EINE UNABHÄNGIGE THEMENZEITUNG VON EUROPEAN MEDIA PARTNER

EUROPEAN MEDIA PARTNER CONTENT WITH A PURPOSE

ANALYSE: DIGITALISIERUNG

MIT FOKUS AUF IT-SICHERHEIT

NR 4 | SEPTEMBER 2017 ANALYSEBUSINESS.DE

„Deutschland braucht dringend ein Digitalministerium – vor allem mit viel Entscheidungsgewalt.“

Lesen Sie das Vorwort mit Frank Thelen, europäischer Seriengründer, Technologie-Experte und Frühphasen-Investor. **Seite 2**

Lesen Sie mehr Artikel auf analysebusiness.de

Weitere Artikel zum Thema IT- Sicherheit, Cloudlösungen und Internet der Dinge auf analysebusiness.de

AKTUELLES

Datenschutz für ganz Europa – Die neue EU-DSGVO

Lange haben sie gerungen und am 26. Mai 2016 ist sie in Kraft getreten – Die neue EU-Datenschutz Grundverordnung. Am 25. Mai 2018 läuft die Übergangsfrist aus. **Seite 6**

FOKUS

it-sa: Gewappnet für die digitale Revolution

Mit über 580 erwarteten Ausstellern ist die „it-sa“ in Nürnberg zur größten Fachmesse für IT-Sicherheit in Europa geworden. **Seite 4**

„WannaCry“: eklatante Zunahme von Cyberangriffen

12. Mai 2017 – zunächst ein ganz normaler Tag. Während Bundeskanzlerin Angela Merkel über Steuerentlastungen sprach und sich die Finanzminister der G7-Staaten in Bari trafen, fraß sich ein Computervirus durch das weltweite Netz. Reisende auf deutschen Bahnhöfen wunderten sich, dass die Anzeigetafeln nicht mehr funktionierten. Doch dies war eine der geringeren Folgen. **Seite 22**

UNSERE EMPFEHLUNGEN – ALLE ARTIKEL IN VOLLER LÄNGE AUF ANALYSEBUSINESS.DE

„Es gibt noch viel zu tun!“
Deutschland darf beim Thema Digitalisierung nicht zurückfallen, warnt Mario Ohoven, der Präsident des Bundesverbands mittelständische Wirtschaft (BVMW). Mit der Digitalisierung der Wirtschaft und Gesellschaft stehen Unternehmen vor einem fundamentalen Wandel.

Unser Wohlstand hängt von der erfolgreichen digitalen Transformation ab
Bernhard Rohleder, Hauptgeschäftsführer des Branchenverbandes BITKOM e.V., zum Thema.

Digitale Transformation im Mittelstand
Der digitale Wandel verändert die Struktur und Wertschöpfungskette von Unternehmen und Branchen. Anpassen oder untergehen – vor dieser großen Herausforderung stehen heute nicht nur Mittelständler, sondern auch Kommunen oder Konzerne.

Foto: Sebastian Husche

Frank Thelen
Europäischer Seriengründer, Technologie-Experte und Frühphasen-Investor

„Deutschland braucht dringend ein Digitalministerium – vor allem mit viel Entscheidungsgewalt.“

WIR VERSPIELEN MIT UNSEREN BEDENKEN DEUTSCHLANDS ZUKUNFT!

„Digital First. Bedenken Second“, so machte FDP-Chef Christian Lindner im Wahlkampf Werbung. Und traf mitten in die DNA der Deutschen. Denn Innovationen sehen wir zuerst als Problem und erst dann als Chance. Wenn überhaupt. Online-Banking: Was kann da alles mit meinen Kreditkartendaten passieren? IT-Sicherheit im Unternehmen: Achtung, Virenalarm! Deshalb regiert in der deutschen Wirtschaft auch das Papier: Jeden Tag werden Millionen Dokumente von Autos und Menschen transportiert. Digitale Unterschriften? Fehlanzeige. Akten digital? Fehlanzeige. Das kostet Unternehmen und Staat jährlich Milliarden – und in fünf bis zehn Jahren Deutschland vielleicht sogar die Wettbewerbsfähigkeit. Noch heute fliegen täglich Helikopter von Hamburg nach London, um dringende Dokumente zu transportieren – nur um sie in Großbritannien unterschreiben zu lassen, während es in Afrika bereits Staaten gibt, die ihre Vermögenswerte digital auf der Blockchain verwalten und kein Bargeld mehr nutzen.

Na, ertappt? Auch Deutschlands Entscheider haben laut Leseranalyse – immer noch – lieber eine Zeitung aus Papier in der Hand als ein ePaper fürs Tablet.

Das Problem: Weil unsere Wirtschaft boomt, glauben wir es uns erlauben zu können, analog zu bleiben. Ein Fehler. Denn zwei bis drei Prozent Optimierung im Jahr: Das war im Ingenieurstaat Deutschland noch okay – im weltweiten Wettbewerb jedoch werden sich Anbieter mit revolutionären Produkten, die zehnmal mehr bieten, durchsetzen. Deutschland braucht dringend ein Digitalministerium – vor allem mit viel Entscheidungsgewalt. Stellen wir uns einmal vor, in staatlichen Behörden würde es ab 2020 kein Papier mehr geben. Bis hin zur Unterschrift wäre alles digital. Der nächste Schritt wäre, ganz viele Routineaufgaben zu automatisieren. Und nur auf dieser Basis können wir dann in fünf bis zehn Jahren künstliche Intelligenz effektiv nutzen. Natürlich werden Fehler passieren! Doch die Digitalisierung wird auch ohne uns kommen. Und wer sich der Digitalisierung verschließt, wird in einigen Jahren sicher der Verlierer sein. Bedenken sind etwas für gute Zeiten. Jetzt müssen wir mit Mut und Konsequenz Deutschland zukunftsfähig machen.

MAX EMPFIEHLT!

Ich empfehle Ihnen den Fachartikel auf Seite 6 zum Thema EU-DSGVO und die Titelstory auf Seite 12 mit/über Elon Musk.
Max Bettzig, Senior Project Manager

INHALT

ANALYSE: DIGITALISIERUNG

Project Manager: Max Bettzig
max.bettzig@europeanmediapartner.com

Geschäftsführer: Kristoffer Andersson
Redaktionsleiter: Mats Gyldorff
Layout und Anzeigengestaltung: Aileen Reese
Lektorat: Nicole Bitkin
Titelbilder: Vern Evans Photo 2010, Sebastian Husche
Distribution: Die Welt Gesamt, September 2017
Druck: Axel Springer SE

EUROPEAN MEDIA PARTNERS CONTENT WITH A PURPOSE

European Media Partner Deutschland GmbH
Neuer Wall 59,
DE-20354 Hamburg
Tel.: +49 40 299 977 400
Email: info@europeanmediapartner.com
www.europeanmediapartner.com

European Media Partner sind Spezialisten im Content-Marketing. Durch ein hochwertiges redaktionelles Umfeld und eine hohe Verbreitung schaffen wir eine optimale Medienpräsenz auf dem Markt. Wir helfen Unternehmen durch passgenaue Produkte ihre Zielgruppe treffsicher zu erreichen.

Folgen Sie uns: @europeanmediapartnerdeutschland | analysebusiness.de | Recyclen oder weiterreichen!

GEWAPPNET FÜR DIE DIGITALE REVOLUTION

Mit über 580 erwarteten Ausstellern ist die „it-sa“ in Nürnberg zur größten Fachmesse für IT-Sicherheit in Europa geworden.

Frank Venjakob, Executive Director it-sa, NürnbergMesse.

Einen so starken Zuwachs an Ausstellern und Interessenten wie in diesem Jahr haben die Macher von Europas größter Messe für IT-Security „it-sa 2017“ in Nürnberg trotz aller positiver Resonanz nicht erwartet. „Wir rechnen bei der diesjährigen Messe vom 10. bis zum 12. Oktober mit mehr als 580 Ausstellern. Im Vergleich zu 489 Ausstellern im vergangenen Jahr ist das ein deutliches Plus“, freut sich Frank Venjakob, der die it-sa bei der NürnbergMesse verantwortet. Neben zwei weiteren großen IT-Security-Messen in den USA und in London hat sich die it-sa, die seit 2011 unter der Regie der NürnbergMesse durchgeführt wird, zu einer der bedeutendsten Drehscheiben der Szene entwickelt. Vom Kleinunternehmer bis zum Großkonzern sind die wichtigsten Player in Nürnberg vertreten.

„IT-Sicherheit ist ein internationales Thema“, sagt Venjakob. „Wir haben in diesem Jahr mit Frankreich, Tschechien und Israel drei Gemeinschaftsstände auf der Messe. Tschechien und Frankreich als Nachbarländer schielen natürlich immer auf den deutschen Markt. Und Israel ist bekannt als Startup-Nation, ein Land, in dem sich junge Firmen zu Weltmarken entwickelt haben.“

Um dem Ansturm im Oktober 2017 gerecht werden zu können, ist die „it-sa“ in Nürnberg in neue Hallen umgezogen. Mit über 40 Prozent mehr Ausstellungsfläche kann sich die Messe in diesem Jahr noch einmal anders darstellen als in den letzten sieben Jahren ihres Bestehens. Die EU-Datenschutz-Grundverordnung wird auf der it-sa 2017 ein ebenso wichtiges Thema sein wie die vielen Produkte und Services, um dem Gefahrenpotenzial der Cyberkriminalität adäquat begegnen zu können. „Ein Gesetzestext ist ja immer nur die eine Seite, die Umsetzung aber eine andere“, meint der Executive Director der it-sa. „Darum haben wir auch viele Vorträge zur Rechtsproblematik – damit klar wird, wie der regelkonforme Schutz eines Unternehmens aussehen kann.“

„Die ‚it-sa‘ bietet Vorträge, die aufzeigen, wo es in Zukunft hingeht. Das ist sowohl für die Besucher anregend, als auch für die Aussteller.“

Ein zentrales Merkmal der „it-sa“ sind die offenen Foren mit Fachvorträgen, bei denen technische Aspekte ebenso im Mittelpunkt stehen wie Hard- und Software-Neuheiten oder die vielen brillanten Ideen der Startup-Szene. „Auf den Vortragsbühnen haben wir zum einen Firmenvorträge, wo die neuesten Entwicklungen gezeigt werden“, sagt Venjakob. „Wir haben zum anderen aber auch die übergreifenden Themen, die wir in diesem Jahr mit ‚it-sa insights‘ neu betitelt haben. Hier halten Experten produktunabhängige Präsentationen und schauen über den Tellerrand hinaus.“

Über den Tellerrand hinausblicken will auch der diesjährige Special Keynote Speaker der „it-sa“, der Netzaktivist und ehemalige WikiLeaks-Sprecher Daniel Domscheit-Berg. Nachdem die „it-sa“ in den vergangenen Jahren mit Edward Snowden und Maximilian Schrems bereits prominente Protagonisten sprechen ließ, wird Domscheit-Berg in diesem Jahr die Frage aufwerfen, ob wir gewappnet sind, wenn die digitale Revolution richtig Fahrt aufnimmt.

