Raubritter 4.0 müssen keine dicken Mauern überwinden.

Sie kommen per WLAN in Ihre Burg. Und vielleicht sind sie schon da.

dwf

DIGITALISIERUNG

OHNE

DIGITALE

SICHERHEIT

IST

UNDENKBAR

UND

GEFÄHRLICH!

Digitale Sicherheit
gibt es nur
beim Spezialisten.

Lassen Sie sich beraten:

@-yet GmbH
Köln/Düsseldorf
Schloß Eicherhof
42799 Leichlingen

Telefon: 02175 1655 0
info@add-yet.de
www.add-yet.de
www.add-yet-iis.de

SICHERHEIT IN DEUTSCHLAND

So sah Sicherheit in früheren Zeiten aus: Eine Burg mit hohen Mauern und Türmen weist jeden ab, der ungefragt eindringen möchte. Was damals wie hier in Schottland funktioniert haben mag, muss heute natürlich ganz anders aufgezogen werden, aber das Prinzip bleibt. Wie Schutzmauern funktionieren Sicherheitsmaßnahmen im Internet, an Haus und Wohnung oder auch bei Großveranstaltungen. FOTO: THINKSTOCK/MR1805

POLITIK

Kampf um die richtigen Maßnahmen

Es scheint paradox: Die Menschen haben ein großes Sicherheitsbedürfnis, zugleich wehren sich viele gegen Maßnahmen, die Sicherheitspolitiker als wirksam erachten. Das ist nur eines der Spannungsfelder inmitten einer komplexen Gemengelage rund um Kriminalität und Terror. Experten versuchen beim RP-Wirtschaftsforum „Sicherheit in Deutschland", in dem brandaktuellen Thema für Durchblick zu sorgen – und dabei auch zu zeigen, was die Sicherheitsbranche dabei leisten kann.

VON JÜRGEN GROSCHE

Schaut man die Nachrichten an oder hört sich im Freundes- und Bekanntenkreis um, scheint es derzeit vor allem ein Thema zu geben: Sicherheit. Gefühlt nehmen Bedrohungen aller Art zu – Diebstähle und Einbrüche, Cyberkriminalität, Terror.

Doch die Statistiken sagen zumindest in Teilen etwas anderes: Laut aktueller Polizeilicher Kriminalstatistik (für 2017) ist die Kriminalitätsentwicklung in Nordrhein-Westfalen rückläufig. Die Zahl der Straftaten ist im vergangenen Jahr um 6,5 Prozent zurückgegangen – nach Angaben des Innenministeriums ist das der stärkste Rückgang seit mehr als 30 Jahren.

Insbesondere am Rückgang von Wohnungseinbrüchen (minus 25,7 Prozent) haben die Bürger selbst einen Anteil. Sie lassen sich intensiver beraten und sichern ihr Heim besser. Die Cyberkriminalität nimmt hingegen immens zu. Und aktuelle Fälle zeigen: Auch die Terrorgefahr bleibt virulent.

Das Thema Sicherheit bleibt ganz oben auf der Tagesordnung. Grund genug, dazu Spezialisten zu Wort kommen zu lassen, die die Hintergründe kennen, die etwas dazu zu sagen haben. Beim RP-Sicherheitsforum „Sicherheit in Deutschland" tauschten sich Vertreter renommierter Sicherheitsunternehmen, aus Verbänden, der Politik sowie der Wirtschaft aus, um den Stand der Dinge zu diskutieren, aber auch Wege aufzuzeigen, wohin die Sicherheitspolitik gehen soll.

Konkrete Ansprechpartner dafür hatten sie: NRW-Innenminister Herbert Reul (CDU) stellte sich der Diskussion ebenso wie Wolfgang Bosbach, Vorsitzender der NRW-Regierungskommission „Mehr Sicherheit für Nordrhein-Westfalen", der Düsseldorfer Polizeipräsident Norbert Wesseler und Düsseldorfs Ordnungsdezernent Christian Zaum.

In einem sind sich alle einig: Bei aller Statistik sind die Bedrohungen virulent, zugleich aber auch Widerstände gegen entsprechende Maßnahmen. Ein Widerspruch: „In Deutschland war der Wunsch nach Sicherheit nie so ausgeprägt wie heute", greift Oliver P. Kuhrt, Geschäftsführer der Messe Essen, die Stimmungslage auf. Sie könne genutzt werden, um die Umsetzung von Sicherheitsmaßnahmen nach vorn zu bringen.

„Die Chancen sind gut, schwieriger wird es, ein Bekenntnis zu notwendigen Maßnahmen zu bekommen", wendet Reul indes ein und denkt dabei sicherlich auch an die Widerstände gegen das geplante neue Polizeigesetz für NRW. „Die schweigende Mehrheit muss auf die Straße kommen", fordert der Mininster. Die Menschen sollten sich auch in ihrem privaten Umfeld dafür einsetzen.

Mangelnde Zustimmung zu wirksamen Sicherheitsregelungen beklagt auch Wolfgang Bosbach. Er leitet die Sicherheitskommission des Landes NRW, in der Sicherheitsexperten an konkreten Vorschlägen für eine Stärkung der Sicherheitsarchitektur in NRW arbeiten. „Wir können die Herausforderungen des 21. Jahrhunderts nicht mit den Methoden des 20. Jahrhunderts meistern", sagt Bosbach und betont unter anderem die Bedeutung von Mindestspeicherfristen in der Telekommunikation für die Verhinderung und Aufklärung von Straftaten. Was die Polizei rechtlich dürfe, müsse sie auch technisch können. Zu oft werde das Schicksal von Verbrechensopfern kaum beachtet.

Beim Thema Vorratsdatenspeicherung sieht IT-Experte Thomas Tschersich von T-Systems einen „Drang, an manchen Stellen ins Absurde zu gehen". Tschersich lenkt den Blick weg von den Telefonverbindungsdaten: „IP-Adressen sind heute wichtiger. Aber Ermittlungen laufen oft ins Leere, weil die Daten nicht mehr da sind." Um Cyberangriffe abzuwehren, müssten „mit Augenmaß neue rechtliche Regelungen" gefunden werden, betont der Experte. ...

Fortsetzung des Artikels auf Seite 2. Lesen Sie auf den folgenden Seiten auch weitere Beiträge zu den Diskussionen im Forum sowie spannende Hintergrundinformationen rund um das Thema Sicherheit.

Kampf um die Maßnahmen

(Fortsetzung von Seite 1) Tragen nicht auch die Medien eine Mitschuld daran, dass das Thema Sicherheit von allen Seiten so emotional geführt wird? Dem widerspricht Tom Bender, Geschäftsführer Rheinische Post Verlagsgesellschaft, vehement: „Wir machen keine Themen - wir berichten über sie, ob sie uns gefallen oder nicht."

Das Sicherheitsbedürfnis wachse, weil auch die Unsicherheit zunehme. „Kommunikation ist hier ein zentrales Thema", sagt Bender und appelliert damit auch an die Gesprächsrunde, für Aufklärung zu sorgen.

Dabei komme es auf Transparenz an, fügt Reul hinzu: „Wenn man transparent ist, gewinnt man an Glaubwürdigkeit." Dazu gehöre auch eine korrekte Angabe von Zahlen etwa in der Ausländerkriminalität.

