SICHERHEIT IN DEUTSCHLAND

Einbrüche, Datenklau, Terrorakte: Die Zeiten scheinen immer unsicherer zu werden – für Privatpersonen und Unternehmen gleichermaßen. Wie sieht es tatsächlich aus? Über Fakten und Strategien tauschten sich Experten beim RP-Wirtschaftsforum „Sicherheit in Deutschland" aus.

VON JÜRGEN GROSCHE

In Manchester sterben viele vor allem junge Menschen durch eine Bombe. Der Cyberangriff „Wanna Cry" legt weltweit Rechner lahm. Und in München wird eine europaweit tätige Einbrecherbande erwischt, die für jeden fünften Einbruch in Deutschland verantwortlich sein soll. Alles Nachrichten aus der jüngsten Vergangenheit. Terror, Cyberattacken, Einbrüche – Privatpersonen und Unternehmen sorgen sich derzeit auf vielen Gebieten um ihre Sicherheit. Das Thema beschäftigt die Menschen und beeinflusst sogar Wahlen. Um rein emotionale Reaktionen zu vermeiden, ist es hilfreich, die Fakten anzuschauen und unterschiedliche Dimensionen des Themas zu analysieren. Es geht um Einbrüche und Überfälle, Terrorgefahren, aber auch – insbesondere für Unternehmen wichtig – um Internet- bzw. Cyberkriminalität.

All diese Aspekte standen bei der Podiumsdiskussion des RP-Wirtschaftsforums „Sicherheit in Deutschland" im Folkwang-Museum Essen im Fokus. Unter der fachlichen Leitung von Uwe Gerstenberg, Geschäftsführender Gesellschafter der consulting plus Unternehmensgruppe, konnten aus seinem Netzwerk die herausragenden Experten für das Thema Sicherheit aus ganz Deutschland für das Forum in Essen gewonnen werden. Dort befänden sich die Gäste des Forums ja „an einem der sichersten Orte der Welt", sagte Essens Oberbürgermeister Thomas Kufen augenzwinkernd, aber durchaus ernst gemeint: Das Museum beherbergt Kunstschätze von hohem Wert und ist natürlich entsprechend geschützt. Doch auch die Stadt sei – wie alle deutschen Kommunen – im weltweiten Vergleich sicher.

Der CDU-Sicherheitsexperte Wolfgang Bosbach bestätigt diese Einschätzung – ohne dabei kritische Entwicklungen außen vor zu lassen. 6,2 Millionen Straftaten weist die Statistik 2016 für Deutschland aus, „die Dunkelziffer liegt jedoch um ein Vielfaches höher". Den Behörden seien 600 Gefährder bekannt, denen man terroristische Straftaten zutraut. Und dass nur 14 Prozent der Einbrüche aufgeklärt werden und sogar nur drei Prozent zur Verurteilung kommen, macht dem Bundestagsabgeordneten ebenso Sorge wie die Erkenntnis, dass über 40 Prozent dieser Straftaten der organisierten grenzüberschreitenden Kriminalität zuzuordnen sind.

Vor diesem Hintergrund sei die Enttäuschung in der Polizei groß, dass die Politik solche Realitäten nicht wahrhaben wolle, beklagt Heinz Sprenger.

Der Autor und Dozent an der Fachhochschule Duisburg/Mülheim weiß, wovon er spricht. Er leitete die Mordkommission Duisburg und hatte die Mafiamorde aufgeklärt, bei denen am 15. August 2007 vor einer Pizzeria sechs Italiener umgebracht worden waren. „Wenn man Kriminalität erfolgreich bekämpfen will, braucht man das Personal dafür", betont Sprenger.

Erfolge sieht der Düsseldorfer Polizeipräsident Norbert Wesseler. Zumindest in Düsseldorf sei die Polizei präsent. Konkrete Einbruchsprognosen führen immerhin dazu, dass Täter abgeschreckt werden. Und die beschleunigten Verfahren vor Gericht funktionieren, so Wesseler. Die Verurteilungsquote liege bei 99 Prozent. Bei den Einbrüchen sei zudem ein Rückgang zu beobachten. „Jeder verurteilte Täter trägt zur Prävention bei", meint Sprenger. Ein Problem sei es aber, wenn einige im Gericht wieder laufengelassen werden. „Wir müssen daher auch die Justiz in den Blick nehmen.

Zur Lösung des Personalengpasses verweist Dr. Frank Nikolaus, Beiratsvorsitzender des Sicherheitsunternehmens W.I.S., auf den Vorschlag, einfache Polizeidienste, die seit Abschaffung des mittleren Polizeidienstes von Kommissaren wahrgenommen werden müssten, an private Unternehmen abzugeben. Private und Polizei seien bereits „wichtige Partner in dem System", sagt Wesseler. Deswegen sei das Interesse groß, dass die Mitarbeiter über eine qualitativ hochwertige Ausbildung verfügen.

Die Menschen können ebenfalls einiges zum Schutz ihres Eigentums beitragen, ist Jérôme F. Soiné, Vorstandsvorsitzender der ISN Technologies AG, überzeugt, vor allem, sich zuerst einmal bei den Beratungsstellen über gesicherte Fenster und Schlösser sowie weitere technische Lösungen zu informieren.

NETZWERK

Orientierung im Dschungel der Zukunft

Sicherheitsexperten haben die „Deutsche Gesellschaft für Zukunft und Sicherheit" ins Leben gerufen. Sie soll Orientierung auf dem komplexen Gebiet der Sicherheit geben.

VON JÜRGEN GROSCHE

Terroristen greifen so genannte weiche Ziele an – Menschen auf der Straße oder bei Großveranstaltungen. Hacker stehlen Daten, lähmen Computersysteme, Einbrecher räumen Wohnungen leer. Das ist Gegenwart. Die Zukunft bringt mit neuen technischen Möglichkeiten auch weitere Bedrohungen mit sich: Wie lässt sich das Smart Home, in dem Kühlschränke und Heizungen mit dem Internet verbunden sind, sichern? Wie sieht die Verkehrssicherheit künftig aus, wenn sich die Fahrzeuge selbst steuern?

„In der Zukunft werden Sicherheitsthemen noch komplexer und vernetzter als heute", ist Uwe Gerstenberg, Geschäftsführer des Sicherheitsberatungsunternehmens consulting plus, überzeugt. Mehr noch: „Viele Risiken sind ja noch gar nicht absehbar, erst recht nicht, wer davon betroffen sein könnte." Zeit, sich des Themas grundsätzlich anzunehmen und zu schauen, was jetzt schon erkennbar ist. Genau das ist die Aufgabe der „Deutschen Gesellschaft für Zukunft und Sicherheit", die Gerstenberg zusammen mit Christian Scherg ins Leben gerufen hat. Scherg ist Geschäftsführer der Revolvermänner GmbH, die sich als Reputations- und Nachrichtendienst für Unternehmen um die digitale Sicherheit ihrer Kunden kümmert.

Die neue Gesellschaft will die Sicherheitsthemen der Zukunft nicht nur theoretisch angehen, sondern auch die praktischen Auswirkungen erfassen. „Geschäftsprozesse verändern sich, ganze Branchen verschieben ihre Schwerpunkte", erklärt Scherg. Sicherheit müsse dabei als relevanter Teil mitbedacht werden. Dabei müsse man auch gesellschaftliche und psychologische Ebenen berücksichtigen, neue Fragen rund um die Sicherheit des Arbeitsplatzes und ebenso neue geopolitische Herausforderungen.

Ein weites Aufgabenfeld also. Die neue Gesellschaft soll sich aber nicht verzetteln. Zunächst wollen die Initiatoren Partner finden, mit denen sie gemeinsam konkrete Projekte voranbringen. Angedacht sind zum Beispiel Branchenthemen. Gerstenberg nennt die Medizintechnik als Beispiel. „Dort wie in anderen Branchen wachsen die realen und die virtuellen Welten zusammen. Wir wollen daher die Entscheider erreichen, um mit ihnen zu analysieren, welche Trends kommen, wie man schon jetzt Weichen richtig stellen kann und welche Risiken sich antizipieren lassen."

Die Gründer „Deutschen Gesellschaft für Zukunft und Sicherheit": Sicherheitsprofi Uwe Gerstenberg von consulting plus (l.) und Reputationsexperte Christian Scherg von Revolvermänner. FOTO: MICHAEL LÜBKE

Ähnliches gilt im Automotive-Sektor. „Künftig wird das Thema Mobilität und Vernetzung noch mehr in den Vordergrund rücken", sagt Scherg, „das führt zu einem Umdenken; Entscheidungen sind mit Unsicherheit verbunden". Im Verkehr der Zukunft wandeln sich die Geschäftsmodelle, „wer die Software beherrscht, zählt zu den zentralen Playern", fügt Gerstenberg hinzu. Man könne aber jetzt schon analysieren, welche Risiken damit verbunden sind. Ein Trend zeichnet sich ja jetzt schon ab – ob in der virtuellen Welt oder im realen Wirtschaften: Die Vernetzung nimmt zu.

Die beste Reaktionsweise darauf ist – natürlich Vernetzung. „In der Zukunft wird der Netzwerkgedanke noch mehr im Vordergrund stehen, auch bei uns. Wir haben deshalb den Begriff der „Virealen Sicherheit" geschaffen – die Verbindung von virtuellen und realen Sicherheitsaspekten", so Gerstenberg. Die neue Gesellschaft soll also Netzwerke etwa für Branchen, aber auch etwa für Themen wie Terrorabwehr bilden – immer mit dem Ziel, präventiv die neuen Sicherheitsthemen anzugehen. „Viele Unternehmen reagieren erst in Krisen", sagt Scherg, „besser wäre es, wenn sie die Risiken vorwegnehmen würden".

„Viele Risiken sind ja noch gar nicht absehbar, erst recht nicht, wer davon betroffen sein könnte"

Als Beispiel verweist Scherg auf digitale Transformationsprozesse. „Sie stellen neue Fragen an die Sicherheit." Gesetze und Patentrechte würden da oft hinterherhinken. Wichtig ist ihm der Hinweis: „Wir wollen die Chancen aufzeigen, nicht nur die angstbehafteten Risikoszenarien betrachten." Sein Wunsch: „Sicherheit wird zu einer in strategischen Planungen immer mitgedachten Komponente, nicht erst ein Thema im Notfall: so selbstverständlich wie das Anschnallen vor dem Losfahren."

Kontakt im Internet:
www.zukunft-sicherheit.org

Mit Hightech gegen Einbrecher

Bezahlbare Sicherheitslösungen für Privatkunden, die leicht montierbar sind und gleichzeitig sabotagesicher sind, sind selten. ISN Technologies aus Münster hat ein eigenes System entwickelt, das auf modernster Funktechnik basiert.