Text: Helmut Peters

FAKTEN

Die IT-Sicherheitsmesse „it-sa“ war ursprünglich ein Teil der Computermesse „Systems“ in München und dort bis 2008 beheimatet. Dann zog sie als eigenständige Veranstaltung nach Nürnberg, wo sie im Oktober wieder die neuesten Produkte der Branche zeigt und auf vier Bühnen mit rund 320 Vorträgen die neuesten Trends und Lösungen der IT-Sicherheit präsentiert.

GEORDNETE ZUGRIFFSRECHTE FÜR DATENNETZWERKE

Anfang September 2017 wurde ein gigantischer Datendiebstahl in den USA bekannt. Hackern war es gelungen, in die Datenbankbestände der Wirtschaftsauskunftei Equifax zu gelangen und sich dort nicht nur der Telefonnummern und Adressen, sondern auch der Sozialversicherungsnummern von 143 Millionen US-Amerikanern zu bemächtigen.

©REDPIXEL - stock.adobe.com

Immer wieder versuchen Hacker etwa unbefugt an die Kundendaten von Onlineshops zu gelangen.

Da diese Nummern zur Identifizierung etwa bei Ratenkreditkäufen dienen und einen US-Bürger von der Wiege bis zur Bahre begleiten, ist dieser Datenklau besonders gravierend. Rund 40 Prozent der US-amerikanischen Bevölkerung sind betroffen. Nun geht man zwar auf der anderen Seite des Atlantiks etwas unbekümmerter mit personenbezogenen Daten um als hierzulande – doch sollte man sich in Europa oder auch im datensensiblen Deutschland deshalb noch lange nicht in Sicherheit wähnen.

Attacken gibt es auch hierzulande, selbst im großen Stil. Immer wieder versuchen Hacker etwa unbefugt an die Kundendaten von Onlineshops zu gelangen. Man kann so viel technischen Schutz wie möglich einsetzen, eine Schwachstelle bekommt ein Unternehmen nur sehr schlecht in den Griff: den Menschen selbst. Immer wieder sind es Leichtsinn, Unwissenheit oder Fahrlässigkeit, mit denen er Tor und Tür öffnet. Aus diesem Grund ist eine vernünftige und konsequente Verwaltung von Berechtigungen auf die Dateien des Unternehmensservers unerlässlich. Sie unterstützt dabei, die Gefahr eines unberechtigten Zugriffs auf Firmendaten zu minimieren.

„Man kann so viel technischen Schutz wie möglich einsetzen, eine Schwachstelle bekommt ein Unternehmen nur sehr schlecht in den Griff: den Menschen selbst.“

Gerade in mittelständischen Unternehmen mit „gewachsenen“ Strukturen sind Prozesse möglicherweise noch nicht durchstrukturiert. So werden beispielsweise beim Ausscheiden eines Mitarbeiters nicht immer gleich die IT-Administratoren unterrichtet, die für eine Sperrung des Accounts sorgen.

Auch sogenannte Überberechtigungen können zum Problem werden. IT-Sicherheitsexperten weisen immer wieder darauf hin, dass ein Berechtigungsmanagement bei IT-Netzwerken mit Bordmitteln und manuell kaum noch ausreichend ist – zum einen, weil der administrative Aufwand zu groß ist und zum anderen, weil dadurch die Benutzerdatenbestände inkonsistent werden. Ein gutes Identity & Access Management ermöglicht eine strukturierte Vergabe der Zugriffsmöglichkeiten an Mitarbeiter, speichert und dokumentiert sie und wertet die Benutzeraktivitäten aus.

Derartige Systeme werden mit der EU-Datenschutz-Grundverordnung (DSGVO), die im kommenden Jahr in Kraft treten wird, immer wichtiger. Unternehmen müssen „geeignete technische und organisatorische Maßnahmen“ ergreifen, vor allem für Datensicherheit und Datenschutz sensibler Daten. Mit Inkrafttreten werden die Auflagen, die eine Meldepflicht von Verstößen vorschreiben, verschärft und die Meldefristen auf 72 Stunden verkürzt. Zudem drohen Unternehmen, die gegen die neuen Vorschriften verstoßen, empfindliche Geldstrafen, die bis zu zwei Prozent des Jahresumsatzes betragen können.

Text: Frank Tetzel

WEITERE ARTIKEL AUF:
ANALYSEBUSINESS.DE

DATENSCHUTZ FÜR GANZ EUROPA – DIE NEUE EU-DSGVO

Lange haben sie gerungen und am 26. Mai 2016 ist sie in Kraft getreten – Die neue EU-Datenschutz-Grundverordnung. Am 25. Mai 2018 läuft die Übergangsfrist aus.


Copyright © Nicola Fioretta

Datenschutzbeauftragte in Firmen werden ab dem nächsten Jahr ein wichtiger Posten sein.

Vier Jahre haben die Gremien darüber verhandelt. Dann stimmten das Europäische Parlament, der Europäische Rat und die Europäische Kommission für die neue EU-Datenschutz-Grundverordnung, kurz EU-DSGVO. Die neue Verordnung ist seit dem 26. Mai 2016 in Kraft und ersetzt die seit 1995 geltende EU-Datenschutzrichtlinie (95/46/EG). Eine Übergangfrist von zwei Jahren soll es allen Unternehmen, Institutionen und der öffentlichen Hand ermöglichen, den Datenschutz und die neue Verordnung richtig und sicher umzusetzen.

Mit der neuen Verordnung wurde der Datenschutz in Europa endlich vereinheitlicht. Es gelten in allen Staaten die gleichen Standards, jeder Einzelne soll mehr Kontrolle über seine Daten haben. So weit der Anspruch der Parlamentarier zur neuen Verordnung – doch was kommt da wirklich auf Privatpersonen und Firmen zu? Was ist erlaubt und was wird verboten? Welche Strafen drohen und wer setzt diese dann um? Für die Seite der Unternehmen gelten ab Mai 2018 auch viele strengere Regeln. So müssen sich der neuen EU-DSGVO künftig auch nicht in Europa ansässige Unternehmen unterwerfen. US-Firmen, die sich auf dem europäischen Markt tummeln, werden dann auch nach der neuen EU-DSGVO überprüft. Das bislang gültige Argument dieser Firmen, sie würden nur nach dem Datenschutzrecht der USA handeln, gilt dann nicht mehr.

Verschärft wurden auch die Strafen bei den Unternehmen. Wurden bislang starre Bußgelder bei Datenverstößen erhoben, können jetzt Bußgelder in Abhängigkeit vom Jahresumsatz des Unternehmens verhängt werden. Bis zu 4 Prozent können die Strafen betragen. Da können schnell Summen in Millionenhöhe bei einem Verstoß zusammenkommen.

Besonders auf den Mittelstand kommen da schwere Zeiten zu. Es gibt leider keine Musterlösung, jedes Unternehmen muss das für sich selbst prüfen. Die Unternehmen tragen in der Zukunft die volle Verantwortung für die im Unternehmen genutzten Daten. Vor allem personenbezogene Daten müssen besonders geschützt werden. Dabei geht es nicht nur um den Diebstahl von außen, sondern auch um Manipulation und Zerstörung von ganzen Datenbanken. Wichtig ist: Nach der neuen Rechtslage hat sich die Beweislast umgekehrt – die Firmen haben die Pflicht, ihre IT und die Systeme sicher zu machen. Alles unterliegt einer erweiterten Rechenschaftspflicht. Sie ist der zentrale Grundsatz der neuen EU-DSGVO. Damit rückt die Verantwortlichkeit von Firmen, Institutionen und Unternehmen in den Vordergrund. Es muss alles lückenlos dokumentiert werden, eine fehlerhafte Dokumentation der datenschutzrechtlichen Umsetzung kann sich ganz erheblich auf die Höhe der möglichen Bußgelder auswirken.

Der Datenschutzbeauftragte in den Firmen wird also ab dem nächsten Jahr ein wichtiger Posten werden. Schon jetzt bereiten viele Berater und Anwaltskanzleien ihre Kunden und Mandanten auf die neuen Gesetze und Verordnungen vor.

Text: Jörg Wernien

FAKTEN

Wenn am 26. Mai 2018 die neue EU-DSGVO wirksam wird, gibt es in Europa endlich eine einheitliche Grundlage dafür, welche Rechte und Pflichten Privatpersonen, Unternehmen und die öffentliche Hand beim Umgang mit Daten haben. Die ganze Verordnung und was alles neu ist, findet sich hier: dsgvo-gesetz.de

EINE HILFESTELLUNG ZUR EU-DSGVO GIBT ES AUF UNSERER WEBSITE: **ANALYSEBUSINESS.DE**

3 FRAGEN AN MATTHIAS STEINKAMP


Foto: Frauke Schumann

Matthias Steinkamp, Vorstand der TAROX AG

Worin unterscheiden sich die Anforderungsprofile mittelständischer Firmen von anderen Kunden in der IT-Branche?

Mittelständler legen Wert auf ganzheitliche Lösungen, die von der ITK-Infrastruktur bis zur Anwendung in Büro und Produktionsbetrieb ein zuverlässiges Komplettpaket auf neuestem Stand mit Ausbaureserven für die Zukunft mitbringen. Tarox versteht sich dabei als Wegbegleiter entlang der Wertschöpfung, um die digitale Transformation erfolgreich umzusetzen und voranzutreiben. Das Spektrum reicht von ganzheitlicher IT-Sicherheit bis zum Komplett-Softwarepaket fürs Enterprise Content Management.

Was stellt aktuell das größte Problem in der Cyber-Security dar?

Eben genau die fehlende Ganzheitlichkeit. Bei vielen Mittelständlern wurden verschiedene Systeme implementiert, die oft nebeneinander ausreichend Schutz gewährleisten sollen. Zuverlässige Security bedarf allerdings des Miteinanders der Instrumente in einem System sowie der Sensibilisierung sämtlicher Kräfte, die Zugriff auf die ITK-Infrastruktur haben.

Warum werden Cloud-Services immer wichtiger?

Im Cloud Computing schwirrt die Rechnerwolke eben nicht irgendwo schutzlos herum, sondern die bereitgestellten ITK-Infrastrukturen wie Speicherplatz, Rechenleistung oder Anwendungssoftware sind professionell gesicherte Dienstleistungen im Internet nur für Autorisierte.

MEHR SICHERHEIT DURCH PENTESTS

Mit sechzehn Jahren startete Frank William Abagnale Jr. eine legendäre Karriere als Scheckbetrüger. Schon mit 21 Jahren hatte sich der junge Mann erfolgreich als Pilot, Arzt, Professor für Soziologie und Regisseur ausgegeben.