Insbesondere den Vertretern von Unternehmen aus der Sicherheitsbranche brennt noch ein ganz anderes Thema unter den Nägeln: Wie steht es um die Zusammenarbeit der privaten Sicherheitswirtschaft mit öffentlichen Stellen? Dazu mehr auf den Seiten 8 bis 11. Interviews mit den Teilnehmern und weitere Informationen über die Veranstaltung finden Sie zudem im Video auf der Internetseite www.rp-forum.de.

Entgegen der allgemeinen Stimmungslage nimmt die Kriminalität ab. Die Zahlen müssen allerdings interpretiert werden, sagen Experten. Auch darum ging es beim RP-Forum „Sicherheit". GRAFIK: ZWEIMETERDESIGN

Wie steht es um die Sicherheit in Deutschland? Darüber tauschten sich Experten und Politiker beim RP-Wirtschaftsforum „Sicherheit" in Räumen der Rheinischen Post in Düsseldorf aus. FOTO: ALOIS MÜLLER

HAUS UND WOHNUNG

Besser einen Schritt voraus

Es ist ein andauerndes Wettrüsten zwischen Kriminellen und allen, die sich schützen wollen. Einbrecher seien oft einen Schritt voraus, heißt es. Es sei denn, Wohnungsbesitzer halten sich ebenfalls auf dem aktuellen Stand der Dinge.

VON JÜRGEN GROSCHE

Selbst wenn man mit einem Kuhfuß mit voller Wucht auf die mit Spezialfolie verstärkte Scheibe schlägt, kann man sie nicht zertrümmern. Das demonstriert Ulrich Weynell vom Unternehmen ISN Technologies (links) zusammen mit einem Mitarbeiter beim RP-Forum „Sicherheit". FOTOS: MICHAEL LÜBKE

Die Kriminalstatistik weist für 2017 einen Rückgang der Wohnungseinbrüche aus – eigentlich eine gute Nachricht. Die Polizeibehörden erfassten für das vergangene Jahr insgesamt rund 117.000 Einbrüche – sowohl versuchte wie auch vollendete. Das sind 23 Prozent weniger als 2016. Die Aufklärungsquote erhöhte sich leicht auf 17,8 Prozent. Im Jahr 2016 hatte sie noch bei 16,9 Prozent gelegen.

Klingt gut. Auf der anderen Seite heißt das aber: „Immer noch werden mehr als 80 Prozent der Wohnungseinbrüche nicht aufgeklärt", sagt Ulrich Weynell, Vorstandsvorsitzender des Sicherheitsunternehmens ISN Technologies, der die Statistik damit für irreführend hält. Zudem sind die Wohnungsbesitzer selbst aktiver als früher, schützen sich mehr und tragen so dazu bei, dass Einbrüche erfolglos bleiben. „Viele Täter ziehen weiter, wenn sie für einen Einbruch zu lange brauchen", erklärt Weynell.

Es bleibt – und wird zunehmend – Aufgabe der Bürger, für Sicherheit zu sorgen. „Wir müssen uns selbst schützen", mahnt Weynell, „vieles kann der Staat nicht mehr leisten". Der Sicherheitsexperte rät aber auch zu einer gewissen Gelassenheit: „Hundertprozentigen Schutz gibt es nicht. Wir müssen mit Restrisiken leben." Die können Wohnungsbesitzer aber minimieren, wie Weynell und Mitarbeiter von ISN eindrücklich beim RP-Sicherheitsforum „Sicherheit in Deutschland" veranschaulichen.

Sicherungsmaßnahmen müssen keine optische Festung aus einem Haus machen. „Man ist heute in der Lage, Gebäude sicherheitstechnisch so auszustatten, dass sie ohne Beeinträchtigung der Optik, des Designs oder der Handhabung gesichert sind", betont Weynell und erläutert, worauf es ankommt: „Ein Gebäude hat bei den Fenstern drei Schwachstellen: Glas, Beschlag und Rahmen."

Und für alle drei Bereiche gibt es Lösungen. Beispiel Scheibe: Selbst standardmäßiges, vier Millimeter dickes Glas lässt sich heute durch Spezialfolie so sichern, dass Einbrecher selbst mit Hammerschlägen die Scheibe nicht so zertrümmern können, dass sie durchs Fenster einsteigen könnten. Die Scheibe zersplittert zwar, aber das Glas wird durch die Folie zusammengehalten.

Den Beschlag öffnen Einbrecher gerne, indem sie ins Getriebe bohren. Dagegen kann man sich mit Schlössern schützen. Nun haben sich die Täter etwas Neues überlegt: Sie brechen das Fenster neben dem Öffnungshebel auf und legen den Griff von innen so um, dass sie das Fenster öffnen können. Doch auch hierfür können Weynell und seine Mitarbeiter Gegenmittel präsentieren: eine Pilzkopfzapfenverriegelung. Sie erschwert es den Missetätern, das Fenster aufzuhebeln.

„80 Prozent der Täter brechen durch Fenster und Rahmen ein", weiß Weynell, „und sie brauchen im Schnitt zehn Sekunden dafür." Umso wichtiger sei ein effizienter Schutz. Zumal sich eine neue Tätergruppe ausbreitet: Organisierte Profis, die sich auch durch eine gute mechanische Sicherung nicht abschrecken lassen. Sie ziehen nicht weiter, wenn es länger dauert. „Wir erzielen hier Top-Resultate, indem wir die mechanische Sicherung mit der elektronischen kombinieren", sagt Weynell. Die Spezialisten installieren eine funkbasierte Alarmtechnik, also ohne Kabel verlegen zu müssen. Die Anlage sendet bei Einbruchsversuchen sofort eine Meldung an die Alarmzentrale.

Das System zeichne sich gleich durch mehrere Vorteile aus, erläutert der Experte. Zum einen: „Die Zeit läuft gegen die Täter." Wegen der aufgerüsteten mechanischen Sicherung brauchen die Einbrecher länger. Die Alarmzentrale wiederum empfängt in Echtzeit Bilder vom Tatort, die Wachleute können sie sofort an die Polizei leiten, die ebenso schnell reagieren kann. „Wichtig ist, dass es hier keine Fehlalarme gibt", fügt Weynell hinzu. Denn sonst verliere die Polizei das Vertrauen in den Sicherheitsdienst.

Daher nutzt ISN VdS-zertifizierte Anlagen, zudem ist die Sicherheitsleitzentrale nach DIN EN 50518 zertifiziert und entspricht damit der höchsten europäischen Norm. Ein solches System genießt in der Branche und bei der Polizei hohe Reputation.

Was gar nicht geht: Fenster offenzulassen. „Auch ein gekipptes Fenster wird von der Versicherung wie ein offenes Fenster gewertet", gibt Weynell zu bedenken. Es gebe heute aber auch eine Lösung dafür, Fenster im gekippten Zustand zu sichern. „Wenn die Lösung zertifiziert ist, akzeptiert die Versicherung das." Und selbst wenn die Täter dann KO-Gas ins Haus leiten, gibt es ein Gegenmittel: KO-Gas-Melder.

Die Entwicklung wird allerdings weitergehen, weiß der Experte auch: „Die Kriminellen informieren sich auf Sicherheitsmessen über die neuesten Maßnahmen." Also müssen sich auch Wohnungsbesitzer auf dem Laufenden halten. Der Kampf zwischen Gut und Böse geht weiter, aber die gute Seite hat immer bessere Argumente.

