend überarbeitet. Mit den „Internauten“ gelingt ein bundesweites Aufklärungsprojekt für Schüler.
Dr. Markus Dürig (BMI) wird zum ersten Vorsitzenden des Beirats gewählt.

2007

Mit „Starthilfe Sicherheit“ wird ein erstes Handlungsversprechen für den Mittelstand präsentiert.
Der Bundesminister des Innern übernimmt die Schirmherrschaft für den Verein; Prof. Dieter Kempf (DATEV) wird Vorstandsvorsitzender.

2006

Auf Initiative von Bundesregierung und Wirtschaft wird der Verein beim 1. IT-Gipfel ins Leben gerufen. Zuvor wurde der Verbund bereits in München mit Bill Gates, Edmund Stoiber und Prof. Dr. Henning Kagermann vorgestellt.
Heinz Bonn wird zum ersten Vorstandsvorsitzenden gewählt.

DsiN Sicherheitsindex 2016

1. WAS IST DER DSIN-SICHERHEITSINDEX?

Der DsiN-Sicherheitsindex erfasst die digitale Sicherheitslage der Onliner in einer Kennzahl. Die Unterscheidung von verschiedenen Nutzertypen erlaubt eine Differenzierung der Sicherheitslage nach Verbrauchergruppen. Denn Sicherheit hängt von individuellen Eigenschaften ab: dem Risikoverhalten, dem Wissensstand sowie der Bereitschaft zum Handeln. Die Ergebnisse zeigen konkrete Aufklärungsbedarfe sowie erforderliche Maßnahmen auf, um die IT-Sicherheit der Verbraucher zu verbessern. Grundlage des Index ist eine jährliche, repräsentative Befragung von zweitausend Nutzern gemeinsam mit TNS Infratest.

2. WAS SIND SEINE ERGEBNISSE?

Der Sicherheitsindex 2016 ergab – das dritte Jahr in Folge – eine leichte Verbesserung der Sicherheitslage auf nunmehr 65,4 Indexpunkte. Diese Entwicklung basiert auf einem leichten Rückgang der selbst registrierten, sicherheitsrelevanten Vorgänge sowie einer teilweisen Verbesserung des Sicherheitsverhaltens. Zugleich bleibt ein digitales Sicherheitsgefälle zwischen den Verbrauchergruppen bestehen – sowie eine Diskrepanz von Wissen und Handeln. Mit dem Anstieg der gefühlten Bedrohungslage vor den tatsächlich registrierten Sicherheitsvorfällen steigt das Risiko einer digitalen Vertrauenskrise.

3. WAS IST ALSO ZU TUN?

Es wird deutlich, dass jede Gruppe eigene Aufklärungsmaßnahmen erfordert. Fatalisten müssen stärker vom Sinn der Sicherheitsmaßnahmen überzeugt, Außenstehende eher mit einfach verständlichen Basisinformationen versorgt werden. Bei Gutgläubigen ist eine Schärfung der Risikoeinschätzungskompetenzen erforderlich. Um die Wissens-Verhaltens-Lücke zu verkleinern, bedarf es übergreifender Motivationsförderung. Diese umfasst auch Hilfe zur Selbsthilfe. Souveräne Nutzer sollten noch stärker als „Multiplikatoren“ von Sicherheitswissen eingebunden werden.

Die Studie zum Download finden Sie hier:

DsiN-Sicherheitsindex 2016

Digitale Sicherheitslage der Verbraucher in Deutschland

Fatalistische Nutzer

Typische Merkmale
Fatalisten sind online sehr aktiv und kennen viele Risiken. Eigene Sicherheitsvorkehrungen sind ihnen aber nicht so wichtig, da „sie eh nichts bringen“.

Sicherheitsniveau
Sicherheitsmechanismen sind zwar bekannt, doch wird deren Wirksamkeit bezweifelt. Das Sicherheitsniveau ist daher gering, insbesondere beim Thema Verschlüsselung hakt es.

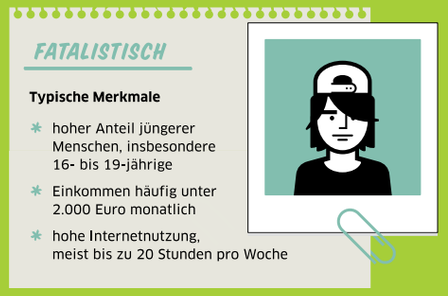
Bedürfnisse, die Aufklärungsarbeit berücksichtigen muss
Im Zentrum der Aufklärungsarbeit steht hier die Motivation zu mehr sicherem Verhalten. Der Sinn von Sicherheitsvorkehrungen im Netz muss positiv erläutert werden.

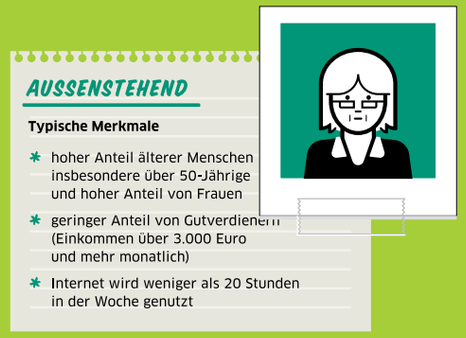
Außenstehende Nutzer

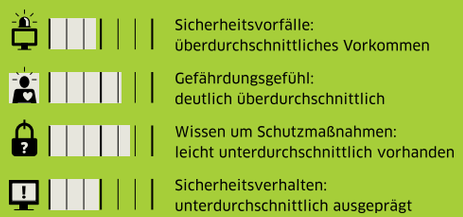
Typische Merkmale
Außenstehende fremdeln mit Computern. Das Netz erscheint ihnen schon jetzt zu kompliziert, um „auch noch Schutzmaßnahmen zu ergreifen“.