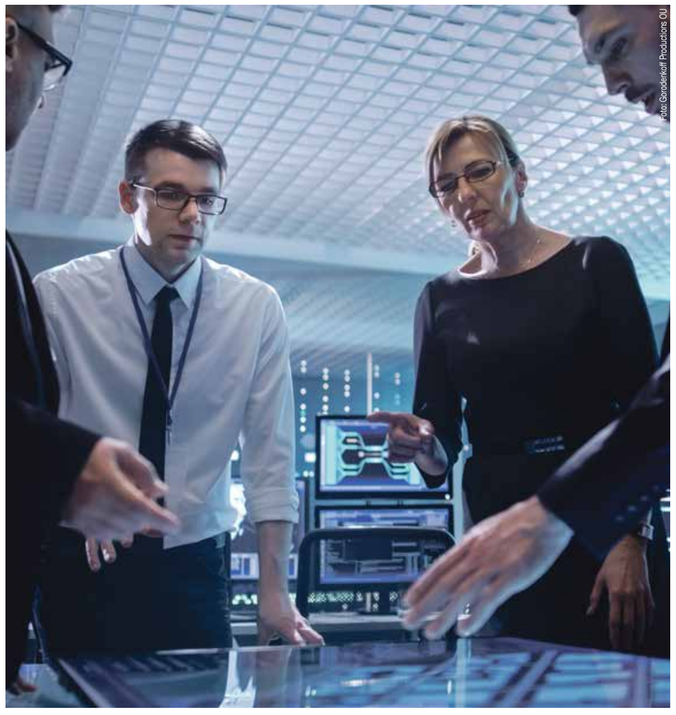


Foto: Gorodenkoff Productions OU

Als Fälscher gelang es ihm rund 2,5 Millionen Dollar – im heutigen Wert von etwa 16 Millionen – zu ergaunern. Leonardo di Caprio spielte Anfang der 2000er-Jahre die Hauptrolle im Steven-Spielberg-Streifen „Catch me if you can". Der richtige Frank William Abagnale Jr. wurde nach wenigen Jahren Haft entlassen und arbeitete fortan für das FBI, wo er – nun auf der anderen Seite – als anerkannter Experte die besten Fälschungen und Blüten erkannte.

Heute lösen Gauner, Kriminelle oder auch Staaten keine ungedeckten und gefälschten Schecks mehr ein, sondern versuchen über das World Wide Web an die Kronjuwelen und vor allem an das neue Gold, die Kundendaten von Millionen von Bürgern oder Kunden, zu gelangen. Umso wichtiger ist es, dass auch auf Unternehmensseite Menschen wie Frank William Abagnale Jr. sitzen, die die Gefahren erkennen, die Unternehmen aus dem Cyberspace drohen können. In der digitalisierten Welt sind vernetzte Systeme zunehmend Angriffen von außen ausgesetzt. Sicherheitsrelevante Unternehmen müssen deshalb Gewissheit haben, wie sicher ihr eigenes IT-Netzwerk ist.

Fachleute nennen den Versuch, einen Sicherheitstest auf Rechnern oder Netzwerken durchzuführen, Penetrationstest oder verkürzt Pentest. Dabei werden alle Systembestandteile und Anwendungen von Netzwerken oder auch der Systemsoftware daraufhin untersucht, ob ein Hacker eine Möglichkeit findet, unerkannt und unautorisiert in ein Netzwerk einzudringen oder eine Schwachstelle auszunutzen.

Wie wichtig die IT-Sicherheit in Unternehmen vom Gesetzgeber gesehen wird, hat er in § 93 Abs. 1 und § 91 Abs. 2 Aktiengesetz festgeschrieben. Hier werden die Sorgfaltspflichten und Verantwortlichkeiten von Vorständen definiert. Juristen weisen beständig darauf hin, dass dies auch GmbH-Geschäftsführer betreffe, da aktuelle Urteile, die Aktiengesellschaften beträfen, immer auch auf GmbHs abstrahlen würden. Grundsätzlich kann also ein Vorstand oder ein Geschäftsführer persönlich in die Haftung genommen werden, wenn es um Schäden in der IT-Sicherheit geht. Wer nämlich eine „Entwicklung, die zukünftig ein Risiko für das Unternehmen darstellen könnte, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt", wird persönlich in die Haftung genommen, zudem drohen hohe Bußgelder.

Unternehmen haben sich auf die Durchführung dieser Penetrationstest spezialisiert, denn ein professionell durchgeführter Pentest ermöglicht der beauftragenden Firma eine genaue Einschätzung der Sicherheit ihrer Unternehmensdaten und die Darstellung des Gefahrenpotenzials des penetrierten Umfeldes aus der Sicht eines Hackers. Damit will man die Erhöhung der Sensibilität zur Sicherheit der technischen Systeme und Infrastruktur erreichen. Dies soll vor allem durch das Aufzeigen von Schwachstellen und Sicherheitslücken, die Überprüfung von umgesetzten Sicherheitsmaßnahmen, daraus abgeleitete Maßnahmenempfehlungen zu gefundenen Schwachstellen und Empfehlungen zur Compliance der IT-Sicherheit in den geprüften Unternehmen gelingen. Zudem werden vom IT-Sicherheitsunternehmen Vorschläge für eine regelmäßige IT-Sicherheitsstrategie erarbeitet.

Ansatzpunkte, an denen Penetrationstests durchgeführt werden, sind meistens die Schnittstelle zwischen dem Firmennetz und dem öffentlichen Netz (Internet). Dazu gehören Firewalls und Sicherheitsgateways. Zudem sind die Komponenten des Netzwerkes – Router und Switches –, Server und andere Speichersysteme, Telefonanlagen, Webanwendungen – wie Webshops oder Internetauftritte –, WLAN-Netze oder Bluetooth, aber auch Gebäudesteuerungen und Zugangskontrollsysteme ideale Punkte, um in die IT-Systeme des zu prüfenden Unternehmens einzusteigen.

Bei Fachleuten wird seit langem darüber diskutiert, ob Penetrationstests als sogenannte Blackbox- oder Whitebox-Tests durchgeführt werden sollen. Während bei einem Blackbox-Test die Penetrationstester nur die Adressinformationen des Zieles kennen, hat der Penetrationstester bei einem Whitebox-Test umfangreiche Informationen über die zu testenden Systeme. Das Bundesamt für Sicherheit empfiehlt bei den Pentests in erster Linie „Whitebox-Tests durchzuführen, da bei einem Blackbox-Test aufgrund nicht vorliegender Informationen Schwachstellen übersehen werden können". Es bestehe die Gefahr, dass im Rahmen eines Blackbox-Tests Szenarien wie der Angriff eines informierten Innentäters nicht berücksichtigt würden. Zusätzlich bestehe bei einem Blackbox-Test ein höheres, durchaus vermeidbares Risiko, einen unbeabsichtigten Schaden zu verursachen.

Im rechtlichen Graubereich, wie manch einer zu glauben scheint, bewegen sich seriöse Unternehmen, die Penetrationstests anbieten, nicht. Auch wenn das Strafgesetzbuch nicht nur schon die Vorbereitung des Ausspähens und Abfangens von Daten als Straftatbestand ansieht, sollte man auf alle Fälle ein umfangreiches Pflichten- und Lastenheft erstellen und einen rechtssicheren Vertrag abschließen, der von unternehmensverantwortlicher Stelle unterschrieben werden sollte. Dann sind beide Parteien auf der sicheren Seite.

Text: Frank Tetzel

DAS INTERNET DER DINGE BRAUCHT VIELE LÖSUNGEN

Big Data Infrastruktur, Embedded Systems, Schutz vor Hackern, Smart Life – der digitale Wandel fordert unternehmerisches Handeln heraus.

Mehr dazu auf **analysebusiness.de**

Windows Server

TAROX empfiehlt Microsoft® Software.

Schichtwechsel!

Wechseln Sie jetzt zur neuesten Generation TAROX Server mit Intel® Xeon® Platin-Prozessor

- Maximale Performance für Ihre Applikation mit hoch skalierbarer Architektur
- Flexible interne Datenspeicherkonfigurationen
- Integrierte Sicherheitsfunktionen zum Schutz der Hardware
- Neuste Generation der Netzwerkkomponenten für einen effizienteren Datentransfer
- Optimiertes Energie- und Temperaturmanagement
- Verbessertes Ressourcenmanagement

Diesen Artikel finden Sie unter **www.tarox.de**

TAROX SecurityAllianz

Erleben sie den viermaligen besten Hersteller des Jahres mit seiner Security Allianz auf der **ITSA 2017!**
Halle 10.1, Standnummer 416

CRN 2016 15 14 13 Bester Hersteller

TAROX
IT-Technologie made im Ruhrgebiet

TAROX Aktiengesellschaft | Stellenbachstr. 49–51 | 44536 Lünen | Telefon: +49 (0)231/98 98 0-300 | vertrieb@tarox.de

Foto: KEVIN EVANS PHOTO

„Über kurz oder lang könnte die Erde für Menschen unbewohnbar werden."

Elon Musk ist einer der innovativsten Erfinder der Welt. Deshalb erkennt er auch, wohin sich KI – ganz ohne unser Zutun – entwickeln könnte.

Mit Tesla hat Technologie-Ass Elon Musk geschafft, was andere Autobauer seit langem erfolglos versuchen: E-Mobility sexy zu machen. Für die massentaugliche und trotzdem schnittige, nur etwa 35 000 Dollar teure Variante des brandneuen Model 3 trafen bei Tesla bereits 400 000 Vorbestellungen ein und nun kommt das Unternehmen kaum mit der Auslieferung hinterher. So super ist Tesla? Dann macht man es gleich noch besser und entwickelt für seine Kunden einen eigenen Musik-Streamingdienst, der via Internet in die Fahrzeuge integriert werden könnte.

„Technologie verbessert sich nur dann, wenn ‚smarte Menschen' wie die Irren arbeiten", erklärt der Tesla-Geschäftsführer, der als Umsatzziel das Erreichen der magischen 500 000-Stück-Grenze im kommenden Jahr nennt. „Teslas Mission ist es, die weltweite Umstellung auf nachhaltige Energie zu beschleunigen." Um den Stromverbrauch zusätzlich zu reduzieren, wurden in die Fahrzeuge Smart Microgrids eingebaut, eine intelligente Steuerung zum Verbrauch elektrischer Energie – ganz automatisch, ohne dass der Fahrer etwas davon mitbekommt.

Elektrische Fahrzeuge liegen den Tech-Milliardär auch deshalb so am Herzen, weil er überzeugt davon ist, sie in absehbarer Zeit auf dem Mars fahren zu lassen. „Über kurz oder lang könnte die Erde für Menschen unbewohnbar werden", erklärt er seine Mission. „Deshalb habe ich SpaceX gegründet. Raketen, mit denen ein Teil der Menschheit zum Mars fliegen kann." Und woher soll der Strom auf dem Roten Planeten stammen? Auch daran hat der Visionär gedacht. Letztes Jahr übernahm er für 2,6 Milliarden Dollar die Ökostromfirma Solar City, die Speicher für Solarenergie produziert. Doch damit nicht genug: auch das eigene Batteriesystem wird ausgebaut. Eine Powerwall für zu Hause mit integrierter Heizungstechnik, die – natürlich – mit dem Internet verbunden ist und smart gesteuert wird. Als letzte Errungenschaft bietet Tesla Solar Roof ab dem Sommer Solardachziegel an.