VON JOSÉ MACIAS

Das Angebot klingt verlockend: Für unter tausend Euro, verspricht ein Anbieter, lassen sich die eigenen vier Wände mit Kameras gegen Einbrecher sichern. Ulrich Weynell schüttelt bei solchen Angeboten den Kopf: „Ein vernünftiger Einbruchschutz lässt sich mit solchen Systemen nicht umsetzen, das Geld ist falsch investiert." Der Geschäftsführer der International Security Network (ISN) Technologies AG in Münster kennt den Markt der modernen Sicherheitssysteme so gut wie kaum ein anderer in der Branche. 36 Jahre Berufserfahrung bringt der Experte mit. Aber müssen Sicherheitskonzepte für Privatleute immer gleich zehntausende von Euro kosten?, wollen wir beim Besuch von Ulrich Weynell in der Redaktion wissen.

„Aus meiner Sicht gibt es nur zwei Wege: Entweder eine High-End-Lösung für einen Neubau oder eine relativ günstige Lösung, die aber dauerhaften Schutz bietet", antwortet der Sicherheitsspezialist. An der günstigen Lösung hat ISN Technologies lange getüftelt und ein System entwickelt, das sich nicht nur für einen neu gebautes Haus eignet, sondern auch als Nachrüstung für ein bestehendes Einfamilienhaus oder sogar eine Wohnung. „Drei bis vier Stunden, länger dauert es nicht, um ein ungesichertes Haus auf einen modernen Stand zu bringen", verspricht Weynell. Dafür bauen seine Mitarbeiter eine Alarmanlage mit Kameras im Innen- und Außenbereich auf, die sich von herkömmlichen Systemen deutlich unterscheidet und zudem einfach einzubauen ist, da sie ohne Kabel und damit ohne aufwändige Montage funktioniert. „Zusammen mit unserem Partner in Langenfeld bieten wir als einzige Firma im deutschsprachigen Raum (und darüber hinaus) eine funkbasierte Lösung an, welche in ‚Echtzeit' jedes Ereignis ad hoc in die Sicherheitsleitzentrale überträgt, wo sofort ohne Zeitverzug eine Bildauswertung vorgenommen wird – dadurch werden die sonst üblichen Falschalarme verhindert." Die Hardware stammt aus Israel, eines der führenden Länder im Bereich intelligenter IT Lösungen. Der Verschlüsselungsaufwand ist so hoch, dass dieses System sabotagegeschützt ist. Hinzu kommen redundante Übertragungswege.

ISN-Geschäftsführer Ulrich Weynell: ISN GmbH und ISN AG beschäftigen über 150 Mitarbeiter, Gründer ist Jérôme Soiné. FOTO: ALOIS MÜLLER

Die Außen- und Innenmelder dieser Anlage lösen im Einbruchfall einen Alarm aus: „Die Täter werden dabei von den Kameras geblitzt – mit zehn Bildern pro Sekunde und in einer Auflösung, die uns sofort erkennen lassen, ob Gefahr im Verzug ist", erläutert Weynell. Hier kommt ein weiterer Vorteil des Systems zum Zuge. Die Bilder werden innerhalb von wenigen Sekunden an die Sicherheitszentrale der Firma Protego 24 in Langenfeld gesendet: Hier sitzen rund um die Uhr speziell geschulte Sicherheitsfachleute, die sich auf einen Blick ein Bild über die Lage im Haus machen können. „Das System sendet Fotos, Adresse, Kontaktdaten der Kunden sowie die Durchwahl der nächstgelegenen Polizeidienststelle an die Sicherheitszentrale. Ist Gefahr im Verzug, so können unsere Fachleute sofort die Polizei informieren und mit den Fotos vom Tatort zugleich den Ernst der Lage dokumentieren", bekräftigt der ISN-Geschäftsführer.

Aber ist so viel Technologie für Privatleute überhaupt bezahlbar? Ulrich Weynell macht die Rechnung auf: „Die Nachrüstung einer rund 120 Quadratmeter großen Wohnung kostet rund 2000 bis 2500 Euro, ein Einfamilienhaus liegt bei durchschnittlich 4000 Euro. Und für die Anbindung an die Sicherheitszentrale fallen monatlich lediglich 27 Euro an – wir bieten damit eines der sichersten und effektivsten Low-Cost-Systeme an."

Zugleich hat ISN Technologies viel Know-how in die Benutzerfreundlichkeit der Systeme gesteckt, schließlich sorgen Fehlalarme und falsche Bedienung bei den meisten Alarmanlagen immer wieder für Verdruss. Kleine, übersichtliche Fernbedienungen sowie eine komfortable Smartphone-App machen es den Bewohnern einfach: „Die Anlage lässt sich darüber auf Knopfdruck ein- oder ausschalten. Zugleich können weitere Komponenten, die die moderne Überwachungstechnik heutzutage bietet, ebenso eingebunden werden wie Smarthome-Lösungen", schwärmt Weynell. Mit diesem System hat ISN Technologies offenbar den Nerv der Zeit getroffen: Über 4600 Aufschaltungen laufen in der Sicherheitsleitzentrale in Langenfeld zusammen.

Unabhängig davon rät der Sicherheitsexperte zu mechanischen Sicherheitslösungen an Fenstern und Türen – auch hier greift sein Unternehmen auf eigene Systeme zurück, die auch Nachrüstmöglichkeiten anbieten. „Wir verzeichnen etwa aktuell eine starke Nachfrage nach sicheren Rückzugsräumen im Haus – kein Panic Room, diese Kosten können sich Normalbürger gar nicht leisten –, sondern etwa ein Schlafzimmer, bei dem die Tür in Anlehnung an die genormte Widerstandsklasse RC2 abgesichert wird." Das reicht, um einen Täter mindestens drei Minuten aufzuhalten und um etwa Hilfe zu rufen. „Bestehende Türen können wir mit unserem Mehrfachverriegelungssystem nachrüsten, ohne dass dies optisch auffällt, und erreichen dadurch einen Mindestwiderstandszeitwert von drei Minuten nach Euronorm und darüber hinaus, je nach gewünschter Widerstandsklasse." Und sogar Fensterglas lässt sich mit speziellen Folien ohne große Probleme entsprechend sichern.

Das Portfolio von ISN umfasst neben der Nachrüstung einbruchhemmender Fenster nach Euronorm bis hin zu Durchschuss-hemmenden Fenstern. Grundstücke werden häufig mit intelligenten Zaunsystemen gesichert, welche ohne Falschalarme rund um die Uhr jedes unbefugte Betreten des Grundstücks melden.

Warth & Klein Grant Thornton
An instinct for growth™

Wirtschaftsprüfung | Steuer- und Rechtsberatung | Corporate Finance & Advisory Services | Private Finance

Mit uns bewegen Sie sich sicher im Cyberraum!

Immer häufiger werden Unternehmen in Deutschland Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl.

Diese Bedrohungslage wird in den nächsten Jahren noch ansteigen. Firmen stehen vor der Herausforderung, den Schutz ihrer geschäftlichen Daten an die Gefahren aus dem Cyberraum anzupassen.

Warth & Klein Grant Thornton zählt zu den TOP 10 Wirtschaftsprüfungsgesellschaften in Deutschland.
Ein Team aus erfahrenen Experten bietet eine Rundumbetreuung beim Thema Cyber-Security. Wir analysieren mögliche Bedrohungen für Daten und Systeme und unterstützen Sie dabei, Risiken zu beseitigen und Ihre IT-Sicherheit zu erhöhen.

Als deutsche Firma des Netzwerks **Grant Thornton International** können wir auch bei grenzüberschreitenden Fragen zur Cyber-Security optimal unterstützen. Sprechen Sie uns an!

Ihr Ansprechpartner
WP/StB Dr. Frank Hülsberg
Senior Partner
T +49 211 9524 8527
E frank.huelsberg@wkgt.com

www.wkgt.com

© 2017 Warth & Klein Grant Thornton AG
Warth & Klein Grant Thornton AG ist die deutsche Mitgliedsfirma von Grant Thornton International Ltd (Grant Thornton International). Die Bezeichnung Grant Thornton bezieht sich auf Grant Thornton International oder eine ihrer Mitgliedsfirmen. Grant Thornton International und die Mitgliedsfirmen sind keine weltweite Partnerschaft. Jede Mitgliedsfirma erbringt ihre Dienstleistungen eigenverantwortlich und unabhängig von Grant Thornton International oder anderen Mitgliedsfirmen. Sämtliche Bezeichnungen richten sich an beide Gechlechter.

extra
Sicherheit in Deutschland

Verlag:
Rheinische Post Verlagsgesellschaft mbH, Zülpicher Straße 10, 40196 Düsseldorf
Geschäftsführer: Dr. Karl Hans Arnold, Patrick Ludwig, Hans Peter Bork, Johannes Werle, Tom Bender (verantwortl. Anzeigen), Stephan Marzen
Druck:
Rheinisch-Bergische Druckerei GmbH, Zülpicher Straße 10, 40196 Düsseldorf
Anzeigen:
Leitung Finanz- und Wirtschafts-Extras: Pia Kemper, RP Media Service, 0211 505-2054, E-Mail: pia.kemper@rp-media.de
Redaktion:
Rheinland Presse Service GmbH, Zülpicher Straße 10, 40196 Düsseldorf, José Macias (verantwortlich), Jürgen Grosche, Dr. Patrick Peters, Mitarbeit: Nicole Wildberger,
Foto S. 1: Peter Dazeley/Getty Images/ Grafik: Christian Küller
Kontakt: 0211 528018-14, redaktion@rheinland-presse.de

IT-Security: Gefahren so weit wie möglich reduzieren

Der Mittelstand ist ganz erheblichen Gefahren im Cyberspace ausgesetzt. Neben individuellen Maßnahmen in der IT-Security steht auch im Vordergrund, das Sicherheitsbewusstsein für den Umgang mit der IT bei den Mitarbeitern zu stärken.

VON PATRICK PETERS

15 Jahre sind weltgeschichtlich keine wirklich lange Zeit. Aber es ist sehr wohl eine durchaus substanzielle Spanne in einem Bereich wie der Informationstechnologie (IT), die ständigen dynamischen Veränderungen unterworfen ist und gefühlt täglich Fortschritte macht. Das zeigt sich auch am Unternehmen @-yet aus Leichlingen. Der von Wolfgang Straßer geführte Spezialist für IT-Risikomanagement wurde am 1. Juni 2002 gegründet. „Wir spüren ganz stark, wie sich die Anforderungen der Auftraggeber, seien es Unternehmen oder auch die öffentliche Hand, in dieser Zeit verändert haben. Heute liegt unser Fokus ganz klar auf der sogenannten Business Security, also die Sicherung gegen beabsichtigte Angriffe wie Spionage und Sabotage, unbefugte Modifikationen und Know-how-Verlust, während die Sicherheit von systembedingten Ausfällen und unbeabsichtigten Notfällen auf Grund von Hardware- und/oder Betriebssystemproblemen, die Business Continuity, wesentlich weniger Raum einnimmt als noch vor einigen Jahren."