Ulrich Weynell (rechts) erklärt beim RP-Forum „Sicherheit" auch, wie Diebe Fenster aufhebeln und was man dagegen tun kann.

extra
Sicherheit

Verlag:
Rheinische Post Verlagsgesellschaft mbH, Zülpicher Straße 10, 40196 Düsseldorf
Geschäftsführer: Johannes Werle, Patrick Ludwig, Hans Peter Bork, Tom Bender (verantwortl. Anzeigen)
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, Monschauer Straße 1, 40549 Düsseldorf, José Macias (verantwortlich), Jürgen Grosche, Mitarbeit: Dr. Patrick Peters
Kontakt: 0211 528018-12, redaktion@rheinland-presse.de

STRATEGIE

Sicherheitskonzepte: Profis beraten Kommunen

Es ist eine komplexe Aufgabe, für Ordnung und Sicherheit zu sorgen. Immer mehr Gemeinden greifen beim Erstellen von Konzepten dafür auf professionelle Berater zurück.

VON JÜRGEN GROSCHE

Das Thema Ordnung und Sicherheit hat an Stellenwert gewonnen. Das merkt man auch daran, dass Kommunen das Thema auf ihren Tagesordnungen höher ansetzen. Stefan Bisanz und Uwe Gerstenberg, Geschäftsführer des Sicherheitsberatungsunternehmens consulting plus, stellen das ganz konkret in Form von neuen Anfragen fest. „Die Zeit ist jetzt reif, Städte und Gemeinden sind bereit, mehr in Sicherheit zu investieren“, sagt Gerstenberg.

Immer mehr Gemeinden machen sich dabei nicht nur Gedanken darüber, wie Ordnung und Sicherheit gestärkt werden können. Sie suchen professionellen Rat, und hier kommt consulting plus ins Spiel. „Wir beraten und unterstützen die Kommunen bei der Analyse, der Planung der Sicherheitsarchitektur, der Umsetzung und auch bei der Evaluierung der Ergebnisse“, erklärt Bisanz. Die Auftraggeber entwickeln zusammen mit den Spezialisten zunächst die Sicherheits-Philosophie: Was will man unter Ordnung und Sicherheit überhaupt verstehen? Darauf setzen Analyse und Strategieberatung an. Die Experten klären zusammen mit ihren Gesprächspartnern, was selbst erledigt werden kann und welche Leistungen dazugekauft werden.

Beispiele aus der Praxis: Die Stadt Essen will eine der sichersten Großstädte in Deutschland bleiben. Man ist mit consulting plus darüber im Gespräch. Was können die Sicherheitsexperten da einbringen? Zum einen Präventionsprogramme. Das fängt sehr früh an. „Das Thema gehört bereits in die Stadtplanung“, betont Gerstenberg. Dunkle Ecken sollten vermieden werden, eine gute Beschilderung ist ebenso wichtig wie weite Sichtflächen. „Und man muss die Anwohner und Nachbarn einbeziehen“, rät Bisanz. „Man muss ein Klima schaffen, dass Nachbarn sich für Ordnung und Sicherheit mit zuständig fühlen“; das könne auch durch Anreize wie Nachbarschaftsfeiern gefördert werden.

Zur Abwehr von Terrorattacken fokussieren sich viele Kommunen derzeit darauf, Poller gegen Lkw zu platzieren. Das allein reiche nicht, bemängelt Gerstenberg: „Ein Attentat mit einem Lkw ist für Terroristen ja nur eine von tausend Möglichkeiten.“ Wenn schon Lkw-Sperren errichtet werden, könne man sie auch für andere Zwecke einsetzen, zum Beispiel, um die Aufenthaltsqualität zu verbessern. So könnte man die Stadtmöblierung (Sitzgelegenheiten, Pflanzenkübel, Bushaltestellen oder Litfasssäulen) mit Beton verstärken und zugleich zur Terrorabwehr nutzen. Zu einer umfassenden Beratung der Kommunen gehört aber mehr. Zunächst geht es darum, Informationen zu sammeln, zu bündeln und auszuwerten, erklären die beiden Sicherheitsstrategen: Wo entwickeln sich Kriminalitätsschwerpunkte, in welcher Art und Weise? Welche Kräfte müssen wo eingesetzt werden? Reichen Mitarbeiter des Ordnungsamtes, oder sollten private Sicherheitsdienste, Polizei oder der Zoll dazugezogen werden?

In Essen habe man die Zeichen der Zeit erkannt, sagt Bisanz: „Die Stadt will die Ordnungsmacht wieder in ihre Zuständigkeit zurückholen.“ Bisanz rät zu einem solchen ganzheitlichen Ansatz, alle Zuständigkeiten zusammenzufassen. Das Unternehmen consulting plus versteht sich in diesen Prozessen als Partner der Kommunen, der die Entscheider strategisch begleitet. Wenn zum Beispiel Aufträge für Sicherheitsunternehmen ausgeschrieben werden, beraten die Experten neutral den Ausschreibungsprozess – sie bewerben sich in solchen Fällen nicht selbst um die operativen Tätigkeiten. Aber sie haben Branchenkenntnis, können zeigen, wo ein Angebot Schwächen hat oder wo es stark ist. „Wir raten immer dazu, nicht den Preis, sondern die Qualität als ausschlaggebendes Kriterium zu nehmen“, betonen beide Geschäftsführer.

Die Stadt Essen will eine der sichersten Großstädte in Deutschland bleiben und sucht dafür auch den Rat von Experten. FOTO: PETER PRENGEL, STADT ESSEN

Darüber hinaus begleiten die Experten die Kommunen beim Aufbau einer Sicherheitsarchitektur in allen weiteren Stufen, also auch beim Qualitätsmanagement. „Wir lassen uns daran messen, ob unsere Vorschläge auch umsetzbar sind“, sagt Bisanz. Letztlich ist das Ganze ein Vertrauensgeschäft – umso wichtiger, dass das Sicherheitsunternehmen auch in seinen operativen Angeboten Qualität zeigt. So gehört eine eigene Ausbildungs- und Fortbildungsakademie zum Unternehmen.

Da erstaunt es nicht, dass man consulting plus schon einige spannende Projekte anvertraut hat, zum Beispiel das Sicherheitskonzept für Olympia 2012. In der operativen Arbeit sind die Experten aber ebenfalls gefragt – auch für so sensible Themen wie die Bewachung von Kasernen. Ein Punkt übrigens, den Gerstenberg und Bisanz gerne ins Feld führen, wenn solche Tätigkeiten als hoheitliche Aufgaben bezeichnet werden, die man nicht privaten Dienstleistern überlassen solle. „Das funktioniert bei der Bundeswehr seit über 30 Jahren“, sagt Gerstenberg. „Warum soll das woanders nicht möglich sein?“

Mittelstand: Risikofaktoren präventiv absichern

Die Unternehmensberatung Geos Germany begleitet mittelständische Unternehmen und Konzerne bei ihren sicherheitsrelevanten Fragestellungen. Im Fokus steht, Ausfälle des Geschäfts zu vermeiden.