Jedes neue smarte Angebot scheint das Leben auf den ersten Blick einfacher zu machen: Ein Streamingdienst, der recht bald erkennt, was zur Lieblingsmusik zählt und diese selbst aussucht. Das Auto, das niemals einschläft oder abgelenkt ist und bremst, wann immer es eine potenziell gefährliche Situation erkennt. Smarte Heizung, die weiß, welche Temperatur als angenehm empfunden wird und diese Einstellung „versteht".

All das geht auf eigene Einstellungen zurück, doch inzwischen zeigen sich erste Anzeichen der Digitalisierung ohne persönliche Steuerung: Google schickt Vorschläge für Cafés und Geschäfte in unmittelbarer Nähe aufs Smartphone, sobald man sich an einen neuen Ort begibt. Facebook lauscht anscheinend bei Telefonaten und schickt Angebote, die sich auf im Telefonat verwendete Begriffe beziehen. Ganz schön clever, wie „selbstständig" die Maschinen der beiden Großkonzerne mittlerweile agieren. Und doch ist es nur eine Frage der Zeit, bis auch Waffen selbstständig Entscheidungen treffen werden. „Zusammen mit Stephen Hawking und Apple-Mitbegründer Steve Wozniak habe ich dazu bereits vor zwei Jahren auf der ‚International Joint Conference on Artificial Intelligence' in Buenos Aires vor aus dem Ruder laufender Künstlicher Intelligenz gewarnt, die im Zuge der Digitalisierung immer weiter voranschreitet."

Denn was nimmt beispielsweise der Computer eines selbstständig fahrenden Autos als Grundlage für seine Entscheidungen? Erkennt er den Unterschied zwischen einem kleinen Kind und einem Reh? Wer programmiert, was lebenserhaltend ist? Mehrere Forscher arbeiten weltweit an der Entwicklung kognitiver Maschinen, und diese Maschinen schreiben sich ihre eigene Software ununterbrochen weiter. Wenn also nun Maschinen selbst entscheiden, was sie für lebenswert halten, könnte dies das Ende der Menschheit bedeuten. Aber halt – wozu ist man schließlich einer der klügsten Erfinder der Welt?

Die Non-Profit-Organisation OpenAI, die Elon Musk 2015 gegründet hat, beschäftigt sich auf Open-Source-Basis mit der Erforschung künstlicher Intelligenz. „Unser Ziel ist, digitale Intelligenz so voranzubringen, dass sie wahrscheinlich der Menschheit als Ganzes dient, unbeschränkt von einem Erfordernis, eine finanzielle Rendite zu erzielen", schreibt er in einem Blogbeitrag zu Open AI. Schließlich verdienen sehr viele Menschen sehr viel Geld mit Entwicklungen im digitalen Sektor und niemand möchte mehr ohne smarte Unterstützung leben – weder in der Produktion noch im Finanzbereich oder im Controlling, geschweige denn in Medizin, Bau und Verkehr und dem Sektor der Wissensvermittlung. Wohin uns diese Reise führen soll, müssen wir uns endlich überlegen und darauf zugeschnittene rechtliche Regelungen und Gesetze formulieren.

Text: Katja Deutsch

FAKTEN

Elon Musk wurde am 28. Juni 1974 in Südafrika geboren. Mit acht Jahren las er die gesamte Encyclopedia Britannica, mit 14 Jahren „Per Anhalter durch die Galaxis", um Antworten auf existentielle Krisen zu finden. 1995 gab ihm sein Vater 28.000 Dollar für sein erstes Unternehmen (Zip2), das er vier Jahre später für 22 Millionen Dollar verkaufte. Er investierte viel Geld in paypal. 2002 verkaufte er paypal für 250 Millionen Dollar. Ob Tesla, Hyperloop, SpaceX, Solar City oder seine aktuelle Boring Company – der Entrepreneur verfolgt seine Ideen unermüdlich. Elon Musk möchte auf dem Mars sterben und dort vorher eine Million Menschen ansiedeln.

DIGICON – DAS „DIGITALE" HIGHLIGHT DES JAHRES

Foto: Alex Schelbert

Prof. Dr. Claudia Linnhoff-Popien, Inhaberin des Lehrstuhls für Mobile und Verteilte Systeme der LMU München und Veranstalterin der DIGICON

Einen Termin hat sich die digitale Elite fest im Kalender vermerkt. Am 23. und 24. November veranstaltet die Digitale Welt Academy der Ludwig-Maximilians-Universität München die DIGICON 2017.

Unter dem Leitthema „Business Intelligence" gibt es Vorträge, Podiumsdiskussionen und Wettbewerbe angefangen vom autonomen Fahren bis hin zu Predictive Analytics. „Business Intelligence benötigt man in den unterschiedlichsten Anwendungen, ob beim Online-Shopping, Radiohören oder bei neuesten wissenschaftlichen Wunderwerken", sagt Prof. Dr. Claudia Linnhoff-Popien vom Lehrstuhl Mobile und Verteilte Systeme der LMU München.

Die Teilnehmer der Digitalen Welt Convention (kurz: DIGICON) erfahren, wie man eine eigene „Business Intelligence" aufbauen kann, welche Kapazitäten bereits in dieser Disziplin stecken und was sie daraus für ihre Unternehmen lernen können.

Die Liste der Speaker umfasst eine hochkarätige Auswahl von Entscheidern, Ideengebern und Innovatoren. „Alle Firmen müssen sich dieser Situation stellen, jeder ist in der gleichen Situation. Jeder kann vom anderen lernen", freut sich die Veranstalterin Claudia Linnhoff-Popien.

Mehr zur DIGICON 2017 hier: digitalewelt magazin.de/digicon

EU-DATENSCHUTZ-GRUNDVERORDNUNG: DIE SCHONFRIST LÄUFT AB

Die neue Verordnung kommt schon bald. Mittelständler, die noch nicht darauf vorbereitet sind, sollten sich spätestens jetzt an die Umsetzung machen.

Mittelständler sollten sich auch darüber im Klaren sein, dass auch gegenüber natürlichen Personen, also Mitarbeitern oder Geschäftsführern Sanktionen vorgesehen sind.

Eine gefühlte Ewigkeit wurde über die Europäische Datenschutz-Grundverordnung (EU-DSGVO) verhandelt. Ab dem 25. Mai 2018 gilt sie nun verbindlich für alle Unternehmen in den EU-Mitgliedstaaten. Die Verordnung wird die Regelungen zur Verarbeitung personenbezogener Daten deutlich verschärfen und in der Konsequenz erhöhte Anforderungen an Unternehmen stellen.

Davon betroffen sind nicht nur international agierende Großkonzerne wie Facebook, Google, Microsoft, Amazon und Co., sondern auch kleinere Unternehmen und Mittelständler. Die meisten großen Konzerne bereiten sich bereits seit Monaten mithilfe eigener Abteilungen und/oder externer juristischer und technischer Berater auf die EU-DSGVO vor.

Bei vielen kleinen und mittelständischen Firmen besteht allerdings noch Nachholbedarf. Das mag daran liegen, dass die Verordnung für manche von ihnen eine besonders große Herausforderung darstellt – und zwar nicht nur, weil der Mai 2018 quasi schon vor der Tür steht, sondern auch, weil ein Großteil von ihnen vor dem Hintergrund der Digitalisierung bei weitem nicht auf dem neuesten Stand der Technik ist.

Da die EU-DSGVO Einfluss auf alle Prozesse im Unternehmen hat, bei denen Kundendaten gespeichert oder verarbeitet werden, müssen viele Mittelständler ihre Compliance-Maßnahmen komplett neu aufbauen. Die Anzahl und Komplexität der einzuführenden technischen und organisatorischen Maßnahmen sollte dabei nicht unterschätzt werden. Angesichts der Fülle an anstehenden Aufgaben und der wenigen noch verbleibenden Monate kann es daher sinnvoll sein, externe Berater einzubinden – zum Beispiel, wenn es darum geht, den Ist-Status zu ermitteln. Externe Berater analysieren die genutzten Verfahren, Daten und IT-Systeme und prüfen, ob diese juristisch und technisch einwandfrei und EU-DSGVO-konform sind.

Darauf aufbauend empfiehlt sich dann mit Unterstützung versierter Berater die Erstellung einer To-do- und Prioritätenliste. Die Vorgehensweise kann dazu beitragen, viel Geld zu sparen und Ärger zu vermeiden. Erhält eine Datenschutzbehörde nämlich Kenntnis über einen Verstoß bei der Nutzung kundenbezogener Daten, so hat das Unternehmen Bußgelder von bis zu 20 Millionen Euro respektive 4 Prozent des weltweiten Firmenjahresumsatzes zu zahlen. Diese Summen werden dann aufgerufen, wenn etwa ein Unternehmen das Recht auf Vergessenwerden verletzt.

Mittelständler sollten sich auch darüber im Klaren sein, dass bei einer Datenschutzverletzung künftig nicht nur das Unternehmen zur Rechenschaft gezogen werden. Vorgesehen sind auch Sanktionen gegenüber natürlichen Personen, also Datenschutzbeauftragten, Mitarbeitern oder Geschäftsführern. Im schlimmsten Fall kann ihnen eine Freiheitsstrafe drohen. Dafür muss die Belegschaft sensibilisiert werden.

Richtig vorbereitet zu sein heißt allerdings nicht nur, möglicherweise hohe Bußgelder zu vermeiden, sondern auch Vertrauen bei den Kunden zu erzeugen und damit die eigene Marke zu stärken. „Das haben wir schon immer so gemacht" gilt ab nächsten Mai also nicht mehr.

Text: Chan Sidki-Lundius

WEITERE ARTIKEL AUF:
ANALYSEBUSINESS.DE

GRUNDSÄTZLICHER WANDEL DER KULTUR-TECHNIK


Klemens Skibicki, Geschäftsführender Gesellschafter der PROFSKI GmbH

Wie weit ist der deutsche Mittelstand bei der Digitalisierung vorangekommen?

Leider ist das Verständnis für die wesentlichen Fragen des digitalen Strukturwandels einfach flächendeckend noch zu gering. Allerdings setze ich meine Hoffnung grundsätzlich voll auf den Mittelstand. Vor allem eigentümergeführte Unternehmen können eine notwendige Geschwindigkeit des Wandels erreichen, wie es in keinem Konzern möglich ist.

Ist Digitalisierung eher eine Chance oder setzt sie die KMU eher unter (Kosten-)Druck?

Wie immer: Chancen für die, die sie erkennen und ergreifen, und Druck für die, die es verschlafen. Ich halte aber nicht viel vom Schönreden – für ganz viele deutsche Unternehmen sind die Risiken größer als die Chancen, weil sie weder das Verständnis noch die Kompetenz für Daten und Software als neue wesentliche Werttreiber des digital vernetzten Zeitalters haben.