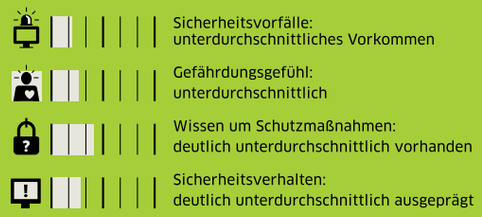
Sicherheitsniveau
Hier mangelt es oft schon am Verständnis für einfache Sicherheitsmaßnahmen, z. B. Antivirenprogramme. Auch der sparsame Umgang mit persönlichen Daten wird kaum beachtet.

Bedürfnisse, die Aufklärungsarbeit berücksichtigen muss
Defizite beim Sicherheitswissen und beim Sicherheitsverhalten müssen durch Sensibilisierung und einfache Informationen abgebaut werden.









Gutgläubige Nutzer

Typische Merkmale
Gutgläubige haben Spaß am Surfen – sind mit Laptop, Desktop-PC oder mit dem Smartphone online. Sie sichern sich aber nur wenig ab – denn „es wird schon nichts passieren“.

Sicherheitsniveau
Mangelnde Sorgfalt im Umgang mit digitalen Diensten ist nicht so sehr fehlendem Sicherheitswissen geschuldet, sondern vielmehr der zu wenig vorhandenen Einsicht, sich vor Risiken schützen zu müssen.

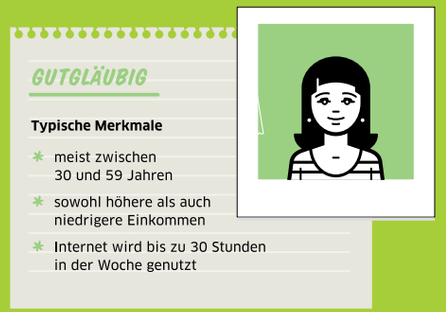
Bedürfnisse, die Aufklärungsarbeit berücksichtigen muss
Um Vorwissen über digitale Schutzmaßnahmen dieser Nutzergruppe zum Einsatz zu bringen, steht die Befähigung zur Risikoeinschätzung und Motivation zum Handeln im Vordergrund.

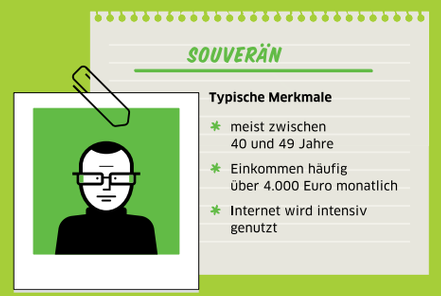
Souveräne Nutzer

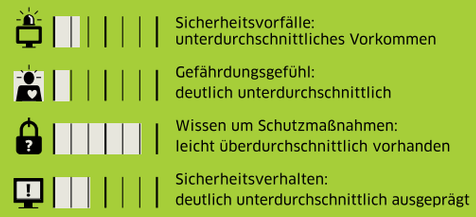
Typische Merkmale
Souveräne schätzen die digitalen Vorteile und nutzen diese auch. Auf billige Spam-Mails fallen sie nicht mehr rein und „könnten auch andere darüber aufklären“.

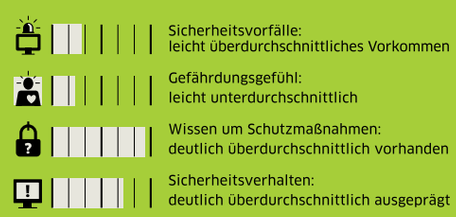
Sicherheitsniveau
Die korrekte Anwendung von Schutzmaßnahmen bewahrt diese Gruppe vor digitalen Risiken. Nachholbedarf besteht teilweise noch bei neuesten Sicherheitsdiensten und der Anwendung komplexer Lösungen.

Bedürfnisse, die Aufklärungsarbeit berücksichtigen muss
Das ausgeprägte Wissen und die Bereitschaft zu sicherem Handeln prädestiniert die Gruppe, ihre Vorbildfunktion zur Aufklärung anderer Nutzer als Multiplikator zu verstärken.









Der digitale Wandel ist allgegenwärtig. Kein Wunder. Es ist der größte Umbruch seit Erfindung des Buchdrucks. Und er ist schnell. Vor nur 10 Jahren, im Jahr 2006, steckten die größten Internetunternehmen unserer Zeit noch in den Kinderschuhen. Moderne Smartphones, die uns rund um die Uhr mit unserer Umwelt vernetzen, gab es noch nicht. 2006 ist auch das Gründungsjahr des Vereins Deutschland sicher im Netz. Seit 10 Jahren klärt er auf: über die Chancen, aber auch über die Risiken im Netz. In 35 kurzweiligen Beiträgen schauen namhafte Vertreter aus Politik, Wirtschaft und Gesellschaft zurück und vor allem nach vorn: auf 10 weitere Jahre im Netz – mit Sicherheit.

Schirmherrschaft

Bundesministerium des Innern

DsiN Deutschland sicher im Netz

www.10jahre.dsin.de www.dsin.de