VON PATRICK PETERS

Jens Washausen hat einen unverstellten Blick auf die Praxis. „Trotz täglicher Nachrichten über eine komplexer werdende Sicherheitslage und regelmäßiger Vorfälle auch in Europa ignorieren viele mittelständische Unternehmen das Thema der Unternehmenssicherheit völlig. Das Management schaut einfach weg und scheut die Beschäftigung damit – oftmals vor dem Hintergrund, dass bestehende Risiken einfach nicht wahrgenommen werden wollen oder weil professionelle Gesprächspartner auf Augenhöhe fehlen.“ Jens Washausen ist Geschäftsführer der Unternehmensberatung Geos Germany, die seit vielen Jahren mittelständische Unternehmen und Konzerne bei ihren sicherheitsrelevanten Fragestellungen begleitet.

Die IT gehört zu den sensibelsten Bereichen eines Unternehmens. Die Firmen sollten sie daher gut sichern. FOTO: THINKSTOCK/KYNNY

Er will daher auch seine Stimme erheben und Unternehmer dafür sensibilisieren, sich mit der Sicherheitsthematik umfassend auseinanderzusetzen. Vor allem der Schutz vor Cyber-Kriminalität und der Schutz kritischer Infrastrukturen stehen dabei im Fokus. Allein Angriffe auf die IT führen zu Schäden in Höhe von 55 Milliarden Euro jährlich für die deutsche Wirtschaft. „Daher haben wir Konzepte entwickelt, die sich insbesondere an den Mittelstand richten und die Bedürfnisse und Notwendigkeiten der Unternehmen erfassen und umsetzen. Wir bauen als Berater auf Augenhöhe Vertrauen auf und können die Geschäftsführung dann davon überzeugen, die richtigen Schritte zu ergreifen“, betont Jens Washausen.

Das Kernprodukt der Beratung bei Geos Germany ist das Risikomanagement. Dabei analysieren die Experten sämtliche Organisations- und Produktionsprozesse und entwickeln so den Blick dafür, in welchen Bereichen ein Unternehmen besonders bedroht ist, sei es durch Cyber-Kriminalität, Wirtschaftsspionage oder, oder, oder. Daraus ergeben sich dann die konkreten Handlungsmaßnahmen des Notfallmanagements. Dies zielt darauf ab, dass präventive Maßnahmen optimal greifen und ein Unternehmen im Rahmen des Notfall- und Krisenmanagements schnell, rechtskonform und erfolgreich handeln kann.

„Wir stellen die kritische Frage, wie lange ein Unternehmen den Ausfall eines wesentlichen Merkmals verkraften kann. Das kann die IT sein, das kann ein wichtiger Produktionsprozess sein – was passiert, wenn bestimmte Dinge nicht mehr funktionieren? Darauf suchen wir die Antwort und entwickeln dann eine strategische Planung dafür, welche Prozesse in Gang gesetzt werden müssen, um die Handlungsfähigkeit wiederherzustellen“, sagt Jens Washausen, der dieses Vorgehen als „Business Impact Analysis“ bezeichnet.

Es sei wichtig, dass aus der Beratung das Bewusstsein hervorgehe, wichtige Schritte im Vorfeld zu ergreifen und bestimmte Fähigkeiten für die Absicherung des Unternehmens zu ergreifen – in „Friedenszeiten“, wie der Geos Germany-Geschäftsführer sagt. Trete der Krisenfall dann doch ein, garantiert Geos Germany eine Reaktion innerhalb von 15 Minuten, und das rund um die Uhr.

Jens Washausen weist auch auf die persönlichen Haftungsrisiken von Geschäftsführern bei sicherheitsrelevanten Vorkommnissen hin. „Tritt ein solcher Fall auf und wird Organisationsverschulden festgestellt, kann das Management wegen eines fahrlässigen Umgangs mit seinen Pflichten im Sinne der sorgfältigen Geschäftsführung in Haftung genommen werden. Das kann zu erheblichen Forderungen gegen das Privatvermögen führen. Wirtschaftsschutz und persönlicher Vermögensschutz gehen Hand in Hand.“ Zumal Jens Washausen dabei auch noch eine weitere Komponente sieht. „Wer sich als Geschäftsführer einem solchen Organisationsverschulden ausgesetzt sieht, beschädigt seine Reputation als Manager und wird in Zukunft mit dem Fehlverhalten umgehen müssen. Eine berufliche Neuausrichtung wird dadurch nicht leichter.“

„Wir wollen Sicherheit erlebbar machen“

Günter Calaminus, Geschäftsführer der W.I.S. Unternehmensgruppe, stellt die Bedeutung der Digitalisierung von Sicherheitsdienstleistungen heraus. Durch die digitale Auswertung von Daten könne die Sicherheit erhöht werden.

VON PATRICK PETERS

Die Digitalisierung ist in aller Munde. Ob Gesundheit, Finanzdienstleistungen, Industrie oder, oder, oder: Immer mehr Unternehmen suchen Möglichkeiten, durch neue digitale Infrastrukturen ihr Geschäft zu entwickeln, neue Services für die Kunden anzubieten und die eigene Organisation immer effizienter zu machen.

Das gilt auch für das Sicherheitsgewerbe, wie Günter Calaminus sagt. Er ist Geschäftsführer der W.I.S. Unternehmensgruppe, einem deutschlandweit tätigen Sicherheitsdienstleister mit mehr als 100-jähriger Erfahrung und deutlich über 4000 Mitarbeitern. „Digitalisierung und Sicherheit gehören aus unserer Sicht einfach zusammen. Genaue Daten geben uns Aufschluss darüber, was passiert und wann etwas passiert – oder eben auch nicht. Dies können wir genau auswerten und dem Kunden gegenüber darstellen.“

Viele Vorfälle bekämen Kunden überhaupt nicht mit, weiß der Sicherheitsexperte aus der Praxis. „Um den Umgang mit organisatorischen, prozessualen und echten Sicherheitsrisiken zu verbessern und mehr Wissen zur Vermeidung solcher Risiken zu vermitteln, sind detaillierte Daten unerlässlich. Denn so können wir alles viel genauer dokumentieren, Erkenntnisse ableiten und miteinander in Verbindung setzen. Durch diese Informationen erhält der Kunde mehr Wissen und kann seine Organisation anders aufstellen, um mit uns gemeinsam präventiv tätig zu werden und auch den aktiven Wert von Sicherheitsdienstleistungen zu erkennen“, betont Günter Calaminus.

Der Ansatz dahinter: Die W.I.S. Unternehmensgruppe möchte Sicherheit erlebbar machen und genau aufzeigen, wie Unternehmens- und Wirtschaftsschutz funktioniert und welchen Mehrwert dies liefert. Dafür führen Günter Calaminus und seine Mitarbeiter in den Unternehmen vor, welche Sicherheitsrisiken im Alltag jederzeit auftreten können und mit welchen Maßnahmen man diesen begegnen kann. „Als Spezialist für Corporate Security und Safety wollen wir für alle Gefahren sensibilisieren und die Entscheider damit erreichen. Das ist der erste Schritt zu mehr Sicherheit und damit zu mehr wirtschaftlichem Erfolg.“ Für den Geschäftsführer ist dieser Zusammenhang eindeutig: Prosperität und Sicherheit hängen eng zusammen, und wenn die Sicherheit gefährdet ist, zieht dies in der Regel auch einen Rückgang der Leistungsfähigkeit eines Unternehmens nach sich.