Wo sehen Sie die größten Defizite?

Im ganzheitlichen Verständnis für wesentliche Treiber des digitalen Strukturwandels. Ein Beispiel ist Social Media. Viele sehen in den Nutzern Idioten, die ihre Katzenbilder ins Internet stellen. Sie begreifen nicht, dass es sich hier um einen grundsätzlichen Wandel der Kulturtechnik handelt, wie Informationen erstellt, gefiltert und verbreitet werden – über Haustiere, aber natürlich auch über Produkte.

Rechtsberatung für den Mittelstand
Europaweit von Unternehmer zu Unternehmer

Die DIRO AG bietet als Netzwerk von Kanzleien kleinen und mittelständischen Unternehmen Rechtsberatung, die speziell auf sie abgestimmt ist – und das in ganz Europa.

Tim Wolters und Patrick Parnière,
Vorstände der DIRO AG

In diesem Jahr feiert die Europäische Union ein Jubiläum: 60 Jahre „Römische Verträge" – sie bildeten die Grundlage und den Startschuss für die EU, so wie wir sie heute kennen. In einem Europa, das bis heute wirtschaftlich immer stärker zusammenwächst, bieten sich zahllose Chancen für Unternehmen. Große Konzerne haben eigene Rechtsabteilungen oder beschäftigen in vielen Fällen Großkanzleien, um ihre immer häufiger auch grenzüberschreitenden Aktivitäten rechtlich begleiten und absichern zu lassen. Kleine und mittelständische Unternehmen scheuen sich hingegen oftmals, eine große Kanzlei für die Rechtsberatung zu beauftragen. Dabei spielt einerseits das Thema Kosten eine zentrale Rolle, aber andererseits sicher auch die Frage, wie sich die Mandanten persönlich betreut und wahrgenommen fühlen. Die DIRO AG bietet mit ihrem europaweiten Netzwerk genau das richtige Angebot für KMUs. Mittelständische Unternehmen brauchen Anwälte, die nicht nur hervorragend qualifiziert sind. Sondern ihr Geschäft verstehen und buchstäblich die gleiche Sprache sprechen. Als mittelständisch geprägtes Kanzlei-Netzwerk bieten wir individuelle Lösungen auf Augenhöhe, bei denen qualifizierte DIRO-Experten von „Unternehmer zu Unternehmer" beraten und laufend auch persönlich zur Verfügung stehen, von der Annahme bis zum Abschluss des Mandats.

Unsere Zentrale in Hamburg steuert das Netzwerk, entwickelt Angebote für Kooperationspartner und tritt als Dienstleister für die DIRO-Kanzleien im In- und Ausland auf. Insgesamt haben sich der 1992 gegründeten Allianz bis jetzt 188 Kanzleien in 25 Ländern angeschlossen. 148 davon haben aktuell ihren Sitz in Deutschland. Durch die im Markt einzigartige Kombination aus breiter regionaler Präsenz im Bundesgebiet und europaweiter Anbindung, finden die Mandanten der DIRO-Kanzleien immer passgenau den Experten, der sie persönlich und kompetent in allen relevanten Rechtsfragen berät.

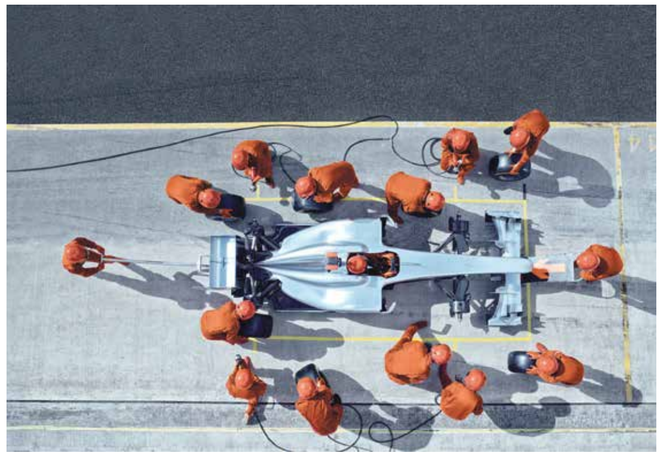
Mehr als 1500 Rechtsanwälte, Wirtschaftsprüfer, Steuerberater und Patentanwälte bürgen mit ihrem Fachwissen und ihrer Erfahrung für eine exzellente Beratung. Die DIRO-Kanzleien in Deutschland zeichnen sich durch einen besonders hohen Anteil an Fachanwälten aus. Zudem sind fast alle deutschen Kanzleien und viele im europäischen Ausland nach einem speziellen DIN ISO 9001-Standard (für anwaltliches Kanzleimanagement) zertifiziert – ein Spitzenwert im Wettbewerbsumfeld und damit weiterer Beleg für den hohen Qualitätsanspruch der DIRO AG und der mit ihr verbundenen Kanzleien.

Rechtsberatung ist und bleibt Vertrauenssache. Davon sind wir bei der DIRO überzeugt. Unsere Präsenz vor Ort sichert in jeder Hinsicht kurze Wege für die Mandanten und neben qualifizierter Beratung zu einem attraktiven Preis-Leistungs-Verhältnis auch eine echte „Chefbetreuung". Und das nicht nur in Deutschland. Die DIRO AG bietet ein europaweites Kanzlei-Netzwerk, auf das Unternehmen jederzeit zurückgreifen können. Noch aber sind gerade auch viele Mittelständler zurückhaltend, was die geschäftliche Expansion in Europa betrifft. Die Gründe dafür sind vielfältig – andere Sprachen und Arbeitsweisen sowie zum Teil gänzlich andere Rechtssysteme.

Die DIRO AG unterstützt diese Unternehmen dabei, Chancen und Potentiale zu nutzen. Unser Netzwerk verfügt über einen ganz entscheidenden Wettbewerbsvorteil: Neben den 148 Kanzleien in Deutschland sind wir auch mit aktuell 40 Kanzleien in insgesamt 25 Ländern Europas vertreten. In allen internationalen DIRO-Kanzleien wird dabei auch Deutsch gesprochen.

Bei unseren Kanzleien erhalten die Mandanten immer genau die Beratungsleistung, die gerade auch im Hinblick auf ein geschäftliches Engagement im Ausland individuell benötigt wird – vom Steuer- und Gesellschaftsrecht, über das Marken- und Urheberrecht bis hin zu juristischen Spezialthemen wie etwa der Umsetzung der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO), die im Mai 2018 endgültig in Kraft treten wird.

Mit aktuell 188 Kanzleien in 25 Ländern zählt die DIRO AG zu den größten, unabhängigen Netzwerken auf dem deutschen Markt sowie zu den führenden Kanzlei-Allianzen Europas. Die insgesamt rund 1.500 Rechtsanwälte, Steuerberater, Wirtschaftsprüfer und Patentanwälte sind Spezialisten auf den unterschiedlichsten Gebieten. Aus aktuellem Anlass, der Einführung der neuen EU-Datenschutz-Grundverordnung kurz EU-DSGVO, zwei DIRO-Experten im Interview.



Dr. Eric Heitzer,
Rechtsanwalt und Fachanwalt für IT- und Datenschutzrecht in der DIRO-Kanzlei Daniel, Hagelskamp & Kollegen, Aachen

Dr. Jens Eckhardt,
Rechtsanwalt und Fachanwalt für IT-Recht Datenschutz-Auditor (TVÜV), Compliance-Officer (TÜV), DIRO-Kanzlei Derra, Meyer & Partner, Ulm

Spätestens seit dem Diesel-Skandal bei VW wird viel über Compliance diskutiert – was können die KMUs unternehmen, um den speziellen Herausforderungen gerecht zu werden?

Dr. Jens Eckhardt:
Der erste Schritt für jede Compliance ist, sich der Aufgaben anzunehmen und die Bereiche zu identifizieren, in denen rechtliche Anforderungen bestehen. Es gibt Kernbereiche, die jedes Unternehmen betreffen. Das sind etwa – beispielsweise, aber nicht ausschließlich – das Steuer- und Datenschutzrecht. Daneben gibt es Bereiche, die nur für bestimmte Branchen oder Unternehmen gelten. Darüber hinaus gibt es aber auch Bereiche, die für bestimmte Rechtsverstöße prädestiniert sind, wie Korruption und Bestechlichkeit. Ausgehend von der Identifikation werden die Handlungsfelder priorisiert und unterschiedliche Maßnahmen ergriffen.

Welche Modelle der Beratung gibt es durch Sie und die DIRO AG?

Dr. Eric Heitzer:
Die DIRO-Kanzlei Daniel Hagelskamp & Kollegen übernimmt seit Jahren im Bereich Compliance für Unternehmen verschiedenster Branchen die Aufgaben externer Beauftragter. Der ursprüngliche Kernbereich Korruptionsbekämpfung und Kartellrechtskonformität ist dabei seit einiger Zeit um das Thema Datenschutz erweitert worden. Ich kenne mittlerweile kein Unternehmen, welches nicht auch diesen Bereich besonders adressiert. In diesem Zusammenhang gestalten wir in Abstimmung mit den Unternehmen auch die internen Regelungen etwa in Form von Unternehmensrichtlinien zum Datenschutz, Korruptionsvermeidung, etc.

Das DIRO-Netzwerk verzahnt in einzigartiger Weise das Know-how der einzelnen DIRO-Kanzleien in ganz Europa. Beispiel: Sie sind ein deutsches Unternehmen und beliefern ihre Auslandstöchter in Ungarn und der Slowakei. Ihre Vorgaben an ein integres Verhalten – etwa das Verbot von Schmiergeldzahlungen – sollten dann auch noch jenseits des Schlagbaums gelten. Das stellen wir sicher durch Einbeziehung von Partnerkanzleien – falls nötig in ganz Europa. Diese etablieren Compliance vor Ort unter Berücksichtigung der vielfältigen nationalen Besonderheiten und Anforderungen in den einzelnen Mitgliedstaaten.

Auch das Thema IT Sicherheit ist in den Schlagzeilen. Die neue EU-Datenschutzgrundverordnung (EU-DSGVO) kommt in Kürze, welche Herausforderungen bedeutet das für die anwaltliche Seite?

Dr. Jens Eckhardt:
Die Herausforderung für uns Rechtsberater besteht darin, einen Schritt voraus zu sein in Bezug auf die Aufarbeitung und das Verständnis der Anforderungen der EU-DSGVO. Gerade die praktische Umsetzung dieser Verordnung erfordert nicht nur ein Verständnis für Einzelfragen des Datenschutzrechts. Die Umsetzung erfordert vielmehr ein Verständnis für das Gesamtmodell bzw. den Ansatz der EU-DSGVO. Dies ergibt sich gerade nicht nur aus einer einzelnen Norm, sondern ist das Ergebnis einer umfassenden Gesamtbetrachtung der Regelungen. An dieser Stelle setzt eine professionelle Rechtsberatung an.