Das hat einfach mit den neuen Risiken zu tun, die nicht nur große Unternehmen betreffen. „Auch der Mittelstand ist ganz erheblichen Gefahren ausgesetzt. Wir sehen in der Praxis immer wieder, dass Organisationen wirtschaftlich durch kriminelle Handlungen im Cyberspace bedroht sind. Typisch ist zum Beispiel, Daten zu verschlüsseln, um Geld zu erpressen, wie es mit Locky und WannaCry passiert ist. Ebenso kommen Fälle von ‚CEO-Fraud' vor. Dabei werden Unternehmen ausspioniert, und mittels gefälschter E-Mails, Websites etc. wird dann vorgegaukelt, der Geschäftsführer oder Vorstand weise eine Geldüberweisung an. Diese landet dann natürlich bei den Verbrechern. Kürzlich ist so ein Schaden von 40 Millionen Dollar entstanden, und auch mehrere unserer Kunden sahen und sehen sich dem Versuch ausgesetzt. In vielen Fällen war die Sensibilisierung hoch genug, sodass nichts passiert ist, aber wir erleben auch viele Fälle, in denen die Angriffe leider erfolgreich sind", erzählt Wolfgang Straßer aus Erfahrung.

„Auch der Mittelstand ist ganz erheblichen Gefahren ausgesetzt"
Wolfgang Strasser
@-yet

Es sei nun eine Frage der richtigen IT-Security-Strategie, diese Gefahren so weit wie möglich zu reduzieren. Doch wie entsteht diese Sicherheit? „Die erste und wichtigste Frage, die sich Geschäftsführer und Vorstände stellen müssen, ist folgende: Wie lange können wir einen Ausfall der IT nach einem Angriff auf die Infrastruktur verkraften und welcher Datenverlust ist der für das Unternehmen schmerzhafteste? Es sind heutzutage so gut wie alle Prozesse und Abläufe, ob in Dienstleistungs- oder Produktionsunternehmen, IT-gestützt. Die Abhängigkeit von funktionierenden Systemen ist also sehr groß. Daher muss der Schutz der Systeme ganz individuell aufgestellt werden. Je kürzer die Ausfallzeit sein darf, desto komplexer und teurer werden die Anforderungen", betont der @-yet-Gründer. Die Experten analysieren den Ist-Zustand der IT-Organisation und leiten daraus die Maßnahmen ab, um den Soll-Zustand herzustellen.

Straßer ruft Unternehmensverantwortliche deshalb dazu auf, sich strategische Gedanken über die Ziele der IT-Sicherheit zu machen. „Was will ich wirklich? Brauche ich einen wirksamen Schutz gegen Erpressungs-Software, oder will ich Industriespionage und den Diebstahl geistigen Eigentums verhindern? Könnten vielleicht manche Bereiche oder bestimmte Mitarbeiter meines Unternehmens besonderes Ziel von Attacken sein? Darauf können wir reagieren – wenn wir wissen, was der Verantwortliche tatsächlich bezweckt."

Unternehmen dürften nicht vergessen, dass es sich bei den Verursachern der Angriffe um absolute Profis handele, denen man eben mit professionellen Maßnahmen begegnen müsse. „Oft steckt die organisierte Kriminalität dahinter. Zahlen zeigen, wie bedeutend das Geschäft mit Cyber-Attacken geworden ist. Der weltweite Umsatz des Cyber-Crime übertrifft nach Angaben von Behörden, den des Drogenhandels."

Aus der umfassenden Business Security entsteht schlussendlich wieder eine Stärkung der Business Continuity. Damit bleiben IT-Störungen und IT-Ausfälle im tolerierbaren Bereich, und die IT ist auf mögliche Notfälle technisch und organisatorisch vorbereitet.

Ebenso betont Wolfgang Straßer die Bedeutung der sogenannten Awareness, also des Sicherheitsbewusstseins für den Umgang mit der IT. „Der Mensch und sein Umgang mit den Daten und Geräten ist der wichtigste Faktor der IT-Sicherheit und muss auf der Unternehmensebene geregelt werden. Die entsprechende Informationspolitik ist die Aufgabe der obersten Geschäftsführung. Wir unterstützen dabei, diese Awareness zu etablieren."

REPUTATIONSMANAGEMENT UND PRIVATER NACHRICHTENDIENST

Kampf in der Internet-Prärie um den guten Ruf

Wehrhaft verteidigen die Revolvermänner die Reputation ihrer Kunden gegen Angriffe aus dem Internet, erklärt Geschäftsführer Christian Scherg – hier augenzwinkernd mit passendem „Schatten".

FOTO/MONTAGE: MICHAEL LÜBKE

Unternehmen und Privatpersonen sehen sich heute schnell Angriffen auf ihren guten Ruf ausgesetzt. Die „Revolvermänner" helfen ihnen, ihre Reputation im Wilden Westen des Internet zu verteidigen.

VON JÜRGEN GROSCHE

Wie gefährlich das Internet sein kann, wissen Betroffene, die gemobbt wurden, Shitstorms erleiden mussten oder unter Falschnachrichten zu leiden hatten. Einige von ihnen – Privatpersonen genauso wie Unternehmen – suchen professionelle Schützenhilfe bei Profis, deren Name schon darauf hindeutet, dass das Internet heute manchmal eine Art Wilder Westen ist: „Revolvermänner" heißen die Spezialisten, die nicht wild um sich schießen, sondern als „virtuelle Bodyguards die Waffengleichheit wieder herstellen" wollen, wie es Christian Scherg, Geschäftsführer der Revolvermänner GmbH, formuliert.

Wie Heckenschützen greifen Hacker, Erpresser oder Neider an, „da muss die Reputation wehrhaft verteidigt werden", sagt Scherg. Um wehrhaft zu sein, ist eine sorgfältige Vorbereitung auf den Kampf notwendig. Zunächst müssen alle Informationen beschafft und ausgewertet werden. Der Gesellschaft, die selbst rund 20 Mitarbeiter beschäftigt, stehen für die Aufgaben weitere Spezialisten und Partner zur Verfügung, unter ihnen Psychologen, Experten für Konzernsicherheit, psychologische Profiler, IT- und PR-Profis und Mitarbeiter von Nachrichtendiensten. Die Revolvermänner sind Europas erster „Nachrichtendienst für Unternehmen", wie Scherg es formuliert.

Die wehrhafte Abwehr selbst können Kunden auch üben, zum Beispiel mit dem hauseigenen Shitstorm-Simulator. Wie ein solcher Entrüstungssturm im Internet entsteht, darüber gibt es klare Erkenntnisse. Der Sender müsse populistisch konform zu Gruppen sein, die für solche Erregungen empfänglich sind, erklärt Scherg. Und es müsse ein Thema sein, bei dem alle mitreden können.

Die Revolvermänner verfügen darüber hinaus über eigenentwickelte Tools, unter anderem das Comanche Monitoring Tool, das Shitstorms vorhersagen kann – mit einer Wahrscheinlichkeit von 85 bis 90 Prozent, versichert Scherg. So lassen sich zum Beispiel Texte semantisch auswerten und daraus aufziehende Stürme ablesen. Die Reputationsexperten und Profiler durchforsten neben Sozialen Netzwerken auch Foren, Blogs, Kommentare, Bewertungen und das Darknet, um frühzeitig Bedrohungen zu erkennen und Angreifern auf die Schliche zu kommen.

Um wirklich wehrhaft den Ruf zu verteidigen, müssen die Revolvermänner und ihre Kunden in puncto Veröffentlichungen auch selbst aktiv werden. Das Internet vergisst nichts. „Auch was fünf Jahre lang her ist, belastet noch heute", sagt Scherg. Man müsse also neue Informationen ins Netz speisen, um die alten zu verdrängen. Selbst auf Wikipedia achten die Experten. Das Online-Lexikon sei oft nur scheinbar neutral. Häufig nähmen negative Dinge unangemessen großen Raum ein. Auch hier lasse sich durch belegbare Fakten manches richtigstellen, sagt Scherg. „Es geht darum, die Deutungshoheit zu behalten."

Der Geschäftsführer der Revolvermänner betont allerdings: „Wir waschen keine schwarzen Schafe rein." Wenn die Reputationsexperten Bedenken oder Zweifel haben, lehnen sie einen Auftrag auch mal ab – schließlich haben sie selbst einen Ruf zu verteidigen.

Amerika ist für die Revolvermänner wichtig: Viele Angriffe kommen von dort

Der ist über die Branche hinaus anerkannt. Die seit zehn Jahren bestehende Gesellschaft zählt bekannte Persönlichkeiten des öffentlichen Lebens, Spitzensportler, Politiker, Vorstände, Unternehmen und internationale Organisationen zu ihren Kunden und ist zudem als Sachverständige für die Bundesregierung tätig. In Schulungen unterrichten die Experten Mitarbeiter von Konzernen, aber auch Mittelständlern, über Maßnahmen zur Sicherung der Reputation, beispielsweise im Umgang mit Shitstorms. Darüber hinaus arbeiten die Revolvermänner mit vielen großen Versicherungen zusammen, um im Ernstfall die Reputation der versicherten Unternehmen zu schützen und wiederherzustellen.

Neben dem Büro in Düsseldorf unterhalten die Revolvermänner auch Partnerbüros in Frankfurt – dort haben viele Klienten ihren Sitz – und in Toronto. Der nordamerikanische Markt ist aus mehreren Gründen wichtig: „Viele Angriffe kommen von dort", erklärt Scherg. Amerika sei hinter Russland und China eines der wichtigsten Angriffsländer.

IHR SPEZIALIST FÜR
CORPORATE SECURITY & SAFETY

Alle Komponenten **professioneller Sicherheit** aus einer Hand: W.I.S. ist ein führender Anbieter für Corporate Security & Safety und bietet Unternehmen jeder Größe und Branche **umfassende Sicherheitskonzepte, innovative Sicherheitstechnik sowie spezialisierte Services** zugeschnitten auf den individuellen Bedarf.

Mitarbeitern bieten wir **beste Entwicklungsmöglichkeiten** und **nachhaltige Karriereperspektiven** durch eine Vielzahl relevanter Aus- und Weiterbildungsangebote in der hauseigenen Akademie.

www.**wis-sicherheit**.de

Wolfgang Straßer,
@-yet

Volker Wagner,
ASW Bundesverband

Uwe Gerstenberg,
consulting plus Beratung

Stefan Bisanz,
consulting plus Beratung

Hans-Wilhelm Dünn,
Cyber-Sicherheitsrat Deutschl.

Frank Ewald,
Deutsche Post DHL

Wolfgang Bosbach,
Deutscher Bundestag

Detlev Weise,
exploqii

Heinz Sprenger,
FH Duisburg/Mülheim

Rolf Tophoven,
IFTUS Institut f. Krisenprävention

Jérôme F. Soiné,
ISN Technologies

UNTERNEHMEN

„Diebe kommen durch die Datenleitung“

Was Einbrecher anrichten können, darüber haben die Menschen eine klare Vorstellung. Die erfolgreichsten Ganoven der Moderne nutzen indes das Internet für ihre Raubzüge. Die Schäden in der Wirtschaft sind immens, doch man kann sich schützen.