Daher bedeutet Unternehmenssicherheit immer auch Werterhalt, sei es durch die Abwehr von Vandalismus und Einbruchdiebstahl oder auch die Verhinderung von schwerwiegenden Straftaten wie Spionage und Datenklau. „Kritische Daten und Informationen werden nicht nur von Cyber-Kriminellen entwendet. Auch physische Diebstähle von Blaupausen, Konstruktionen, Verträgen, Mitarbeiterdaten etc. sind an der Tagesordnung. Daher gehört zur Cyber-Security immer auch der analoge Schutz einer Einrichtung inklusive aller kritischen Bereiche. Denn was ist, wenn zwar die Netzwerkstrukturen vor Eindringlingen geschützt sind, aber der Server einfach entwendet wird?“, gibt Günter Calaminus ein Beispiel, wie es leider gar nicht so selten vorkommt.

Der W.I.S.-Geschäftsführer spricht sogar von „täglichen Zugriffen“, die für ein Unternehmen hochbedrohlich sein können – man stelle sich zum Beispiel den Fall vor, dass ein Wettbewerber Pläne für eine neue Maschine entwendet. Oder es kämen Personalakten mit schützenswerten Daten abhanden. „Dies bedingt auch erhebliche Haftungsrisiken für einen Geschäftsführer. Davor gilt es das Management eines Unternehmens ebenso zu bewahren. Wir schützen unsere Kunden durch individuelle Sicherheitskonzepte vor diesen Gefahren.“

Digitalisierung in der Sicherheitsdienstleistung setzt aber laut den Erfahrungen von Günter Calaminus voraus, dass ein Anbieter selbst wirklich digital aufgestellt ist. W.I.S. hat zuerst eine interne Struktur geschaffen, um überhaupt digital auftreten zu können, und dabei eine hohe Transparenz und ein professionelles System für den Umgang mit den Daten geschaffen – eine Frage der Unternehmenskultur, wie der Chef sagt. Erst danach wurden die Angebote bei den ersten Kunden implementiert.

Mit Erfolg, übrigens: „Wir erhalten sehr gute Rückmeldungen und werden daher die Kompetenz unserer Mitarbeiter vor Ort mit digitalen Möglichkeiten immer stärker kombinieren.“

Daten und IT-Einrichtungen sollten gut gesichert sein. Unternehmen brauchen hier den Rat von Spezialisten. FOTO: THINKSTOCK/PESHKOV

CYBERKRIMINALITÄT

Foto: Thinkstock/chaiyapruek2520

VON JOSÉ MACIAS

Mutig war er schon, als er 2002 sein Unternehmen für IT-Risikomanagement gründete. „Damals spielte IT-Sicherheit im Markt keine nennenswerte Rolle“, erinnert sich Wolfgang Straßer. Firewalls, Antiviren- und Antispamprogramme – das waren zu jener Zeit die üblichen Mittel gegen Gefahren, die von Angreifern drohten. Der Gründer des Leichlinger IT- Sicherheitsspezialisten @-yet GmbH wird für seinen Mut jetzt belohnt: Die Auftragsbücher sind voll von Nachfragen aus nahezu allen Branchen: Dax-Konzerne, kleine und mittelständische Betriebe aus Handel, Automotive, Banken, Versicherungen, Pharma, Gesundheitswesen oder auch Handwerk geben sich bei den Leichlingern die Klinke in die Hand.

„Das Bedrohungsszenario hat sich komplett geändert. Durch die totale Durchdringung und Abhängigkeit der Unternehmen von IT und Internet merken viele Manager, dass Digitalisierung ohne digitale Sicherheit undenkbar, gar existenzgefährdend sein kann!“, berichtet Straßer. Mit rund 40 festangestellten Mitarbeitern zählt @-yet nunmehr zu den größeren im Bereich IT-Risikomanagement.

Die Branche ist klein, hochspezialisiert – und vor allem absolut verschwiegen. „Keine Namen!“, stellt er deshalb klar. Dabei könnte der IT-Spezialist „hunderte von Geschichten erzählen“, wie sich Angreifer mittlerweile auf breiter Front Zugang zu den IT-Infrastrukturen deutscher Unternehmen verschaffen. „Es gibt immer noch viele Unternehmenslenker, die behaupten, bei ihnen sei nie etwas in Bezug auf IT-Angriffe passiert – dabei wissen viele gar nicht, dass ihre Daten längst abgesaugt wurden“, erläutert Straßer.

Lange Jahre lang war allein im Bereich Industriespionage offensichtlich, woher die Angriffe kamen: China, Russland, USA – dort saßen die üblichen Verdächtigen. Doch in Sachen Cybersecurity hat sich die Welt dramatisch verändert: „Vor allem die Organisierte Kriminalität hat deutlich zugelegt: Nahezu alle deutschen Unternehmen stehen dabei im Fokus, weil diese Banden vor allem darauf aus sind, an das Geld zu kommen – sei es durch Erpressung, sei es durch Betrug oder andere Szenarien.“

Wolfgang Straßer macht zudem deutlich, warum Cyberkriminalität boomt: „Das Geschäft ist äußerst einträglich: Schon jetzt werden mit Cybercrime mehr Umsätze gemacht als mit dem Drogenhandel. Dahinter stecken auch mafiöse Strukturen – also die gleichen Banden, die schon mit Drogen, Menschenhandel und Prostitution ihr Geld verdienen.“

Hinzu kommt, dass die Entdeckungsgefahr bei Cyberangriffen deutlich geringer ist. Und das, obwohl laut Straßer gerade Nordrhein-Westfalen mit dem Landeskriminalamt und der Schwerpunkt-Staatsanwaltschaft in Köln über die seiner Meinung nach „besten Ermittler in diesem Bereich in Deutschland“ verfügt. „Aber sobald die Angriffe aus dem Ausland kommen, sind den Ermittlern oftmals die Hände gebunden.“

Zurück zu den Angreifern: Neben Industriespionen und Organisierter Kriminalität drohen Gefahren auch aus der Hacker-Szene. „Nicht zu vergessen sind auch die Innentäter –

„Sobald die Angriffe aus dem Ausland kommen, sind den Ermittlern oft die Hände gebunden“

oftmals Mitarbeiter aus dem eigenen Unternehmen, die aus Frust Rache üben wollen.“ Eines käme dabei allein Angreifern zugute. Im Gegensatz zu 2002, als Internet und E-Mails noch nicht geschäftskritisch waren, „stehen Wirtschaft und Gesellschaft heute in einer dramatischen Abhängigkeit zur Informationstechnologie“.

Der Risikomanager schätzt, dass nur rund zehn bis zwanzig Prozent der Unternehmen tatsächlich über eine angemessene sichere IT-Infrastruktur verfügen. „Das ist zu wenig! Und wenn ein Unternehmer darauf verweist, dass er doch über eine eigene IT-Abteilung verfügt, heißt das gar nichts: Wenn ich IT kann, kann ich noch lange nicht IT-Sicherheit.“

Der @-yet-Chef bedauert, dass die Unternehmen in der Vergangenheit den IT-Sicherheitsaspekt zu wenig beachtet und zu wenig Geld in die Prävention gesteckt haben. Heute werden seine Mitarbeiter nicht nur dann zu Hilfe gerufen, wenn Produktionen durch Angriffe stillgelegt oder Datendiebstähle entdeckt werden – immer häufiger führen sie im Auftrag der Unternehmen selbst Angriffe durch, um die Schwachstellen der Auftraggeber zu entdecken. „Viele Unternehmen machen es den Angreifern immer noch zu leicht. Denn nicht nur die Technik muss auf dem neuesten Stand sein, auch die Schnittstelle Mensch gilt es zu beachten“, so Straßer.