Dr. Eric Heitzer:
Unternehmen, die in mehreren Mitgliedstaaten der EU tätig sind, stehen vor der Herausforderung nicht nur die europäischen Vorgaben ab dem 26. Mai 2018 unmittelbar beachten zu müssen, sondern zusätzlich die nationalen Umsetzungsmaßnahmen, die in den Mitgliedstaaten sehr unterschiedlich ausgefallen sind. Dies wirkt sich an vielen Stellen aus, etwa bei der Frage, welche Aufgaben der Datenschutzbeauftragte in Deutschland, Polen oder Griechenland wahrzunehmen hat. Hier kommt unser DIRO-Netzwerk ins Spiel: Auf Basis der europäischen Verordnung können wir über die DIRO die Einzelanforderungen in den einzelnen Mitgliedstaaten genau benennen, so dass eine effiziente Umsetzung der neuen Datenschutzregeln nach europäischem und nationalem Recht erfolgt.

Mehr Informationen zum DIRO-Netzwerk finden Sie unter: diro.eu

Kontakt:
DIRO AG
Große Bleichen 32
20354 Hamburg
Tel.: +49 (0)40 413522 31
E-Mail: diro@diro.eu

DIRO
VIELE KANZLEIEN. EIN STARKES TEAM.

DIGITALE ZUKUNFT IM YEAR OF THE X

Mit seinen Innovationskonferenzen „Year of the X“, die jedes Jahr ein Tier anstelle der Variablen „x“ im Titel tragen, gibt Markus von der Lühe der digitalen Community wichtige Impulse.

Foto: FOTOGRAFIE Eva-Elisabeth Schneider, evaphoto.com

Herr von der Lühe, wie kann „Year of the X“ helfen, den Bedarf an Führungskräften und Mitarbeitern mit hoher Reflexionsfähigkeit und Mut zum Wachstum im digitalen Zeitalter zu decken?

Unser Anspruch ist es, das Mindset im digitalen Zeitalter zu verändern. In der digitalen Welt brauchen wir flache Hierarchien, Agilität, maximale Autonomie für Mitarbeiter und ein neues Bildungssystem, das Skills wie Flexibilität und emotionale Intelligenz fördert.

Meist sind Fachkongresse und -veranstaltungen ja ziemlich theorielastig. Wir groß ist der Praxisbezug bei „Year of the X“?

Unsere Workshops sind extrem interaktiv: Wir bieten Themen an wie Growth Hacking und Digital Products Accelerator und vieles mehr, wo wir interaktiv digitale Kompetenzen, aber auch Softskills wie emotionale Intelligenz vermitteln. Außerdem haben wir eine Touch Tech Area, wo man neue Gadgets ausprobieren kann.

> „Wir haben uns für Community entschieden – ein ganz zentraler Bestandteil, wenn wir über Digitalisierung sprechen, denn wir bewegen uns weg von geschlossenen Systemen hin zu mehr offenen Ökosystemen. Kollaboration, Co-Creation und Community werden immer wichtiger.“

Welches sind die größten Fehler, die unerfahrene Unternehmen bei der digitalen Umstellung von Arbeitsprozessen am häufigsten machen?

Sie haben keinen Buy-in von ganz oben und glauben, dass sie den Change-Prozess alleine gewuppt bekommen. Sie stellen Prozesse um, ohne diese kulturell über Change Management und Mindset Change verankert zu haben.

„Year of the Monkey“ oder „Year of the Dog“ sind als Bezeichnungen für so ein Event schon ungewöhnlich. Wie ist es zu der Idee gekommen?

In der Digitalisierung bewegen wir uns mit Lichtgeschwindigkeit in die Zukunft. Für uns war es wichtig, dass wir eine Marke kreieren, die Change in der DNA hat, und da hat sich das chinesische Horoskop sehr gut angeboten. Wir müssen uns selbst jedes Jahr verändern und einen neuen Narrativ konstruieren, der die jeweils aktuellen Trends repräsentiert.

Welche Kriterien gelten für die Auswahl der Speaker?

Unkonventionell, in die Zukunft gerichtet, cool und international.

Wie ist denn überhaupt die Atmosphäre bei „Year of the X“, welche Nebenschauplätze gibt es und wie setzt sich das Publikum zusammen?

Beim letzten Festival war es ja das „Year of the Rooster“ und wir entschieden uns für eine US-Farm aus den 50er-Jahren als Design für die Location. Da kamen dann viele im Cowboy-Outfit mit Hüten, es gab eine Country-Rockband und viele bunte Charaktere.

Was steht beim Event „Year of the Dog“ 2018 im Fokus?

Wie immer rankt sich das Festival um Innovation und Digitalisierung. Als Emblem haben wir Schäferhunde gewählt. Die sind loyal und halten das Rudel zusammen. Deshalb haben wir uns für Community entschieden – ein ganz zentraler Bestandteil, wenn wir über Digitalisierung sprechen, denn wir bewegen uns weg von geschlossenen Systemen hin zu mehr offenen Ökosystemen. Kollaboration, Co-Creation und Community werden immer wichtiger.

Die Entwicklung der Digitalisierung läuft in einem atemberaubenden Tempo. Lassen sich konkrete Entwicklungen für die kommenden zwei Jahre überhaupt voraussagen?

Die Automatisierung wird weiter voranschreiten und die Arbeitslandschaft nachhaltig verändern. Das wird auch Ärzte, Anwälte und Manager betreffen. Autos werden im Zuge des autonomen Fahrens ihre Status-Funktion weitgehend verlieren und mehr und mehr zu Utilities.

Die Digitalisierung birgt auch große Gefahren. Welchen Stellenwert hat dieses Thema bei „Year of the X“?

Wir gehen die Gefahren konstruktiv an: so bieten wir z. B. einen „How to become a hacker“-Workshop an, wo ein erfahrener Hacker den Teilnehmern zeigt, wie man z. B. Passwörter hacken kann. Wir gehen gemeinsam ins „Darknet“ und nehmen den Teilnehmern so die diffusen Ängste, indem wir ihnen konkret zeigen, was die Gefahren sind, aber dann auch gleich Lösungen für diese Gefahren vorschlagen.

Text: Helmut Peters

WIE SKY INNOVATIONS-TREIBER BLEIBEN WILL


Mareike Lassner, Senior Projektmanagerin von „Play“


Auch Netflix und Amazon zeigen Serien, produzieren selbst und steigen jetzt sogar in die Bundesligaberichterstattung (Amazon) ein. Sky Deutschland will weiterhin kräftig dagegenhalten und seine Vormachtstellung als innovatives Medienunternehmen behaupten. Innovationskraft verspricht sich der Sender auch vom Play Innovation Hub, der vor einem Jahr gegründet wurde. Sky nimmt viel Geld in die Hand, um über den Hub außergewöhnliche Ideen zu fördern. „Open Innovation gibt uns kreativen Raum für unterschiedliche Perspektiven, andere Gedanken und neue Ideen. Es ist wichtig, dies auch losgelöst vom Kerngeschäft tun, mit einem gewissen Freiraum. Wir suchen aber nicht nur extern nach innovativen Ideen, sondern auch intern von Sky Mitarbeitern“, so Mareike Lassner, die Senior Projektmanagerin von „Play“.

Bewerben kann sich im Prinzip jeder, der eine innovative Idee für das Entertainment von morgen hat. Im ersten Schritt müssen die Bewerber in fünf Minuten eine Jury überzeugen. Danach haben sie Zeit, um Prototypen und Produktversionen zu entwickeln. Die Startups und Ideengeber erhalten 25 000 Euro als Kompensation. „Wir sind sehr zufrieden mit der Entwicklung unserer Startups. Sowohl die externen als auch die internen Ideen weisen großes Potenzial auf. So hat es etwa mit dem Projekt CustomerLED eine Idee eines Sky-Mitarbeiters gleich aus unserer ersten Runde vollumfänglich in das operative Tagesgeschäft von Sky geschafft.“

Bewerber können sich jetzt schon für den nächsten Pitch am 13. November 2017 unter www.play-hub.de anmelden.

FAKTEN

Seit 2015 gibt es in München ein Digital-Festival, bei dem die digitale Transformation und Innovation im Mittelpunkt stehen. Internationale Speaker informieren in Vorträgen, Workshops, aber auch anhand praktischer Beispiele über neue Trends und Denkansätze der Digitalwirtschaft. Das Event öffnet sich Vertretern aus Business und Kultur gleichermaßen.

SPRACHSTEUERUNG UND VERNETZUNG WAREN DIE IFA-TRENDS

Hans Joachim Kamp (gfu) zieht ein IFA-Fazit.


Quelle: Messe Berlin

Hans-Joachim Kamp, gfu Aufsichtsratvorsitzender, zu den Trends der IFA.

> „Ohne Digitalisierung und technische Innovationen werden wir dieser wohl größten Herausforderung für die Menschheit, dem Klimawandel, nicht begegnen können.“

Herr Kamp, welche Trends sind im Rückblick auf die diesjährige IFA im Rahmen der Digitalisierung, die inzwischen in viele Lebensbereiche eingreift, die spannendsten?

Die Digitalisierung macht vor kaum einem Lebensbereich mehr halt. Dies betrifft beide Segmente der IFA, Consumer Electronics und Home Appliances. Sie wachsen nicht zuletzt durch die Digitalisierung mehr und mehr zusammen. Besonders spannend: Digitale Vernetzung bedeutet heute viel mehr als nur den Austausch von Daten. Künstliche Intelligenz sorgt dafür, dass Systeme „mitdenken“ und Gerätefunktionen automatisch an die Bedürfnisse ihrer Nutzer anpassen.

Welche Trends werden denn unsere Zukunft bestimmen?

Einerseits setzen die klassischen Produktbereiche Trends. Dazu gehören zum Beispiel bei Consumer Electronics ultraflache TV-Bildschirme, die nahtlos mit der Wand verschmelzen, HiFi-Komponenten für Musik in extrem feiner Auflösung und Kameras für 360-Grad-Videos. Die Trends bei den Hausgeräten reichen von smarten und vielseitigen Funktionalitäten über Ressourcenschonung, Energie-Effizienz, Nachhaltigkeit sowie komfortable, einfache und individualisierbare Nutzung. Weitere große Themen sind Sprachsteuerung, Robotik und natürlich die umfassende Vernetzung in allen Produktbereichen. Vom Smartphone oder vom Auto kennt man die Sprachsteuerung bereits. Nun gibt es eine Vielzahl sprachgesteuerter Apps, die Consumer-Electronics-Produkte und auch immer mehr Hausgeräte steuern. Dazu gehören beispielsweise die Heizung, die auf Zuruf reagiert und die gewünschte Temperatur einstellt, Kaffeemaschinen, die auf Sprachbefehl ein Wunschgetränk zubereiten oder Jalousien, die auf Sprachbefehl in die gewünschte Position fahren. Fast überall sind die digitalen Helfer einsetzbar, um die Wohn- und Lebensqualität zu erhöhen. Sie sind sogar selbstlernend und erkennen Gewohnheiten der Benutzer.