VON JÜRGEN GROSCHE

Sicherheitsspezialisten warnen vor Leichtsinn und Blauäugigkeit: Vernetzung und Cloud-Anwendungen machen Unternehmen verletzlich. Die hier entstehenden Gefahren sind mittlerweile fast bedrohlicher als die herkömmliche Kriminalität, betonen die Experten beim RP-Forum „Sicherheit in Deutschland“ im Museum Folkwang, Essen. FOTOS: ALOIS MÜLLER

So gut wie es den Unternehmen gerade geht: Die Gefahren sollte man dabei nicht übersehen. „Die deutsche Wirtschaft steht gut da“, erläutert Volker Wagner, Vorstandsvorsitzender des Bundesverbandes der Allianz für Sicherheit in der Wirtschaft, in seinem Impulsvortrag beim RP-Wirtschaftsforum „Sicherheit in Deutschland“. Die Rahmenbedingungen seien gut: funktionierender Warenaustausch, internationale Vereinbarungen, ein intaktes Finanzsystem und eine offene Gesellschaft. „Aber die Verletzlichkeit ist groß“, warnt Wagner, „alles ist vernetzt“.

Bei den Risiken hat die Allianz für Sicherheit vier globale Megatrends identifiziert: den Verfall von Staaten, ökonomische Verwerfungen, asymmetrische Kriegsführung und eben die digitale Vernetzung. Bei den Cybercrimes, den Verbrechen übers Internet, wird die Schadenshöhe auf 1,5 bis zwei Prozent des Bruttoinlandsprodukts geschätzt. Das wären allein in Deutschland mindestens 50 Milliarden Euro. Ähnlich kalkulieren auch andere Experten das Schadensvolumen.

„Der Faktor Mensch ist dabei ebenso wichtig wie die Technik“, sagt Wagner. Doch auch die Prozessabläufe in den Unternehmen müssten auf den Prüfstand, kritische Abläufe müssten besser geschützt werden. „Es gibt aber bereits einige gute Maßnahmen“, beobachtet Wagner und nennt als Beispiele die Initiative Wirtschaftsschutz der Bundesregierung im Kampf gegen Spionage und Sabotage oder die Allianz für Cyber-Sicherheit, die vom Bundesamt für Sicherheit (BSI) und dem Digitalverband Bitkom als Plattform initiiert wurden. Auch dass sich die globalen Akteure und Konzerne auf dem Weltwirtschaftsforum mit Cyberkriminalität beschäftigt haben, fällt dem Experten positiv auf: „Das gab es früher nicht.“

Wagner begrüßt ausdrücklich die Digitalisierung: „Sie ist mit großen Chancen verbunden. Deutschland muss diese auch nutzen.“ Allerdings müsse man eben auch die Gefahren berücksichtigen: „Durch die Vernetzung und die Cloud-Anwendungen können auch Angreifer die Digitalisierung nutzen.“ Die Angriffe reichen von der Spionage über den Datendiebstahl bis zur Manipulation der Öffentlichkeit. „Es ist unsere Aufgabe, hier Vertrauen aufzubauen“, appelliert Wagner an die Experten.

Diese bestätigen das in der anschließenden Diskussion. „Unternehmen müssen sich den globalen Herausforderungen anpassen und dürfen nicht in Insellösungen denken – das bedeutet, in sämtliche Strukturen und Prozesse ganzheitlich das Thema Sicherheit zu integrieren“, konstatiert Uwe Gerstenberg, Geschäftsführender Gesellschafter der consulting plus Unternehmensgruppe und Vorsitzender des Präsidiums der Deutschen Gesellschaft Zukunft und Sicherheit.

Kleine und mittelgroße Unternehmen könnten gemeinsam über die Verbände stark werden, ist Frank Ewald, Vice President Corporate Security Deutsche Post, überzeugt. Die bestehenden Initiativen seien gut, aber noch nicht ausreichend. „Wir brauchen Wirtschaftsschutz-Beauftragte in Unternehmen und Behörden“, ist sich Ewald mit Wagner einig. Stefan Bisanz, Geschäftsführender Gesellschafter beim Beratungsunternehmen consulting plus, beschreibt aus der Praxis: „Das Thema Sicherheit macht bei mittelständischen Unternehmen irgendjemand nebenher mit.“ Bisanz appelliert an die Unternehmen, die Prävention ernstzunehmen. „Nach dem Schadenseintritt sind die Kosten viel höher.“ Sicherheit müsse „ein natürlicher Bestandteil des Lebens werden, so wie man auch die Tür selbstverständlich abschließt“.

„Die Prävention beginnt meist erst, wenn das Kind schon in den Brunnen gefallen ist“

„Die Prävention beginnt meist erst, wenn das Kind schon in den Brunnen gefallen ist“, beobachtet Detlev Weise, Geschäftsführer des Kommunikationsdienstleisters exploqii, immer wieder. Im Mittelstand fehle das Wissen und die Erkenntnis über die Bedrohungslage. „Diebe kommen heute aber weniger durch die Tür, vielmehr durch die Datenleitung.“

Christian Scherg, Geschäftsführender Gesellschafter der Krisen- und Sicherheitsberatung Revolvermänner GmbH, ist überzeugt, dass es gerade deshalb von entscheidender Bedeutung ist, ganzheitlich sowohl virtuelle als auch reale Risiken bei der Sicherheitsarchitektur zu berücksichtigen. „Unternehmen müssen den wackeligen Spagat zwischen IT, Kommunikation und physischer Sicherheit auflösen. Nur die Kombination schafft einen sicheren Stand.“

Internet: Initiative Deutschland sicher im Netz: www.sicher-im-netz.de, Allianz für Cyber-Sicherheit: www.allianz-fuer-cybersicherheit.de, Initiative Wirtschaftsschutz (die sich insbesondere an kleinere und mittlere Unternehmen richtet): www.wirtschaftsschutz.info, Allianz für Sicherheit in der Wirtschaft: www.asw-bundesverband.de

porträt Provinzial Rheinland

ANZEIGE

Wirksamer Schutz für die eigene Sicherheit muss nicht kompliziert sein

Die Zahlen sind erschreckend. Jedes Jahr brennt es in rund 200.000 deutschen Haushalten – mit der traurigen Bilanz von Schäden in Höhe von 2,5 Milliarden Euro und etwa 500 Toten.

„Das bedeutet: Jeden Tag sterben durchschnittlich ein bis zwei Menschen an den Folgen eines Brandes, die Hälfte davon aber nicht durch das Feuer an sich, sondern durch eine Rauchvergiftung. Und wer jetzt sagt, er passe doch auf und das könne ihm nicht passieren, irrt: Viele Brände überraschen die Bewohner nachts, sodass regelmäßig Menschen im Schlaf sterben und gar nicht die Möglichkeit haben, Feuer und Rauch zu entkommen“, sagt Stefan Weber, Abteilungsleiter Schadenverhütung der Provinzial Rheinland Versicherung.

Dabei sei es gar nicht so kompliziert, sich gegen die tödlichen Gefahren eines Haus- oder Wohnungsbrandes zu schützen, betont der Sicherheitsexperte. „Rauchwarnmelder retten Leben. Ob angebranntes Essen, ein durchgeschmortes Kabel, eine vergessene Kerze: Rauchwarnmelder reagieren auf die kleinste Rauchentwicklung bei einem Feuer und machen die Bewohner dann mit einem lauten Warnton auf die Gefahr aufmerksam. Wir empfehlen die Installation von Rauchwarnmeldern in allen Fluren, Treppenräumen, Schlaf-, Kinder- und Gästezimmern, um einen optimalen Schutz zu gewährleisten.“ Zudem besteht in Nordrhein-Westfalen mittlerweile eine Rauchwarnmelderpflicht für private Wohnräume. Stefan Weber rät dazu, beim Kauf von Rauchwarnmeldern dringend auf die Qualität zu achten. Zeichen dafür seien unter anderem unabhängige Gütesiegel wie „VdS“, „GS“ und „Q“.

Ein Feuer ist laut dem Provinzial Rheinland-Experten aber bei weitem nicht die einzige Gefahrenquelle für Mieter und Eigentümer. Alle drei Minuten wird in Deutschland in eine Privatwohnung eingebrochen, die Tendenz ist steigend, die Aufklärungsquote zugleich nicht. „Wirksamer mechanischer Schutz ist das effektivste Mittel, einen Einbruch zu verhindern. Einbrecher suchen die Ziele, die für sie leicht zugänglich sind – je mehr Zeit sie brauchen, desto eher lassen sie von einem Einbruch ab. Eine Grundabdeckung bilden damit solide, mechanische Sicherungen, die den Zugang zu Haus und Wohnung versperren. Mechanische Sicherungen zu knacken, ist für Einbrecher zu zeitaufwendig. Untersuchungen der Polizei bestätigen, dass viele Einbruchversuche an fachgerecht eingebauter mechanischer Sicherungstechnik scheitern“, führt Stefan Weber aus. Ebenso rät er, unisono mit anderen Sicherheitsexperten, dazu, Beleuchtungsanlagen zu installieren, die automatisch eingeschaltet werden. Auch gut beleuchtete Objekte schreckten Einbrecher ab. Nicht zuletzt ist auch eine aufmerksame Nachbarschaft nicht zu unterschätzen.

Stefan Weber, Abteilungsleiter Schadenverhütung der Provinzial Rheinland Versicherung

Ergänzend existieren moderne Gefahrenmeldeanlagen, die das Sicherheitsniveau weiter anheben. Im Mittelpunkt stehen laut Stefan Weber Einbruchmeldeanlagen. Sie erkennen, wenn Einbrecher ins Haus eindringen und warnen akustisch. Alarmanlagen können Gefahrensituationen zudem erfassen und entsprechende Alarmmeldungen zum Beispiel an einen Wachdienst oder den Bewohner weiterleiten, zum Beispiel per Sprachansage oder SMS.

Der Abteilungsleiter Schadenverhütung ruft Mieter und Eigentümer aber dazu auf, nur auf geprüfte und zertifizierte Produkte, zum Beispiel durch den VdS, zu setzen und sich für die Installation an anerkannte Fachbetriebe zu wenden. „Schlechte Produkte werden von Einbrechern leicht überwunden, und was schlecht montiert ist, hält keinem Einbruch stand.“

Michael Krons, Phoenix

Norbert Wesseler, Polizeipräsidium Düsseldorf

Christian Scherg, Revolvermänner

Ralf Offelder, ThyssenKrupp Regional Services

Dr. Frank M. Hülsberg, Warth & Klein Grant Thornton

Dr. Frank Nikolaus, W.I.S. Sicherheit + Service

Günter Calaminus, W.I.S. Sicherheit + Service

CYBERKRIMINALITÄT

Wirtschaft unterschätzt Gefahren

Unternehmen erleiden bereits Milliarden-Schäden durch Cyberkriminalität. Dennoch beobachten Experten eine mangelnde Sensibilität für das Thema in der Wirtschaft. Und staatliche Stellen seien zu mager ausgestattet, um den Gegnern auf Augenhöhe zu begegnen.