So mancher spektakuläre Fall ist der breiten Öffentlichkeit bekannt geworden. Der sogenannte „CEO-Fraud“ funktioniert aber immer noch: Dabei werden Unternehmen ausspioniert und E-Mails gefälscht, mit denen sich die Angreifer als Geschäftsführer oder Vorstand ausgeben, um dann eine Geldüberweisung anzuweisen. Einem Unternehmen entstand so ein Schaden von 40 Millionen Dollar.

Kritisch sieht der IT-Risikomanager auch den Einsatz vieler Innovationen, wie etwa Cloud-Technologien. „Clouds sind alles – nur nicht die Lösung der Sicherheitsprobleme“, konstatiert Wolfgang Straßer. „Wir haben über hundert Cloud-Lösungen untersucht, aber nur einen gefunden, dessen Daten tatsächlich vor Diebstahl geschützt sind.“ Auch von biometrischen Lösungen, wie sie neuerdings bei Smartphones angeboten werden, hält der Leichlinger Unternehmer nicht viel. „Ein Passwort ist immer noch sicherer, weil veränderbar, als ein Zugang per Fingerabdruck oder die Iris des Auges. Die lässt sich nämlich mit einem normalen Fotoapparat in bester Qualität festhalten – und schon haben wir einen Zugang zum Smartphone.“

Mit den Passwörtern ist das aber so eine Sache, die meisten sind doch nicht wirklich sicher. Straßer rät daher allen Anwendern, Passwörter mit mindestens 16 Stellen zu verwenden. „Den Namen des Haustiers oder das eigene Geburtsdatum sollten Sie dabei aber nicht für das Passwort verwenden. Ich finde meine Passwörter in der Zeitung: Eine prägnante Überschrift zum Beispiel, bei der ich einige Buchstaben durch Zahlen ersetze, das ist der beste Schutz und lässt sich gut merken.“


Foto: Thinkstock/the-lightwriter

INTERNETKRIMINALITÄT

Schutzlos gegen Cyberangriffe?

VON JOSÉ MACIAS

Mit der Datensicherheit ist das in deutschen Unternehmen so eine Sache. Die IT-Abteilungen strengen sich an, um die Daten vor Diebstahl zu schützen, doch funktioniert das wirklich? Klaus M. Brisch von der Wirtschaftskanzlei DWF in Köln schüttelt den Kopf. Der renommierte Fachanwalt für Informationstechnologierecht hat international einen guten Überblick über die tatsächliche Bedrohungslage.

Und die sieht alles andere als gut aus: „Die Schäden, die jährlich in deutschen Unternehmen durch Cyberdiebstahl entstehen, sind hoch: rund 54 Milliarden Euro. Europaweit schätzen wir die Schäden auf insgesamt 327 Milliarden Euro.“ Zahlen, die aufhorchen lassen.

Sind denn nicht gerade deutsche Firmen dafür bekannt, besonders penibel auf ihre Daten zu achten? „Im europäischen Vergleich ist Deutschland tatsächlich etwas besser aufgestellt, weil wir hier seit Jahren den Datenschutz durch technische Anforderungen sicherstellen mussten. Allerdings ist Deutschland im weltweiten Vergleich allenfalls Durchschnitt – in der Spitze sind wir schlecht“, konstatiert Brisch.

Wie schlecht es um die Cybersecurity bestellt ist, macht der weltweite Leiter des Technologiesektors am Beispiel Großbritannien deutlich. Hier seien über 50 Prozent aller Unternehmen schon einmal Opfer von Datendiebstahl geworden. „Die Schäden betragen dort im Durchschnitt zwischen 1000 und 9000 Pfund – was zeigt, dass gerade auch kleine und mittelständische Unternehmen oft Ziel von Cyberangriffen sind“, berichtet der Experte. „Schlimmer ist aber, dass die andere Hälfte der Unternehmen glaubt, nicht betroffen zu sein. Dabei sind bei vielen dieser Firmen die Daten längst abgeschöpft worden – sie haben es nur nicht bemerkt.“

Die Sorglosigkeit im Umgang mit Datensicherheit ist gerade auch in deutschen Unternehmen stark verbreitet. „Das Management vertraut oftmals blind den Aussagen der IT-Abteilungen, dass alles sicher sei. Die Wahrheit ist: Die IT-Abteilungen sind in der Regel nicht in der Lage, Cyberangriffe abzuwehren, denn sie unterschätzen die Qualität der Angriffe und konzentrieren sich immer noch darauf, dass die Systeme schlicht laufen.“

Klaus M. Brisch ist aber keiner, der weitere gesetzliche Regelungen und noch schärfere Gesetze fordert. „Das führt nur zu noch mehr Kosten und Bürokratie. Effektive Datensicherheit beginnt schon mit der Rolle, die der IT-Cybersecurity in einem Unternehmen zugesprochen wird“, kritisiert der IT-Fachanwalt: „Viele Manager sehen Cybersecurity als Kostenfaktor, dabei ist es ein Nutzenfaktor, der erheblich zur positiven Reputation eines Unternehmens beitragen kann!“ Er ist davon überzeugt, dass es sich gerade international tätige Firmen in Zukunft nicht mehr leisten können, nachlässig mit ihrer Datensicherheit umzugehen. „Verträge werden in Zukunft nur noch mit Partnern geschlossen, die nachweisen können, dass sie über ein funktionsfähiges Cybersecurity-Management verfügen.“

Genau hier setzen Brisch und die international tätige Wirtschaftskanzlei an: Die Wirtschaftsanwälte kümmern sich zwar selbst nicht um die technischen Prüfungen, aber sie unterstützen die Unternehmensführungen dabei, den Prozess hin zu einer neuen Sicherheitsarchitektur intern im Unternehmen und extern mit technischen Dienstleistern zu steuern.

Doch Klaus M. Brisch sieht auch den Staat in der Pflicht. Ein positives Beispiel ist für ihn Israel: „Als der Computervirus WannaCry weltweit hunderttausende Rechner befiel, passierte bei Israels Firmen nichts. Hintergrund ist, dass Israel ein Frühwarnsystem für Unternehmen betreibt, mit dem alle Firmen im Rahmen von Notschleifen frühzeitig informiert werden. In Deutschland gibt es ein solches System für die Wirtschaft nicht.“ Zwar gebe es mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine staatliche Stelle, die Informationen zu Cyberrisiken sammelt – allerdings würden diese Informationen nicht in Echtzeit und flächendeckend für die deutsche Wirtschaft zur Verfügung gestellt.