Welchen Sinn hat das Ganze? Sind das nicht einfach Gimmicks, die Spielkram für Erwachsene sind?

Auf den ersten Blick scheint das vielleicht so zu sein. Aber schauen Sie sich die großen Herausforderungen für die Zukunft an. Eine große Bedrohung ist der Klimawandel. Ohne Digitalisierung und technische Innovationen werden wir dieser wohl größten Herausforderung für die Menschheit nicht begegnen können. Smart Homes steigern einerseits den Komfort und erleichtern das Leben, sie dienen aber auch der Ressourceneffizienz und der Einsparung von Energie und CO_2.

Wenn wir über Vernetzung sprechen, dann ist Datenschutz ein wichtiges Thema …

An vernetzte Produkte der Consumer Electronics stellen wir dieselben Sicherheitsanforderungen wie an alle anderen Geräte, die mit dem Internet verbunden sind. Es ist bekannt, was Cyberkriminelle anrichten können, wenn sie in ein System eindringen. Der Industrie ist dieses Thema selbstverständlich bekannt und die Hersteller sind sich ihrer Verantwortung bewusst. Stets wachsender Komfort und wirksamer Schutz der Privatsphäre sind also kein Gegensatz.

Text: Frank Tetzel

WEITERE ARTIKEL AUF:
ANALYSEBUSINESS.DE

IT-FACHKRÄFTE TRAGEN BESONDERE VERANTWORTUNG

Sie werden überall gesucht und notfalls aus dem Ausland eingesetzt: Software-Entwickler und Programmierer gehören zu den begehrtesten Experten. Leicht zu finden sind sie nicht.

An etlichen Universitäten und Hochschulen werden Module wie „Cyber War" unterrichtet, wo Studierenden die Arbeitsweise von Geheimdiensten veranschaulicht wird.

Viele Unternehmen auch jenseits der klassischen IT-Branche implementieren digitale Lösungen in ihre Geschäftsabläufe, Produktionen, Warenwirtschafts- und Kommunikationssysteme sowie ihre Finanzhandlungen. Doch jemanden zu finden, der diese riesigen Datenmengen programmiert und steuert und sie in die richtigen Bahnen lenkt, wird zunehmend zum Problem. Die Nachfrage nach Programmierern ist ungebrochen und steigt durch die Ausbreitung des Internet der Dinge weiter an.

Dabei haben vor allem Unternehmen jenseits der Ballungszentren große Probleme, Software-Entwickler, IT-Projektmanager und Systemadministratoren zu finden. Doch müssen diese Spezialisten überhaupt zwangsweise im Unternehmen vor Ort agieren? Bei Programmierern beispielsweise ist das schon lange nicht mehr der Fall.

Denn Programmieren ist eine klassische Outsourcing-Industrie, bei der sich die Gehälter mittlerweile länderübergreifend auf relativ hohem Niveau angeglichen haben. Konnte man vor einigen Jahren noch für Monatsgehälter von unter 2.000 Euro auf Fachkräfte beispielsweise aus dem Baltikum zurückgreifen, so verlangen diese heute den gleichen Stundensatz wie einheimische Profis. Mittlerweile wird jeder genommen, der nur irgendwie programmieren kann. Dabei lässt sich ein großer Unterschied zwischen einem exzellent ausgebildeten Programmierer und einem, der mit Mühe sein Studium geschafft hat, bemerken. Erstgenannter leistet das Zehnfache – bekommt aber nur ungefähr das doppelte Gehalt.

Warum dann nicht in aufstrebenden Ländern mit Millionen IT-Absolventen suchen?

Auch das scheint nicht so einfach zu sein, denn hier muss in Ländern mit einem oft ganz anderen Rechtsspielraum eine gut eingespielte Organisation aufgebaut werden. Deshalb raten Experten dazu, gerade beim Outsourcing unbedingt auf die Qualität der Verträge zu achten.

Gesucht werden gründlich arbeitende, gewissenhafte Menschen mit hervorragenden handwerklichen Fähigkeiten und hohem Verantwortungsbewusstsein, die besonders sichere Software-Entwicklung im Fokus haben. Denn viele Geräte des IoT werden preisgünstig im asiatischen Raum produziert und sind erschreckend ungesichert, dabei jedoch voll internetfähig – können also relativ einfach gehackt werden und dank Botnetzen riesigen Schaden anrichten. Vorbeugen könnte man relativ einfach durch das Programmieren eines sicheren Codes. Die Gefahr lauert nämlich bereits beim Login: Ist diese Zeile schlecht geschrieben, kann ein möglicher Angreifer in der Datenbank landen und hat hier leichtes Spiel.

Der Kampf um die Most Wanted wird zusätzlich durch die Bundeswehr angetrieben, die gerade mit allen Mitteln versucht, ihre Cyberkräfte von derzeit einigen Hundert Mitarbeitern auf knapp 14 000 zu erhöhen. An etlichen Universitäten und Hochschulen werden deshalb auch Module wie „Cyber War" unterrichtet, wo Studierenden die Arbeitsweise von Geheimdiensten veranschaulicht wird. In der IT-Ausbildung wird es immer wichtiger, Menschen auszubilden, die neben hervorragenden handwerklichen Fähigkeiten auch Verantwortung und ein Bewusstsein für Sicherheit entwickeln.

Text: Katja Deutsch

3 FRAGEN AN DR. GERD BEUSTER

Prof. Dr. Gerd Beuster, Dozent für IT-Sicherheit an der Fachhochschule Wedel

Was umfasst der Studiengang IT-Sicherheit der FH Wedel?

Wir bieten das Studium IT-Sicherheit in einem 3-semestrigen Master-Studiengang an. Der Fokus liegt auf den Bereichen Security Engineering und Security Management. In den Lehrveranstaltungen geht es zum einen um die technischen Aspekte der Entwicklung und des Betriebs sicherer IT-Systeme sowie zum anderen um die Gestaltung und Umsetzung organisatorischer IT-Sicherheitsmaßnahmen im Unternehmenskontext. Darüber hinaus beinhaltet das Studium Workshops zu Kryptographie, Webapplikationssicherheit und Netzwerksicherheit. In Kleingruppen bearbeiten die Studierenden zudem ein IT-Sicherheitsprojekt und schreiben ihre Thesis zu einem Thema der IT-Sicherheit.

Wie steht es um Studiengebühren und nötige Vorkenntnisse?

Voraussetzung ist ein guter Bachelor-Abschluss in Informatik oder einem ähnlichen Studiengang. Die Studiengebühren betragen 1 980 Euro pro Semester.

Wie sind die Berufsaussichten, in welchen Berufsfeldern?

Der Bedarf an IT-Sicherheits-Experten übersteigt die Anzahl der Absolventen deutlich. Kein Unternehmen kommt heute ohne IT aus, und kein Unternehmen mit IT kann auf IT-Sicherheit verzichten. Daher stehen unseren Absolventen alle Branchen und Unternehmen offen, vom Startup bis zum Großkonzern.

„WANNACRY“: EKLATANTE ZUNAHME VON CYBERANGRIFFEN

Der 12. Mai 2017 war zunächst einmal ein ganz normaler Tag. Während Bundeskanzlerin Merkel über Steuerentlastungen sprach, sich die Finanzminister der G7-Staaten im italienischen Bari trafen und das Statistische Bundesamt meldete, dass das Bruttoinlandsprodukt um 0,7 Prozent im Vergleich zum Vorjahreszeitraum zugelegt hatte, fraß sich ein Computervirus durch das weltweite Netz. Reisende auf deutschen Bahnhöfen wunderten sich, dass die Anzeigetafeln der Bahn nicht mehr funktionierten.

fotomek.com - stock.adobe.com

Die Schöpfer des Virus hatten eine Sicherheitslücke in alten Windows-Systemen entdeckt und den Virus dort eingeschleust.

Doch dies war eine der geringeren Folgen. Nahezu weltweit traf dieser Cyberangriff global agierende Unternehmen. So war der spanische Konzern Telefónica genauso betroffen wie die brasilianische Vivo oder die Autobauer Renault und Nissan, der britische National Health Service, das russische Innenministerium oder der chinesische Ölkonzern Petro China, wo an 20 000 Tankstellen die Kartenzahlung versagte und die Kunden nur noch mit Bargeld zahlen konnten. WannaCry wurde der Virus genannt, der sich selbstständig – ohne fremdes Zutun – verbreitete und mit einer Erpressungssoftware gekoppelt war, die die befallenen Rechner nur wieder freigab, wenn man eine entsprechende Summe in der Kryptowährung Bitcoin zahlte. Weltweit waren rund 300 000 Rechner betroffen.

Die Schöpfer des Virus hatten eine Sicherheitslücke in alten Windows-Systemen entdeckt und den Virus dort eingeschleust. Pikanterie am Rande: Das Sicherheitsrisiko war längst bekannt. Der amerikanische Geheimdienst NSA hatte das Leck entdeckt, aber nicht bekannt gemacht und wahrscheinlich sogar selbst für eigene Zwecke genutzt. Microsoft erfuhr im Frühjahr dieses Jahres von den Schwachstellen, worauf das amerikanische Unternehmen aus Redmond zum Schließen des Risikos schnell ein Update zur Verfügung stellte. Doch längst nicht alle Nutzer hatten ihre IT-Systeme aktualisiert, was den Angriff ermöglichte. Die zunehmende Digitalisierung und damit Vernetzung macht Computersysteme anfälliger als je zuvor für Angriffe von Cyberkriminellen, aber auch von Staaten.

Das Beispiel WannaCry zeigt sehr deutlich, wie wichtig das Thema Cybersicherheit für Unternehmen ist. Vor allem regelmäßige Updates von Computerprogrammen sind dabei essenziell. Vernachlässigen IT-Abteilungen diese Aktualisierungen, kann es teuer werden: In Einzelfällen sind durch dieses Vorgehen Schäden in Millionenhöhe entstanden.

„In kleineren Firmen können womöglich aber auch einige zehntausend Euro die Existenz gefährden“, erläutert der Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Arne Schönbohm. Allerdings werde man die Kompromittierung eines einzelnen Computers nicht immer verhindern können, aber sie dürfe nicht zum Ausfall eines ganzen Netzwerks führen. Informationssicherheit müsse zur Chefsache gemacht werden.

„Nur zwei Monate nach ‚WannaCry‘ stiftete der Virus ‚NotPeya‘ in großen IT-Netzen riesige Verwirrung.“

Cyber-Sicherheit sei die Voraussetzung für eine erfolgreiche Digitalisierung.

WannaCry war übrigens nicht der einzige Virus, der in den letzten Monaten viele Computer und Netzwerke heimsuchte. Nur zwei Monate später stiftete der Virus „NotPeya“ in großen IT-Netzen riesige Verwirrung. „Cyber-Angriffe verursachen erheblichen volkswirtschaftlichen Schaden. In einigen Unternehmen ist es zu massiven und langanhaltenden Einschränkungen der Produktion oder geschäftskritischer Prozesse gekommen“, so Schönbohm.