Sicherheitsexperten, unter ihnen der CDU-Politiker Wolfgang Bosbach (links), diskutierten im Museum Folkwang, Essen, über die aktuelle Sicherheitslage. FOTOS: ALOIS MÜLLER

VON JÜRGEN GROSCHE

Eigentlich hat der Angriff durch die Schadsoftware „Wanna Cry“ das Potenzial zum Weckruf. Mehr als 200.000 Computer waren weltweit – in rund 150 Ländern! – infiziert. Die Nutzer sollten Lösegeld zahlen, damit der Computer wieder freigeschaltet wird. Den Virus schleusten die Kriminellen über eine Sicherheitslücke in alten Windows-Systemen ein. Dieser Angriff im Mai war einer der prominentesten in einer Vielzahl ähnlicher Vorkommnisse. Dennoch beklagen Experten, dass das Bewusstsein für die Gefahr immer noch fehlt. „Das Thema wird noch nicht wirklich beachtet“, stellt Hans-Wilhelm Dünn, Generalsekretär des Cyber-Sicherheitsrates Deutschland e.V., in seinem Impulsvortrag beim RP-Wirtschaftsforum „Sicherheit in Deutschland“ im Folkwang-Museum Essen fest. Das Thema sei hochkomplex. „Daher müssen wir Entscheider und Politiker dafür sensibilisieren.“

Das scheint dringend nötig, schaut man sich die Zahlen an. Im Bundeshaushalt seien 88,8 Millionen Euro für das Thema eingestellt. Das Bundesamt für Sicherheit (BSI) muss mit gerade einmal 680 Mitarbeitern auskommen. In Landesbehörden befassen sich im Schnitt weniger als zwei Mitarbeiter mit Wirtschaftsspionage.

Dabei schädigt Cyberkriminalität die Unternehmen immens. Deutsche mittelständische Unternehmen geraten – so Dünn – durchschnittlich nach zweieinhalb Tagen Betriebsausfall in Liquiditätsengpässe, also in eine unternehmensbedrohende Lage. Solche Ausfälle sind durch Hackerangriffe oder Ransomware (Erpressersoftware) schnell provoziert. „Cyberkriminalität verursacht in Deutschland Schäden von 55 bis 60 Milliarden Euro im Jahr“, warnt Dünn, weltweit seien es 970 Milliarden Euro. „Kriminelle verdienen im Darknet an Cyberkriminalität mehr als andere mit Drogen.“

Auch für Staaten, die Cyberspionage von regierungsnahen Hackerkollektiven oder den

„Man kann unbemerkt von überall auf der Welt auf alles von Wert zugreifen“

Nachrichtendiensten betreiben lassen, biete die virtuelle Welt eine lukrative Einnahmequelle. Hinter der globalen Ransomwareattacke Wanna Cry, die durch die Verschlüsselung von Daten Lösegeld erpresste, vermuten einige Cyberforensiker etwa die dem nordkoreanischen Regime nahestehende Lazarus-Gruppe. „Bei der Attribution solcher Angriffe muss man allerdings vorsichtig sein, der Cyberraum bietet ein hohes Maß an Anonymität und Verschleierung“, sagt Dünn. „Für Cyberangriffe verwenden Täter zum Beispiel Botnetze, also ein Netzwerk aus gekaperten und fremdgesteuerten Rechnern. Angriffe können so über Server von Krankenhäusern oder Schulen ausgeführt werden.“

„Unternehmen müssen endlich aus dem Dornröschenschlaf aufwachen, schließlich stehen Arbeitsplätze und ganze Unternehmensexistenzen auf dem Spiel“, appelliert Uwe Gerstenberg, Geschäftsführender Gesellschafter der consulting plus Unternehmensgruppe und Vorsitzender des Präsidiums der Deutschen Gesellschaft Zukunft und Sicherheit, an die Verantwortung der Entscheider in Unternehmen.

Die Gefahr lauert also hinter jeder Ecke. „Man kann unbemerkt von überall auf der Welt auf alles von Wert zugreifen“, kommentiert Dr. Frank M. Hülsberg, Senior Partner bei der Wirtschaftsprüfungsgesellschaft Warth & Klein Grant Thornton. Antwortversuche mit einer Cyberarmee, wie sie die Bundeswehr aufstellen will, sieht Hülsberg kritisch: „Wo sollen die Spezialisten für 14.000 Stellen herkommen? Und was dürfen die denn?“ Im Inland dürfe die Bundeswehr ja nicht eingesetzt werden, und für Auslandseinsätze bedürfe es eines Bundestagsbeschlusses.

Doch auch in der Privatwirtschaft sieht es mager aus. Es gebe wenig Fähigkeiten in der deutschen Wirtschaft, konstatiert Wolfgang Straßer, Geschäftsführer des IT-Beratungsunternehmens @-yet. Er beobachtet einen „dramatischen Mangel an Erkenntnis in den Unternehmensleitungen“. Und sogar in den Fachabteilungen: „Der größte ‚Feind‘ der IT-Sicherheit sitzt im Vorstand und in der IT. Das Thema wird immer noch zu häufig als fürs eigene Unternehmen nicht so relevant eingestuft.“ Unternehmen setzen hauptsächlich auf Firewall, Antiviren- und Antispamprogramme. Das sei die Abwehr der 90er-Jahre, während die Angriffe mit Mitteln von 2017 geschehen. „Mittelständler haben jetzt das Thema ganz oben auf die Tagesordnung gesetzt. Sie hängen aber 15 Jahre hinterher“, beklagt der Experte.

Dass Security und IT häufig nicht zusammenarbeiten, sondern sogar gegeneinander, bemerkt auch Detlev Weise, Geschäftsführer des Kommunikationsdienstleisters exploqii. Welchen Stellenwert man dem Thema zumesse, sei auch eine „Frage der Qualifikation der handelnden Akteure“. Christian Scherg, Geschäftsführender Gesellschafter der Krisen- und Sicherheitsberatung Revolvermänner GmbH und Präsident der Gesellschaft Zukunft und Sicherheit ist überzeugt: „Der zunehmende Strom an Bedrohungen verlangt von Unternehmen, tragfähige Brücken zu bauen: zwischen Prozessen, Abteilungen und Mitarbeitern. Nur so kann man zukünftig sicher seine unternehmerischen Ziele erreichen.“

Immerhin kann der Düsseldorfer Polizeipräsident Norbert Wesseler auf Erfolge verweisen, die auch in der Sicherheitsbranche Anerkennung finden. Die Spezialisten des Landeskriminalamtes seien gut mit der Polizei vernetzt – eine „gute Bündelung“, wie Straßer bestätigt. „Die Polizei bietet auch Beratung an“, erinnert Hülsberg. Unternehmen sollten sich mit den Behörden abstimmen. Eine Amtsermittlungspflicht hätten die staatlichen Behörden, wenn es zum Beispiel um Erpressung wie beim Virus Wanna Cry geht. „Das kann die Polizei aber nicht alles allein stemmen“, betont der Experte, „da ist Zusammenarbeit gefordert“.

RP-Forum: Die Teilnehmer

@-yet GmbH Wolfgang Straßer, Geschäftsführender Gesellschafter
ASW Bundesverband (Allianz für Sicherheit in der Wirtschaft e.V.) Volker Wagner, Vorstandsvorsitzender
consulting plus Unternehmensgruppe GmbH Uwe Gerstenberg, Geschäftsführender Gesellschafter und Vorsitzender des Präsidiums der Deutschen Gesellschaft Zukunft und Sicherheit
Cyber-Sicherheitsrat Deutschland e.V. Hans-Wilhelm Dünn, Generalsekretär
Deutsche Post DHL Frank Ewald, Vice President Corporate Security
Deutscher Bundestag Wolfgang Bosbach, Mitglied
exploqii gmbh Detlev Weise, Geschäftsführer

Auch der Terrorismusexperte Rolf Tophoven diskutierte mit.

FH Duisburg/Mülheim, Dozent; Mordkommission Duisburg (aD) Heinz Sprenger
IFTUS Institut für Krisenprävention Rolf Tophoven, Direktor
ISN Technologies AG Jérôme F. Soiné, Vorstandsvorsitzender (CEO)
Phoenix Michael Krons, Moderator
Polizeipräsidium Düsseldorf Norbert Wesseler, Präsident
Revolvermänner GmbH Christian Scherg, Geschäftsführender Gesellschafter und Präsident der Deutschen Gesellschaft Zukunft und Sicherheit
Sachverständigenbüro Personenschutz Stefan Bisanz, öffentlich bestellter und vereidigter Sachverständiger für Personenschutz
ThyssenKrupp Regional Services Germany GmbH Ralf Offelder, Corporate Security
Warth & Klein Grant Thornton AG Dr. Frank M. Hülsberg, Senior Partner
W.I.S. Sicherheit + Service GmbH & Co. KG Dr. Frank Nikolaus, Beiratsvorsitzender
W.I.S. Sicherheit + Service GmbH & Co. KG Günter Calaminus, Geschäftsführer

Moderation
José Macias (Rheinland Presse Service GmbH)

RP Foren: Einblick in viele Branchen

(rps) Bei den RP-Wirtschaftsforen tauschen sich Experten aus zahlreichen Branchen über ihre Märkte, die Auswirkungen auf die Menschen, Trends und Perspektiven aus. Vor mehr als zehn Jahren gestartet, hat sich das Spektrum mittlerweile auf viele Branchen erweitert.

Ob Privatbanken, Wirtschaftskanzleien oder die Sicherheitsbranche – immer diskutieren Spezialisten auf hohem Niveau. Die Ergebnisse werden über Sonderveröffentlichungen der Rheinischen Post sowie rp-online.de und weitere crossmediale Formate des Verlages einer breiten Öffentlichkeit mit mehr als einer Million Lesern zugänglich gemacht, darunter ein überdurchschnittlicher Anteil von Unternehmern und Privatpersonen mit hohem Interesse an Wirtschafts- und Finanzthemen.

All diese Aktivitäten sind gebündelt im „Rheinische Post Forum“, das von Pia Kemper geleitet wird. Einen guten Überblick über Veranstaltungen und Publikationen vermittelt die Seite www.rp-forum.de. Dort gibt es nicht nur die aktuellen Sonderpublikationen zum Nachlesen im pdf-Format, sondern auch Bildergalerien, Hinweise auf die geplanten Aktivitäten, Partner und vieles mehr. Sehenswert sind auch Videos mit Interviews, die im Rahmen der Foren gedreht wurden.

SECURITY FOR A CHANGING WORLD

SICHER.
REGIONAL. ÜBERREGIONAL. INTERNATIONAL.

ISN INTERNATIONAL SECURITY NETWORK
Als internationales Sicherheit-Netzwerk bieten wir unseren Kunden alle Dienstleistungen aus einer Hand.