Brisch hat hier eine klare Vision: „Wir denken etwa an eine elektronische Plattform, die für die Wirtschaft in real-time Informationen über Cyber-Bedrohungslagen zur Verfügung stellt. Das braucht natürlich klare Regeln für alle, die sich an dieser elektronischen Plattform beteiligen“, argumentiert der Wirtschaftsanwalt. „Vor allem würde der deutsche Mittelstand von einer solchen Lösung profitieren, da sogenannte „kritische Infrastrukturen durchaus über unmittelbare Kontakte zu Sicherheitsbehörden verfügen.“

Die Zeit drängt, wie ein Blick auf die Angreifer zeigt. Die sind technisch auf dem neuesten Stand und oft militärisch organisiert: Schätzungen zufolge setzt allein Nordkorea über 7000 Hacker ein, die weltweit Cyberattacken starten.

Wann kommen die Roboter?

VON JOSÉ MACIAS

Wer einen kleinen Ausblick in die Zukunft der privaten Sicherheitsfirmen haben will, fährt am besten dorthin, wo die halbe Welt ohnehin die meisten IT-Innovationen erwartet: in das kalifornische Silicon Valley. „Dort haben wir die ersten Roboter im Einsatz“, berichtet Daniel Schleimer. Roboter, die Aufgaben von Wachpersonal übernehmen, das ist in Deutschland derzeit noch eine Zukunftsvision. Zu Testzwecken hat Securitas Deutschland die ersten zwei Wachroboter schon bestellt. Der Geschäftsführer der Securitas NRW ist überzeugt: „Das wird auch hier in Deutschland kommen: Etwa die Hälfte der Dienstleistungen im Sicherheitsbereich, die heute mit Personal umgesetzt werden, werden in Zukunft durch technische Lösungen geleistet, teilweise auch mit Robotern!“

Beim Redaktionsbesuch zeigt der regionale Leiter von Securitas in Nordrhein-Westfalen auf, vor welchen Herausforderungen seine Branche steht. Er muss es wissen, zählt doch der schwedische Sicherheitsgigant mit über 343.000 Mitarbeitern weltweit (davon 21.500 in Deutschland) zu den erfahrensten und erfolgreichsten Sicherheitsdienstleistern. „Wir müssen allein schon deshalb mehr Technik einsetzen, weil auch diese Branche immer mehr Anreize setzen muss, um passendes Personal zu finden.“

Dafür sorgt auch die technische Entwicklung, die die Angreifer immer findiger werden lässt. Heute müssen Securitas-Mitarbeiter nicht nur Personenkontrollen in Firmen und öffentlichen Gebäuden beherrschen, sie müssen sich auch mit ganz neuen Gefahren auseinandersetzen. „Die Abwehr von Drohnen etwa ist in den letzten Jahren zu einer neuen Herausforderung geworden“, erläutert der Geschäftsführer. So wollten in Hamburg Neugierige schon vor der Taufe eines Kreuzfahrtschiffes mit einer Drohnenkamera Bilder erhaschen – Securitas konnte hier schnell den „Piloten“ ermitteln, zum Glück ein harmloser Fall. „Wir selbst haben Drohnen ebenfalls im Einsatz, etwa Feuerwehr-Drohnen, um nach Opfern zu suchen oder den Brandherd zu lokalisieren.“

Drohnen, Roboter, Kamera-Überwachung, Bodycam – unser Interview wird zeitweise stark von den neuen technischen Möglichkeiten beherrscht, die dem Sicherheitsdienstleister dazu dienen, in Zukunft noch effektiver für seine Kunden zu arbeiten. Aber Daniel Schleimer macht gleichzeitig deutlich, was ihm und dem Management besonders am Herzen liegt: gut ausgebildete Mitarbeiter zu finden und zu beschäftigen. „Die Rekrutierung von Personal ist eine Kernaufgabe.“

Das ist alles andere als einfach, denn in Sachen Image habe die Sicherheitsbranche in Deutschland durchaus Nachholbedarf, schränkt Schleimer ein: „In anderen europäischen Ländern und insbesondere in Skandinavien hat die Branche ein wesentlich positiveres Image.“ Warum ist das so? Der Securitas-Geschäftsführer

„Die Abwehr von Drohnen ist zu einer neuen Herausforderung geworden“

führt das vor allem auf die unterschiedlichen Marktverhältnisse zurück. Die Eintrittsbarrieren in Skandinavien für Sicherheitsfirmen sind hoch, die Mitarbeiter gut ausgebildet, sie verdienen dort dementsprechend gut.

Ganz anders die Situation in Deutschland. Daniel Schleimer verweist auf die über 5000 Sicherheitsunternehmen, die im Lande um Kunden buhlen. Es sind deshalb so viele, weil die Markteintrittshürden hierzulande lächerlich niedrig sind. Ein simpler IHK-Kurs (80 Stunden) reicht in der Regel schon aus, um ein Sicherheitsunternehmen gründen zu dürfen. Securitas, der Branchenverband BDSW und viele andere renommierte Anbieter wollen das ändern: „Wir wollen Mindeststandards für Sicherheitsdienste schaffen, um den Herausforderungen der Branche gerecht werden zu können.“ Zwar gebe es seit fast zwei Jahrzehnten einen Ausbildungsberuf, aber die Nachfrage ist insgesamt gering. Außerdem achten viele Kunden in Deutschland bei der Auswahl des Sicherheitsunternehmens oft nur auf eines – auf den Preis.

Daniel Schleimer weiß jedoch, dass es beim Thema Sicherheit immer stärker auf die Kombination von Technik und Menschen sowie Qualität ankommt. Der Branchenriese investiert daher seit vielen Jahren stark in die Aus- und Weiterbildung. In Schwerin betreibt die Gruppe ein eigenes Ausbildungszentrum, hat zu verschiedenen Themen auch regionale Schwerpunkte gebildet. „In Hamburg etwa steht die Hafensicherheit stark im Vordergrund, die ganz andere Voraussetzungen hat als die Absicherung des Oktoberfestes in München“, erläutert der Manager.

Neben der Ausbildung baut Securitas die Weiterbildung aus, zum Beispiel zur „Geprüften Schutz- und Sicherheitskraft“. „Allein in Nordrhein-Westfalen haben wir in den letzten Monaten 60 neue Stellen mit dieser Qualifikation besetzt. Nur so können wir den steigenden Anforderungen des Marktes gerecht werden und gleichzeitig unseren eigenen Mitarbeitern Karrieremöglichkeiten und Perspektiven eröffnen.“

Die Weiterbildungen sind beliebt, zumal damit ein deutlich höheres Einkommen verbunden ist. „Wir brauchen wachsames Personal, das nicht nur fachlich auf dem neuesten Stand ist, sondern immer mehr auch Beratungsfunktionen übernehmen kann – denn der Wandel in der Sicherheitstechnik ist rasant“, unterstreicht Schleimer. Seine Mitarbeiter machen schon heute individuelle Risiko-Schätzungen über das iPad, befassen sich mit radargestützter Sicherheitstechnik, machen Erfahrungen mit Bodycams und beherrschen ein ausgeklügeltes Sicherheitssystem, inklusive technisch gut ausgerüsteter Leitstellen.