Text: Frank Tetzel

WEITERE ARTIKEL AUF:
ANALYSEBUSINESS.DE

Mit Vollgas in Richtung Datenschutz

Dr. Frederike Rehker, Datenschutzbeauftragte, und Florian Goldenstein, Head of IT Security bei Konica Minolta, über die Herausforderungen der EU-DSGVO.

Welche Anforderungen stellt die EU-Datenschutz-Grundverordnung an Unternehmen, die Daten von EU-Bürgern speichern?
Die EU-DSGVO leitet eine völlig neue Ära des Datenschutzrechts ein. Alle Prozesse, in denen personenbezogene Daten eine Rolle spielen, müssen neu bewertet werden. Zu beachten ist auch ein verändertes Haftungsgefüge zwischen Betroffenen, Unternehmen und deren Dienstleistern: Bei Kooperationen besteht eine gesamtschuldnerische Haftung, sodass eine Kontrolle der Partner an Relevanz gewinnt. Insgesamt drohen bei Verstößen Sanktionen in Millionenhöhe.

Welches sind die größten Herausforderungen hierbei?
Die Erfüllung erweiterter Betroffenenrechte, das Erarbeiten von Konzepten zur Datenlöschung sowie die Beachtung des Grundsatzes „Privacy by Design“ bei der Entwicklung neuer Produkte verlangen Unternehmen einiges ab. Eine weitere Herausforderung stellen veraltete Infrastrukturen dar. Die EU-DSGVO fordert Sicherheitsmaßnahmen nach „Stand der Technik“. Dazu gehören etwa belastbare Abwehrmechanismen gegen Attacken, Antiviren- und Antimalware-Software sowie strenge Identifizierungs- und Authentifizierungsmechanismen. Kommunikationswege müssen verschlüsselt sein. Eine Next-Generation-Firewall und ein IT-Governance-Konzept sind nun ein Muss.

Mit welchen Problemen kämpfen Unternehmen?
Die Bewältigung der Abweichung zwischen Ist und Soll der datenschutzrechtlichen Anforderungen ist ein Kraftakt. Innerhalb eines jeden Unternehmens muss eine tiefgreifende Sensibilisierung für das Thema Datenschutz erfolgen, die sich in einer veränderten Unternehmenskultur widerspiegelt. Die Erfüllung von Betroffenenrechten, insbesondere des Anspruchs auf Datenlöschung und des „Rechts auf Vergessen“, ist mit Sicherheit eine große technische und organisatorische Herausforderung. Betroffen ist nicht nur die eigene Datenverarbeitung, sondern auch die aller Dienstleister und Partner, die solche Informationen verarbeiten. Auch die Cloud ist eine Herausforderung. Fakt ist: Wenn ein Unternehmen Daten in eine Public Cloud ablegt, ist es für diese verantwortlich.

Was müssen Unternehmen jetzt tun, um die Anforderungen bis Mai 2018 umzusetzen?
Das hängt natürlich von der Branche des Unternehmens und der Menge sowie der Art verarbeiteter personenbezogener Daten ab. Ein mittlerer Handwerksbetrieb hat sicherlich einen überschaubareren Aufwand als der Betreiber eines Online-Shops. Als Faustregel gilt: Je mehr Prozesse digital ablaufen, desto aufwändiger ist die Umsetzung des Datenschutzes. Vielen Unternehmen ist nicht klar, wie viele Prozesse betroffen sind. Die Umsetzung bis Mai 2018 erfordert eine strukturierte Vorgehensweise. Wer bis heute noch nicht angefangen hat, sollte jetzt Vollgas geben, am besten mit externer Unterstützung.

Wie unterstützt Konica Minolta Unternehmen hierbei?
Wir bieten das gesamte Portfolio: Angefangen bei einer Ist-Analyse unserer zertifizierten Consultants über die daraus resultierenden „to dos“ unter Erstellung einer Prioliste bis hin zur Unterstützung bei der Umsetzung. Dabei ist zu berücksichtigen, dass alle Abteilungen betroffen sind, die mit personenbezogenen Daten umgehen. Die Datenverarbeitung mit Subunternehmen ist zu prüfen. Im Bereich unserer Multifunktionssysteme unterstützt Konica Minolta mit einem großen Angebot an Dienstleistungen, wie mit speziellen Apps, Einstellungsmöglichkeiten und der sicheren Datenlöschung bei Rückgabe. So profitieren Kunden von einem umfangreichen Paket an Lösungen.

Wer prüft denn Vergehen gegen das Gesetz und wie realistisch sind die hohen Bußgeld-Auflagen?
Neben der Verhängung von drastischen Bußgeldern durch die Aufsichtsbehörden verfügen auch Betroffene, Verbraucherverbände und Datenschutzvereine über erweiterte Rechte. Wir sehen es als realistisch an, dass die Verhängung von abschreckenden Sanktionen erfolgen wird.

Florian Goldenstein,
Head of IT Security bei Konica Minolta

Der Datentisch bei G DATA in Bochum kann weltweite digitale Bedrohungen anzeigen.

Hauptstadt der Cyber-Sicherheit

Bochum hat sich mit einem Drei-Säulen-Modell zum wichtigsten Standort der IT-Sicherheitsbranche gemausert. Eine Entwicklung, die viel Potenzial birgt.

Frage: Welche Stadt ist Deutschlands Hauptstadt der IT-Sicherheit – Hamburg, München oder Berlin? Antwort: Bochum. Was für den Laien vielleicht erstaunlich klingen mag, ist für Experten überhaupt keine Überraschung. Bochum, die 370 000-Einwohner-Stadt mitten im Ruhrgebiet, hat sich in den vergangenen Jahren zum Zentrum für alles das entwickelt, was mit der Sicherheit von Computerdaten zu tun hat. Mit Unternehmen wie dem Erfinder des Antivirus, G DATA, mit innovativen Start-ups und mit dem Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum (HGI), das weltweit eine der führenden Institutionen für Cybersicherheit ist, hat sich mitten im Ruhrgebiet ein Cluster gebildet, wie es ihn sonst in Deutschland nicht gibt. „Als Ausbildungsstandort für IT-Sicherheitsexperten ist Bochum sogar die Nummer 1 in Europa“, sagt Thorsten Holz, Professor für Systemsicherheit am HGI. Mehr als die Hälfte aller deutschen Experten wird hier ausgebildet.

Der Standort Bochum habe einfach alles, was es braucht, findet Thomas Wollinger, Geschäftsführer bei ESCRYPT, einem Unternehmen, das sich auf IT-Sicherheit für eingebettete Systeme, zum Beispiel in Autos, spezialisiert hat. „Es gibt hier eine sehr gute Ausbildungssituation, eine starke Konzentration von Experten und Unternehmen sowie von jungen Start-ups, die mit ihren innovativen Ideen dafür sorgen, dass wir hier immer am Puls der Zeit sind.“ Professor Christof Paar, Direktor des HGI, spricht von den drei Bochumer Säulen: Spitzenwissenschaft, Vernetzung zur Wirtschaft und Ausbildung. Und er lobt die „äußerst agile Wirtschaftsförderung“. Sie fördere bewusst die Unternehmen der Branche und unterstütze Start-ups durch Beratung und die Bereitstellung von Infrastruktur und Räumen im eigens gegründeten Zentrum für IT-Sicherheit. Gefördert werde auch ein enger Kontakt zwischen Start-ups, Unternehmen und Wissenschaftlern.

Die Nähe von Wissenschaft und Wirtschaft ermöglicht es Start-ups, sich vor Ort direkt aus dem HGI auszugründen. 16 solcher jungen Unternehmen gibt es in Bochum inzwischen. ESCRYPT ist ein Beispiel, das den Erfolg zeigt. Das Unternehmen gründete sich 2004 aus dem HGI aus und hat heute Standorte in 15 Ländern weltweit. Doch auch wenn ESCRYPT inzwischen ein Unternehmen der Bosch-Gruppe, von Bochum in die weite Welt ausgreift, so betont Wollinger: „Wir sind gerne hier, nutzen die Vorteile des Standorts und werden auch vor Ort weiterwachsen.“

Auch Kai Figge, Gründer und Vorstand von G DATA, sieht Bochum als den richtigen Standort für sein Unternehmen, das vor 30 Jahren hier als erstes weltweit einen Antivirenschutz entwickelte. Besonders freut es ihn, dass sich Bochum als Ausbildungsstandort einen exzellenten Ruf erarbeitet hat. Figge: „Auf dem Campus trifft man Headhunter aus dem Silicon Valley, die neue Leute für Facebook, Google und Co suchen.“

Mehr Infos zum Standort Bochum:
www.bochum-wirtschaft.de

Ralf Meyer, Geschäftsführer der Bochum Wirtschaftsentwicklung

Interview mit Ralf Meyer

Welche Bedeutung hat die IT-Sicherheitsbranche für Bochum?

Meyer: Für die Stadt spielt diese Branche eine sehr wichtige Rolle. Sie ist das einzige Alleinstellungsmerkmal, das Bochum hat. So etwas wie das Horst-Görtz-Institut, das weltweit führend ist in der Kryptologie-Branche, und das IT-Sicherheits-Unternehmen G DATA sowie alle Unternehmen und Start-ups, die sich hier angesiedelt haben, findet man sonst in keiner Stadt. Nicht zuletzt sind wir der größte Standort für die Ausbildung von IT-Sicherheitsexperten in Deutschland – die Hälfte aller deutschen Fachleute wird in Bochum ausgebildet.

Wie unterstützt die Stadt Bochum die Branche?

Das tun wie mit einer ganzen Reihe von Maßnahmen. Wir haben beispielsweise ein Zentrum für IT-Sicherheit gegründet, in dem sich Unternehmen und Start-ups ansiedeln und Projekte durchführen können. Auch sonst stellen wir Infrastruktur zur Verfügung. Zum Beispiel wird Bochum 2018 durch das Projekt Gigabit City Deutschlands erste Großstadt mit einem flächendeckenden Gigabit-Internet sein. Und Bochum bewirbt sich derzeit auch um die Ansiedlung eines weiteren Instituts für IT-Sicherheit. Das wird die Strahlkraft weiter erhöhen.

Welche Rolle spielen Start-ups?

Eine sehr große – und sie wird weiterwachsen. Wir bieten deshalb bei Ausgründungen aus dem Horst-Görtz-Institut Beratung und finanzielle Unterstützung an. Derzeit arbeiten wir auch an einem speziellen Beteiligungsfonds für Start-ups in der IT-Sicherheit.

Was bietet Bochum sonst noch?

Wir haben hier eine große Konzentration von IT-Sicherheitsexperten. Das macht die Stadt für Unternehmen, die sich neu gründen oder eine neuen Standort suchen, sehr interessant. Aber man sollte auch nicht vergessen, dass Bochum in der Mitte des Ruhrgebiets mit seinen 5,5 Millionen Einwohnern liegt. Das bedeutet: Hier ist auch neben der Arbeit viel los – wir sind die größte Party Deutschlands.