Sicherung der Privatsphäre
Sicherung materieller Werte
Nachrüstung | Neubau
Einbruch | Überfall
Vandalismus | Terrorismus
Mechanik | Elektronik

ISN Technologies AG
Ulrich Weynell
Am Mittelhafen 16 | 48155 Münster
Tel: +49 251 67 44 43 - 0
Mail: u.weynell@isn.eu.com
www.isn-technologies.com

Personenschutz | Eventsicherheit
IT-Security | Investigation
Maritime Sicherheit | Training
Transport | Logistik

ISN GmbH
Jérôme F. Soiné
Montreal Ave. D 415 | 77836 Rheinmünster
Tel: +49 7229 69 76 900
Mail: info@ isn.eu.com
www.isn.eu.com

600 Millionen Viren-Varianten

(jgr) Lange haben Unternehmen die Gefahren aus dem Internet unterschätzt. „Jetzt ist das Thema angekommen“, stellt Helmut Brechtken, Associate Partner Governance, Risk & Compliance bei der Wirtschaftsprüfungsgesellschaft Warth & Klein Grant Thornton, fest. Bei der Podiumsdiskussion im Rahmen des RP-Wirtschaftsforums „Sicherheit in Deutschland“ geht es natürlich auch um die Unternehmen. Brechtken verweist auf das aktuelle Risikobarometer des Versicherungskonzerns Allianz, nach dem sich deutsche Unternehmen erstmals am meisten vor Cyberrisiken wie IT-Ausfällen, Spionage und Datenmissbrauch fürchten.

Doch in der Praxis würden mittelständische Unternehmen zuerst an die Sicherung von Aufträgen und Arbeitsplätzen denken und erst dann an die Sicherheit, beobachtet Uwe Gerstenberg, Geschäftsführer des Beratungsunternehmens consulting plus. „Dann aber häufig deutlich zu spät“. „Die Unternehmen müssen da schneller werden“, bestätigt Volker Wagner. Der Vorstandsvorsitzende des Bundesverbandes Allianz für Sicherheit in der Wirtschaft hat erschreckende Zahlen parat: 69 Prozent der Unternehmen sind bereits Opfer von Schadsoftware geworden. Von solchen schädlichen Programmen gebe es mittlerweile 600 Millionen Varianten.

Heute geht in Betrieben und Unternehmen nichts mehr ohne Computer, betont Wolfgang Straßer, Geschäftsführer des IT-Beratungsunternehmens @-yet. Das müsse bei der Frage, wie Unternehmen ihr Wissen schützen, immer mitbedacht werden. Viele Unternehmen seien auf Angriffe nicht vorbereitet, so fehlten Beschreibungen, wie etwa bei Cyberattacken vorzugehen sei. Großkonzerne investierten derweil zwar viel, stellt Hans-Wilhelm Dünn, Generalsekretär des Cyber-Sicherheitsrat Deutschland e.V., fest. Allerdings arbeiten die großen Unternehmen häufig mit vielen Zulieferern zusammen; dabei seien die Schnittstellen immer noch Einfallstore für Cyber-Angriffe.

Hauptrisikofaktor ist aber der Mensch. Cyberkriminelle suchen heute gerne über Mitarbeiter den Zugang zu Unternehmen, sagt Brechtken. Man müsse sie also besonders und vor allem kontinuierlich schulen, schlussfolgert Detlev Weise, Geschäftsführer des Kommunikationsdienstleisters exploqii.

Reputationsexperte Christian Scherg von der Kommunikationsberatung Revolvermänner und Präsident der Deutschen Gesellschaft für Zukunft und Sicherheit ergänzt, dass viele Angriffe sogar auf Geschäftsführer und Vorstände abzielen. Präventiv die geeignete Strategie auf allen Ebenen zu finden, ist laut Scherg entscheidend: „Sicherheit darf im digitalen Zeitalter nicht als Lazarettwagen der unternehmerischen Entwicklung hinterherfahren.“

Sicherheit im Fokus: Experten haben sich im Museum Folkwang, Essen, getroffen und über verschiedene Aspekte des Themas und die Auswirkungen auf Bürger und Unternehmen diskutiert. FOTOS: ALOIS MÜLLER

SCHWERPUNKTTHEMEN ALLTAGSKRIMINALITÄT, CYBER SECURITY UND TERRORISMUS

„Sicherheitsbedürfnis der Menschen steigt“

Innere Sicherheit in Deutschland ist ein großes Thema. Alltagskriminalität, Cyber Security und Terrorismus sind aktuell die größten Treiber der Diskussion, wie das zweite Rheinische Post-Wirtschaftsforum „Sicherheit in Deutschland“ zeigte.

VON PATRICK PETERS

Wolfgang Bosbach ist einer der herausragenden Kenner der Innen- und Sicherheitspolitik in Deutschland. Der CDU-Politiker aus Bergisch Gladbach war lange Jahre stellvertretender Vorsitzender der Bundestagsfraktion der Union und Vorsitzender des Innenausschusses des Deutschen Bundestages und soll unter der neuen nordrhein-westfälischen CDU-/FDP-Regierung eine Regierungskommission zur inneren Sicherheit leiten. Beim zweiten Rheinische Post-Wirtschaftsforum „Sicherheit in Deutschland“ trug Wolfgang Bosbach einige Kernthesen rund um sein Spezialthema vor und stieß damit eine große Diskussion an. „Wir sehen drei große Themen bei der Sicherheit. Das ist zum einen die Alltagskriminalität wie Einbrüche, die zu einem hohen Anteil von organisierten ausländischen Banden begangen wird. Die Aufklärungs- und Verurteilungsquote ist sehr schlecht und es kann nicht die einzige Lösung sein, dass der Staat finanzielle Zuschüsse für den Einbruchsschutz vergibt. Er muss auch für Sicherheit sorgen.“ Zum anderen weist der Experte auf die hohe Anzahl an terroristischen Gefährdern mit einem hohen Bedrohungspotenzial in Deutschland hin und fordert, die juristischen Maßnahmen wie den vorbeugenden Unterbindungsgewahrsam zur Verhütung einer unmittelbar bevorstehenden Straftat auszuweiten. „Und zuletzt geht es um die Datensicherheit. Die digitale Infrastruktur ist ein neues Schlachtfeld, dem wir uns stellen müssen. Wir aber diskutieren in Deutschland politisch fast ausschließlich über den persönlichen Datenschutz“, kritisiert Wolfgang Bosbach. Zudem betont er, dass die Zahl der Rohheitsdelikte und die Angriffe gegen Polizei, Feuerwehr zunähmen; das habe mit einer steigenden Respektlosigkeit zu tun.

Diese neue Bedrohungslage in Deutschland wirkt sich natürlich auch auf die Sicherheitsindustrie aus. „Das persönliche Sicherheitsbedürfnis der Menschen steigt, sie suchen nach individuellen Lösungen. Wir müssen ihnen dafür die Konzepte liefern“, sagt Günter Calaminus, Geschäftsführer der W.I.S.-Gruppe. Uwe Gerstenberg (consulting plus) weist darauf hin, dass die Branche ein Umsatzplus von 24 Prozent für 2016 erwirtschaftet hat und das private Sicherheitsgewerbe mit 270.000 Mitarbeiter mehr Personal beschäftigt als alle öffentlichen Sicherheitsbehörden. „Es fehlen aber aktuell rund 12.000 Mitarbeiter.“

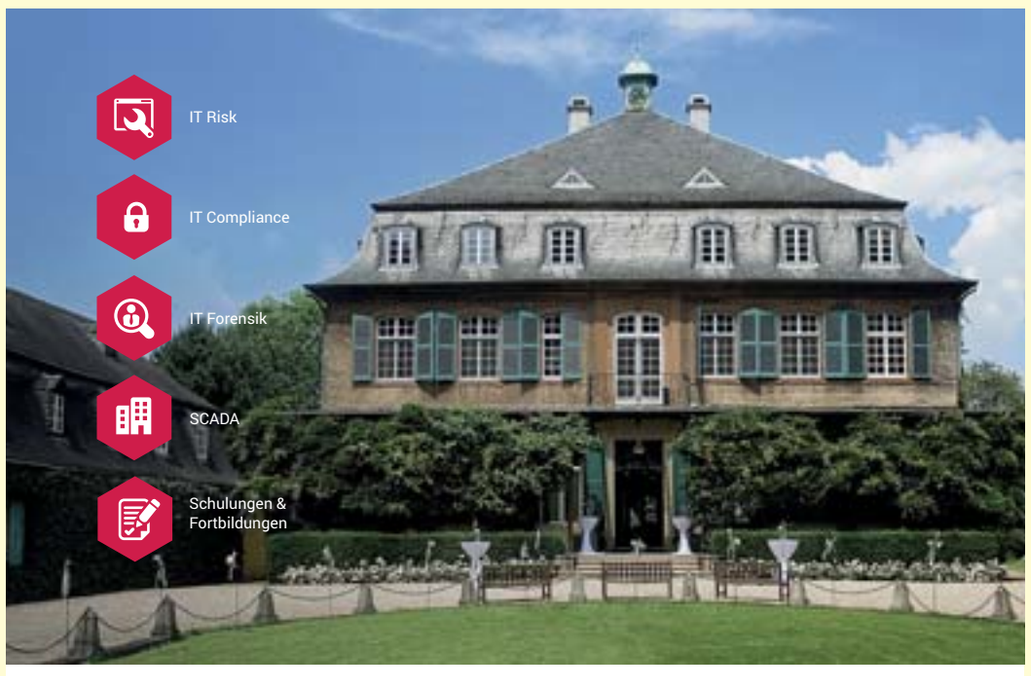
Heinz Sprenger, ehemaliger Leiter der Mordkommission Duisburg und heute Fachhochschul-Dozent und Buchautor, ist der Auffassung, dass die Sicherheitswirtschaft vom Versagen der Politik profitiert, die immer nur reagiere und die Polizei am absoluten Limit arbeiten lasse. Dagegen wendet sich der Düsseldorfer Polizeipräsident Norbert Wesseler. Er sagt: „Personal allein reicht nicht aus. Wir müssen auch über die richtige Ausrüstung sprechen und uns fragen, wie Unsicherheit entsteht.“ Darauf hat Stefan Bisanz (consulting plus), öffentlich bestellter Sachverständiger für Personenschutz und Buchautor, eine Antwort: „Jeder redet mit, daher kommt Unsicherheit. Wir müssen die Menschen in der privaten Sicherheitswirtschaft viel stärker qualifizieren und die Struktur der Sicherheitsbehörden überdenken. Denn die Branche wird immer noch stark ausgebremst.“

Auch über Alltagskriminalität diskutierten die Experten, unter ihnen Heinz Sprenger, ehemaliger Leiter der Mordkommission Duisburg (2. v.r.) und der Düsseldorfer Polizeipräsident Norbert Wesseler (rechts).

Bessere Ausrüstung der Polizei fordert auch der Terrorismusexperte Rolf Tophoven, schließlich befinde man sich nach dem Selbstverständnis der Terroristen „im Krieg“, denn wie die Anschläge in Paris gezeigt hätten, operierten Terroristen – neben dem Einsatz mit Bomben und Sprenggürteln – zunehmend auch mit Kriegswaffen, zum Beispiel Kalaschnikows. Christian Scherg von der Krisenkommunikationsberatung Revolvermänner meint in dem Zusammenhang, dass viele Polizeieinheiten falsch organisiert seien und großer Verbesserungsbedarf bestehe – beispielsweise hinsichtlich einer spezialisierten kriminalistischen Ausbildung und des sofortigen Einsatzes. Ebenso ist Scherg der Auffassung, dass die Polizei an ihrer Reputation arbeiten müsse.

Frank Ewald, weltweiter Sicherheitschef der Deutschen Post, bestätigt den Eindruck von Wolfgang Bosbach aus Unternehmenssicht. „Wir erleben eine neue Form der Gewaltkriminalität in Deutschland. Unsere Mitarbeiter sind überall im Einsatz, auch unter Umständen, die eine besondere Aufmerksamkeit der Unternehmenssicherheit bedürfen. Wir werden der steigenden Zahl von bisherigen und neuen Kriminalitätsphänomenen mit neuen Technologien und angepassten Prozessen begegnen.“

Volker Wagner, Vorstandsvorsitzender des ASW Bundesverbandes, sieht in der Krisensituation aber auch Chancen. Sicherheit sei Teil einer umfassenden politischen Diskussion geworden. Jetzt sei die Zeit, versäumte Maßnahmen nachzuholen, ohne gleich Gesetze zu verschärfen.



Wir beschränken uns nicht darauf, Schwachstellen aufzuzeigen, sondern beraten und begleiten unsere Kunden auf dem Weg zur optimalen IT-Sicherheit.
Lernen Sie uns kennen.

Schloß Eicherhof
42799 Leichlingen
info@add-yet.de
www.add-yet.de

RHEINISCHE POST | Forum

Experten diskutieren Themen, Trends und Perspektiven, die unsere Leser bewegen.

Direkter Austausch, Diskussionen und Vernetzungen entfachen Ideen und fördern Innovationen – und das Rheinische Post Forum ist genau dafür die geeignete Plattform. Bei unseren Veranstaltungen bringen wir die lokale und regionale Expertise aus Wirtschaft, Politik und Kultur zusammen. Die Ergebnisse der Veranstaltungen werden in den Produkten der Rheinischen Post veröffentlicht.

Informieren Sie sich jetzt über unsere Veranstaltungen und Veröffentlichungen:
www.rp-forum.de

FINANZIELLES RISIKO

Professionelle IT-Security vermeidet Haftungsforderungen

Risiken in der IT-Sicherheit können zur persönlichen haftungsrechtlichen Inanspruchnahme von Organen eines Unternehmens führen – Compliance ist das Stichwort. Die Wirtschaftsprüfungsgesellschaft Warth & Klein Grant Thornton berät umfassend bei allen Fragen rund um die IT, wozu auch die Einhaltung aller rechtlichen Vorgaben gehört

VON PATRICK PETERS

Der Angriff auf den Bundestag im September 2015, der Locky-Virus im Frühjahr 2016, Attacken mit der Schad-Software „WannaCry“ im Mai dieses Jahres: Die Cyber-Kriminalität boomt. Und damit steigen die Risiken für Privatleute, Unternehmen – und deren Führungskräfte. „Die IT-Sicherheit ist ein wichtiger Aspekt der Compliance.

„Compliance und Risikomanagement gehören eng zusammen“
Dr. Frank Hülsberg
Warth & Klein Grant Thornton

Darunter verstehen wir ganz allgemein die Einhaltung aller gesetzlichen Vorschriften in einem Unternehmen, die durch bestimmte Maßnahmen innerhalb eines Compliance Management-Systems sichergestellt werden. Verstöße gegen diese Compliance-Richtlinien führen regelmäßig zu Haftungsforderungen gegen Führungskräfte. Und das kann teuer werden. Wir haben schon Fälle gesehen, in denen gegen Vorstände Forderungen in zweistelliger Millionenhöhe gestellt worden sind“, sagt Dr. Frank Hülsberg, Senior Partner der Wirtschaftsprüfungsgesellschaft Warth & Klein Grant Thornton in Düsseldorf und verantwortlich für den Bereich Governance, Risk & Compliance mit den Schwerpunkten Risikoprävention, Sonderuntersuchungen und Cyber-/IT-Security.

Organisation und Prozesse eines Unternehmens seien heutzutage in großem Umfang in IT-Systemen abgebildet beziehungsweise würden von diesen wesentlich unterstützt. Die IT sei daher ein wichtiger Bestandteil eines Unternehmens, deshalb sollte sie in der Unternehmensstrategie und auch im Risikomanagement einen entsprechenden Stellenwert besitzen. „Resultierend aus den laufend komplexer werdenden gesetzlichen und regulatorischen Anforderungen ergeben sich damit ständig neue Aspekte für den IT-Bereich, die über die rein technischen Entwicklungen hinausgehen“, sagt der Wirtschaftsprüfer und Steuerberater.

Dr. Frank Hülsberg, Senior Partner der Wirtschaftsprüfungsgesellschaft Warth & Klein Grant Thornton in Düsseldorf und verantwortlich für den Bereich Governance, Risk & Compliance FOTO: WKGT

Insofern sei es für Vorstände und Geschäftsführer von entscheidender Bedeutung, Maßnahmen zur Verankerung der IT-Sicherheitsstandards und Datenschutz-Vorschriften im Unternehmen zu etablieren, um allen Vorgaben hinsichtlich der Compliance zu genügen.

Umfragen zeigen, dass digitale Kompetenz in deutschen Aufsichtsgremien eine Seltenheit ist

„Dies ist genauso wichtig wie die Einhaltung aller steuerlichen Vorschriften oder auch der Grundsätze der ordnungsgemäßen Buchführung. Ohne eine professionelle IT-Security ist es nicht möglich, dem gesetzlich geforderten Risikomanagement dauerhaft nachzukommen. Und Compliance und Risikomanagement gehören eng zusammen“, betont Frank Hülsberg. Konkret bedeutet das: Kommen Führungskräfte den Anforderungen an die IT-Sicherheit nicht nach und versäumen es, für ausreichende technische und organisatorische Sicherheitsmaßnahmen zu sorgen, kann beispielsweise eine Attacke auf die Systeme eines Unternehmens zu einem Haftungsrisiko für sie werden – persönliche haftungsrechtliche Inanspruchnahme ist das Stichwort. Haftungsrisiken bestehen auch für Überwachungsorgane. „Aufsichts- und Beiräte benötigen Digitalkompetenz, um digitale Geschäftsmodelle zu begleiten. Andernfalls können sie das Management nicht effektiv überwachen und gehen damit ein erhebliches persönliches Haftungsrisiko ein“, gibt Hülsberg zu bedenken: „Leider zeigen Umfragen, dass digitale Kompetenz in deutschen Aufsichtsgremien eine Seltenheit ist.“

Unternehmen können durch Beratung ihre IT- Systeme und Prozesse verbessern

Frank Hülsberg und die anderen Warth & Klein Grant Thornton-Experten beraten Unternehmen und Organe umfassend bei allen Fragen rund um die IT, beginnend bei den Erwartungen der Geschäftsführung an den Beitrag der IT zur Geschäftsstrategie (IT-Strategie) über die Einhaltung aller rechtlichen Vorgaben in der IT (IT-Compliance) bis hin zur Begleitung zu allen Fragen des Datenschutzes (Data Privacy). Auch die sogenannte IT-Assurance gehört zum Dienstleistungsangebot. Darunter fallen die Prüfung und Beurteilung der Ordnungsmäßigkeit und Sicherheit der IT-Anwendungen, IT-Infrastruktur und der IT-internen Abläufe und die Unterstützung bei der Auslegung und Umsetzung regulatorischer Vorgaben auf konkrete Sachverhalte, etwa bei der Einführung interner Lösungen oder der Vermarktung neuer Lösungen im deutschen Markt.

„Auf diese Weise stellen wir sicher, dass alle Vorschriften hinsichtlich Compliance und Risikomanagement erfüllt und dadurch Haftungsrisiken begrenzt werden können. Unternehmen und deren Organe erhalten durch eine spezialisierte und professionelle Beratung die Möglichkeit, ihre eingesetzten IT-Systeme und Prozesse zu verbessern“, fasst Senior Partner Frank Hülsberg zusammen.

Unternehmen sind über Cyber-Vorfälle besorgt

Das sechste jährliche Allianz Risk Barometer stellt einmal mehr die Bedrohungen für Unternehmen heraus. Und die sind mittlerweile breit gefächert.

VON PATRICK PETERS

Politische Instabilität, Terrorrisiken, Kriminalität im Internet, Wirtschaftsspionage und, und, und: Die Großwetterlage von Unternehmen rund um den Globus ist von vielen Unsicherheiten geprägt. Das stellt auch das sechste jährliche Allianz Risk Barometer heraus. Die Studie fasst die wichtigsten Unternehmensrisiken im Jahr 2017 zusammen und kommt zu dem Ergebnis, dass die Wirtschaft es mit einer umfassenden Bedrohungslage zu tun. Dafür hat die Allianz mehr als 1200 Sicherheitsexperten aus 50 Ländern befragt.

Auf Platz 1 steht die allgemeine Sorge vor einer Betriebsunterbrechung – zum fünften Mal in Folge das größte Risiko für Unternehmen, wie die Untersuchung herausstellt. Gefahren wie Naturkatastrophen und Brände sind weiterhin die Ursachen, die Unternehmen am meisten fürchten, aber die Art des Risikos verschiebt sich zunehmend auf Nicht-Schaden-Ereignisse. Ein Cyber-Vorfall oder die indirekten Auswirkungen eines terroristischen Gewaltakts sind Ereignisse, die zu großen Verlusten führen können, ohne physische Schäden zu verursachen. Eine Zunahme solcher Ereignisse werde erwartet.

Mittlerweile ist alles vernetzt. Dementsprechend können beispielsweise ein technischer IT-Ausfall oder auch menschliches Versagen zu schweren Schäden füllen. FOTO: THINKSTOCK/COFOTOISME

Apropos IT-Risiken: Im vierten Jahr in Folge sind die Unternehmen zunehmend über Cyber-Vorfälle besorgt, heißt es. „Die Bedrohung geht weit über Hacking, Datenschutzverletzungen oder Datendiebstähle hinaus, obwohl neue Datenschutzbestimmungen die Folgen solcher Vorfälle für Unternehmen verschärfen werden. Auch ein technischer IT-Ausfall oder menschliches Versagen können zu teuren Schäden führen. In einer Industrie 4.0-Umgebung können nicht korrekt verarbeitete oder misinterpretierte Daten die Produktion zum Stillstand bringen“, ist im Allianz Risk Barometer zu lesen.

Die Abhängigkeit von Technologie und Automatisierung können disruptive Folgen haben

Marktentwicklungen seien das zweitwichtigste Risiko insgesamt, auch wenn sich branchenspezifische Unterschiede zeige. Die zunehmende Abhängigkeit von Technologie und Automatisierung transformiere die Industrie und könne disruptive Folgen für Unternehmen aller Branchen haben. Die Digitalisierung berge nicht nur Vorteile, sondern auch neue Risiken und führe zu zunehmend immateriellen Vermögenswerten bei Unternehmen.

Die Sicherheitsarchitektur der Zukunft ist „vireal“

Wer Bedrohungen umfassend begegnen will, muss Gebäude und Leben sichern, aber neben realen auch die virtuellen Gefahren im Blick haben. Also alles in ein „vireales“ Konzept integrieren, wie Experte Uwe Gerstenberg es beschreibt.

Realität und virtuelle Welt wachsen zusammen – die Sicherheitsarchitektur muss dies berücksichtigen und „vireal“ werden, wie Experte Uwe Gerstenberg es formuliert. FOTO/MONTAGE: CONSULTING PLUS

VON JÜRGEN GROSCHE

Ein diffuses „Alles ist unsicher derzeit“ reicht nicht für eine adäquate Beschreibung der Gegenwart. Um richtig zu reagieren, ist schon eine genauere Betrachtung notwendig. Wenn Sicherheitsexperten die Bedrohungen analysieren, klärt sich das Bild doch deutlicher. Uwe Gerstenberg, Geschäftsführer und Gesellschafter der consulting plus Unternehmensgruppe und ein erfahrener Spezialist in Sachen Sicherheit, identifiziert als zentrale Risikofelder derzeit den Terrorismus, die Cyberkriminalität und Einbrüche in die Privatsphäre im weitesten Sinne. „Anschläge in Deutschland und Europa werden zunehmen“, fürchtet der Experte. Die islamistische Terrororganisation IS wird derzeit in Syrien und im Irak zurückgedrängt, viele radikalisierte Kämpfer tragen den Terror dafür in die Welt hinaus. Sicherheitsbehörden bereiten sich zwar darauf vor, das reiche aber nicht, warnt Gerstenberg. „Man muss sich auch als Privatperson damit auseinandersetzen.“

Was heißt das konkret? Die Menschen müssten „weg von einer Vollkasko-Mentalität hin zu mehr Eigenverantwortung kommen“, sagt der Sicherheits-Profi. Wenn alle vor dem Besuch einer Großveranstaltung mal schauen, wo die Rettungswege entlanglaufen, könnte das im Ernstfall die Evakuierung erleichtern. Zudem kann man sich überlegen, was alles in eine Tasche muss oder eben nicht. Man macht es damit übrigens allen leichter – Vielflieger kennen die ärgerliche Situation, wenn an der Sicherheitskontrolle mal wieder darüber diskutiert wird, warum die Flasche oder das Nageletui nicht mitgenommen werden dürfen. Muss ja nicht sein.

Wenn es um den Schutz vor Einbrechern oder Hackern geht, gibt es trotz aller Ängste vor den Bedrohungen einige Hindernisse, stellt Stefan Bisanz, ebenfalls Geschäftsführer und Gesellschafter von consulting plus immer wieder fest. Mal fehlt das Geld dafür, mal glaubt man, eigentlich ja gut aufgestellt zu sein. An der Stelle empfiehlt der Sicherheitsfachmann einen richtigen Stresstest oder ein Qualitäts-Auditing. Die Experten von consulting plus zum Beispiel checken nicht nur die Systeme, sondern prüfen auch die Qualität der Sicherheitsdienstleister ihrer Kunden.

Problem bei vielen solcher Dienstleister: „Drei Viertel der Mitarbeiter sind nicht ausreichend qualifiziert“, zieht Gerstenberg Bilanz aus seinen Beobachtungen. Sicherheitsfachkraft ist ein Ausbildungsberuf, doch in der Praxis sind häufig nur Mitarbeiter beschäftigt, die eine einwöchige Qualifizierung für den Sicherheitsdienst absolviert haben. Wer hier spart, tut es an der falschen Stelle, betont Gerstenberg. Die immensen Schäden durch Einbrüche und Cyberkriminalität bestätigen seine Einschätzung.

„Für all das muss man erst einmal ein Bewusstsein schaffen, bevor man mit Sicherheitskonzepten anfängt“, sagt der Geschäftsführer des Beratungsunternehmens. Es bietet deshalb auch keine Lösungen von der Stange an. „Wir müssen zunächst die konkrete Situation eines Kunden eruieren und daraus Lösungen entwickeln“, erklärt Bisanz. Bei einem Unternehmen muss ein Schwerpunkt vielleicht eher auf dem Schutz vor physischen Einbrechern liegen, bei einem anderen vor den virtuellen, den Hackern. Consulting plus hat sich daher „vom Sicherheitsdienstleister zum Systemanbieter für integrale Sicherheitslösungen“ entwickelt, wie Gerstenberg es formuliert.

Die Herangehensweise hat sich damit komplett umgedreht: Statt vom Ende, von der Lösung her zu denken, betrachten die Sicherheitsexperten von consulting plus das Thema aus Sicht möglicher Täter. „Die dringen heute über alle Zugangswege ein – über physische ebenso wie über digitale. Realität und virtuelle Welt wachsen zusammen.“ Die integrale Antwort müsse daher „vireal“ sein, beides also kombinieren, formuliert es Gerstenberg mit einer Wortneuschöpfung.

Dieses Denken sei in der Sicherheitsarchitektur häufig noch unbekannt, sagt der Experte und nennt als Beispiel, dass Terrorabwehr- und Cyberzentren immer noch getrennt arbeiten, während Terroristen längst in beiden Welten leben. So haben vermutlich die Attentäter, die im November 2015 in Paris Anschläge auf das Fußballstadion während des Deutschland-Frankreich-Fußballspiels und auf ein Konzert im Bataclan-Theater verübten, über die Spielekonsole Playstation 4 kommuniziert – ein Thema also für Terror- und Cyberexperten gleichermaßen. Auch für Unternehmen und Privatpersonen ist es höchste Zeit, beim Thema Sicherheit über den Tellerrand von Einzelproblemen zu schauen.

Tipps von consulting plus zum Thema Sicherheit: www.consulting-plus.de/sicherheitstipps

Uwe Gerstenberg (links) und Stefan Bisanz (consulting plus) gehen das Thema Sicherheit aus neuer Perspektive an. FOTO: ALOIS MÜLLER

ABWEHRKONZEPTE

Paradigmenwechsel in der Branche

Bei der W.I.S. Unternehmensgruppe sind Führungskräfte und Mitarbeiter stolz auf mehr als 100 Jahre Firmengeschichte. In dieser Zeit hat sich das Aufgabenspektrum des Unternehmens stark verändert. Und das besonders schnell im vergangenen Jahrzehnt.

Günter Calaminus, Vorstandsvorsitzender der W.I.S.-Gruppe, sieht die Branche vor großen Herausforderungen. FOTO: LARS LANGEMEIER/WIS

VON NICOLE WILDBERGER

Die W.I.S. Unternehmensgruppe ist einer der Großen in der Branche: seit mehr als einem Jahrhundert bietet das Unternehmen private Sicherheitsdienstleistungen an und gehört mit einem umfassenden Dienstleistungsangebot zu den größten privaten Anbietern der Branche. Aktuell beschäftigt das Unternehmen fast 4000 Mitarbeiter an insgesamt 29 Standorten bundesweit und hat aufgrund seiner langen Tradition viele Entwicklungen von Markt und Gesellschaft miterlebt.

„Nie waren die Herausforderungen größer“, sagt Günter Calaminus, Vorstandsvorsitzender der W.I.S.-Gruppe, und führt weiter aus: „Aktuell verändern sich die Paradigmen des Marktes tiefgreifend, denn einerseits steigt das individuelle Sicherheitsbedürfnis durch Terroranschläge sprunghaft an, durch die zunehmende Bedrohung aus dem Netz verändern sich allerdings auch gleichzeitig die Waffen und Werkzeuge der Angreifer.“ Private Sicherheitsdienstleister müssen mit dieser Entwicklung Schritt halten und wirksame Abwehrkonzepte entwickeln.

Das geht jedoch nicht ohne die passenden Mitarbeiter, die der zunehmenden Digitalisierung möglicher Bedrohungslagen gerecht werden müssen. „Der Sicherheitsmitarbeiter von heute hat schon lange nichts mehr mit dem Wachmann gemein“, resümiert Calaminus. Die Mitarbeiter müssen ein Grundverständnis für den Umgang mit computergesteuerten Prozessen entwickeln, um die Kunden weiterhin zuverlässig zu schützen und moderne Werkzeuge wie Smartphones, RFID-, NFC oder Beacon -Technologien und die damit verbundenen Informationstechnologien zum Einsatz zu bringen.

Günther Calaminus versteht es als eine soziale Verantwortung seines Unternehmens, die Mitarbeiter dabei zu unterstützen, die notwendigen Kompetenzen zu entwickeln. Denn bei einem Defizit von rund 12.000 Mitarbeitern am gesamten Sicherheitsmarkt in Deutschland kann es nicht mehr nur darum gehen, die richtigen Talente zu gewinnen, sondern vielmehr, bestehende

„Der Sicherheitsmitarbeiter von heute hat schon lange nichts mehr mit dem Wachmann gemein“

Talente zu fördern und auszubauen. Dies könne jedoch nur gelingen, wenn auch die rechtlichen Bedingungen für private Sicherheitsdienstleistung den aktuellen Gegebenheiten angepasst werden.

„Aktuelle Anpassungen des Arbeitnehmerüberlassungsgesetzes und der Bewachungsverordnung sind die richtigen Schritte hin zu einer besseren Qualitätsauslese leistungsfähiger Dienstleistungsunternehmen und werden deshalb durch die W.I.S. begrüßt und unterstützt“, sagt Calaminus.

Vor dem Hintergrund der Digitalisierung von Attacken muss allerdings auch die Definition von Eigentum neu überdacht werden. Denn zukünftig wird es für private Sicherheitsdienstleister nicht mehr nur um den Schutz fremder, beweglicher Sachen gehen können. Wirtschaftsspionage und Diebstahl von Knowhow gewinnen eine immer größere Bedeutung und verursachen in Deutschland die bei weitem größten Schadenssummen für Unternehmen.

Digitale Werte, wie Tokens oder Kryptowährung, werden von der herkömmlichen Definition für Eigentum noch gar nicht klar erfasst. Sie sind allerdings bereits jetzt ernstzunehmende Zahlungsmittel im globalen Handelskreislauf. Die gesamte Vorschriften-, Ausbildungs- und Qualitätswelt der Sicherheitsbranche hingegen fußt auf einer Definition, die dieser Entwicklung keine Rechnung trägt. Deshalb müssen auch diese Grundlagen angepasst werden, um privaten Sicherheitsdienstleistern den passenden Rahmen für zeitgemäße Geschäftsmodelle zu bieten.

Die fachlichen Anforderungen an private Sicherheitsdienstleister steigen im gleichen Maße wie das Risiko für deren Kunden. Dennoch bleibt die Bereitschaft der Kunden gering, für gestiegene Anforderungen einen angemessenen Preis zu zahlen. Die seriöse Sicherheitsindustrie und damit auch Unternehmen wie die W.I.S. ist davon überzeugt, dass sich mit preisgetriebenen Ausschreibungen das steigende Risiko für die Kunden längst nicht mehr ausreichend kompensieren lässt.

Genauso wenig ließen sich mit Mindestlöhnen die Mitarbeiter finden, die eine digitale DNA mitbringen und bereit sind, das erhöhte Risiko zu tragen. Deshalb werden am Ende nur jene Unternehmen langfristig erfolgreich sein, die hybride Sicherheitslösungen mit digitalen und personellen Komponenten entwickeln, um damit die Dienstleistung als solche für den Kunden erlebbar zu machen. „Wir sehen der Zukunft positiv entgegen“, schließt Günter Calaminus.