Daniel Schleimer und die im Bundesverband der Sicherheitswirtschaft (BDSW) zusammengeschlossenen Unternehmen wünschen sich aber auch eine bessere gesellschaftliche Akzeptanz. „Dazu gehört unser Wunsch, dass die Branche am Innenministerium aufgehängt sein sollte und nicht am Wirtschaftsministerium“, kritisiert der Securitas-Manager. „Wir wollen schließlich Teil der Sicherheitsarchitektur in Deutschland sein. Und das funktioniert nur, wenn wir uns mit Behörden, Polizei und staatlichen Stellen intensiv austauschen.“


Technik spielt für private Sicherheitsfirmen eine zunehmend große Rolle. Das Beispiel von Securitas macht deutlich: Gut ausgebildetes Personal bleibt unverzichtbar. FOTO: SECURITAS

Christian Zaum
Landeshauptstadt Düsseldorf

Oliver P. Kuhrt
Messe Essen

Norbert Wesseler
Polizeipräsidium Düsseldorf

Günter Calaminus
W.I.S. Sicherheit + Service

Lukasz Wrobel
ISN Technologies GmbH

Rolf Tophoven
IFTUS Institut f. Krisenprävention

Dr. Michael J. Kaldasch
Aimedis B.V.

Klaus M. Brisch
DWF Germany

Wolfgang Bosbach
NRW-Sicherheitskommission

Herbert Reul
NRW-Landesregierung

Tom Bender
Rheinische Post

Das RP-Forum „Sicherheit" öffnete sich am Nachmittag für RP-Leser, die weitere Diskussionsrunden zum Thema Sicherheit mitverfolgen konnten – wie hier etwa mit dem Politiker Wolfgang Bosbach (rechts) und dem Essener Messechef Oliver P. Kuhrt (links). Michael Krons vom Fernsehsender Phoenix moderierte die Runden. FOTO: M. LÜBKE

RP-Forum: Die Teilnehmer

Aimedis B.V.
Dr. Michael J. Kaldasch, Geschäftsführer
ASW NRW e.V.
Dr. Christian Endreß, Geschäftsführer
consulting plus Unternehmensgruppe
Uwe Gerstenberg, Geschäftsführender Gesellschafter
Stefan Bisanz, Geschäftsführender Gesellschafter
Cyber Sicherheitsrat Deutschland e.V.
Hans-Wilhelm Dünn, Präsident
Cyomed Deutschland GmbH
Dr. Michael J. Kaldasch, Geschäftsführer
DWF Germany Rechtsanwaltsgesellschaft mbH
Klaus M. Brisch, Geschäftsführer
GEOS Germany GmbH
Jens Washausen, Geschäftsführer
IFTUS Institut für Krisenprävention
Rolf Tophoven, Direktor und Autor
ISN Technologies AG
Ulrich Weynell, Vorstandsvorsitzender (CEO)
ISN Technologies GmbH
Lukasz Wrobel, IT-Sicherheit
Landeshauptstadt Düsseldorf
Christian Zaum, Beigeordneter
MESSE ESSEN GmbH
Oliver P. Kuhrt, Geschäftsführer
Minister des Innern des Landes Nordrhein-Westfalen
Herbert Reul
Polizeipräsidium Düsseldorf
Norbert Wesseler, Präsident
Regierungskommission „Mehr Sicherheit für Nordrhein-Westfalen"
Wolfgang Bosbach, Vorsitzender
Rheinische Post Verlagsgesellschaft mbH
Tom Bender, Geschäftsführer
SECURITAS Services GmbH
Daniel Schleimer, Geschäftsführer
T-SYSTEMS INTERNATIONAL GMBH
Thomas Tschersich, Senior Vice President Internal Security & Cyber Defense
W.I.S. Sicherheit + Service GmbH & Co. KG
Günter Calaminus, Geschäftsführer

Moderation José Macias und Jürgen Grosche, Rheinland Presse Service GmbH, Michael Krons, Phoenix

SICHERHEITSARCHITEKTUR

Private Unternehmen bieten sich a

Die private Sicherheitswirtschaft könnte sich noch viel stärker in die strategische Planung der Sicherheitsarchitektur einbringen, betonen Branchenvertreter im Dialog mit Ansprechpartnern aus Politik und Ordnungsbehörden. Dabei gibt es durchaus unterschiedliche Vorstellungen darüber, wie Ordnung und Sicherheit am effizientesten gewährleistet werden können.

Vertreter aus der Sicherheitsbranche nutzten beim RP-Wirtschaftsforum „Sicherheit" in Räumen der Rheinischen Po schaft anzubieten. Da sei mehr drin, betonten mehrere Gesprächsteilnehmer.

VON JÜRGEN GROSCHE

Das RP-Wirtschaftsforum „Sicherheit in Deutschland" bietet einen guten Anlass, offen über Dinge zu reden, die unter dem Nagel brennen. Zumal, wenn man Ansprechpartner hat, die etwas bewegen können. Vertreter von Sicherheitsunternehmen nutzen die Gelegenheit, den NRW-Innenminister Herbert Reul (CDU) auf ihre Anregungen anzusprechen. „Die Polizei ist immer noch sehr zurückhaltend bei der Zusammenarbeit mit Kommunen und mit privaten Sicherheitsdiensten", bemerkt Uwe Gerstenberg (Geschäftsführer der consulting plus Beratung).

Auch Günter Calaminus (W.I.S. Sicherheit) bemängelt: „Die gute Informationsbasis von Unternehmen unserer Branche fließt nicht in die öffentliche und staatliche Arbeit ein." Calaminus regt eine stärkere Kooperation der Akteure an. „Davon könnte der Staat profitieren." Stefan Bisanz (Geschäftsführer der consulting plus Sicherheit) meint, die Polizei tue sich keinen Gefallen, wenn sie Sicherheitsdienste nur als „Befehlsempfänger" sehe. „Besser wäre es, wir würden gemeinsam darüber sprechen, was Aufgabe der Polizei ist und was Sicherheitsunternehmen leisten können."

Ähnlich argumentiert Daniel Schleimer (Securitas): Wenn von Sicherheitspartnerschaft geredet werde, sei das derzeit eine Einbahnstraße. „Wir brauchen eine andere Kommunikation miteinander." Schleimer nennt als Beispiel Bilder und Videos, die Kameras der Unternehmen aufnehmen. Die könne man doch mit der Polizei teilen, auf deren Tablets zum Beispiel. „Es müsste geklärt werden, wie dies technisch und rechtlich umsetzbar wäre."

„Die Polizei ist immer noch sehr zurückhaltend bei der Zusammenarbeit"

Reul verweist auf Bereiche, in denen die Zusammenarbeit bereits gut funktioniere und wo sie ausgebaut werden könnte: „Bei der Begleitung von Schwertransporten zum Beispiel wurde die Polizei durch die Einbindung von privaten Diensten schon entlastet." Auch beim Personen- und Objektschutz und an Flughäfen könne man schauen, ob man mit weniger Polizei auskommen könne. Eines stellt der Minister indes klar: „Sicherheit ist Aufgabe des Staates." Der Staat müsse aber nicht alles allein machen.

In Düsseldorf funktioniere eine Ordnungspartnerschaft bereits sehr gut, die Zusammenarbeit der Mitarbeiter vom Ordnungsamt mit der Polizei sogar vorbildlich, sagt Ordnungsdezernent Christian Zaum. Bei Veranstaltungen arbeite man auch gut mit privaten Diensten zusammen. Zaum verweist in dem Zusammenhang auch auf den Kriminalpräventiven Rat, ein vor 25 Jahren ins Leben gerufenes Netzwerk, das seinerzeit eine Vorreiterrolle in Deutschland gehabt habe.

Beim Objektschutz sei die Polizei ebenfalls durchaus an einer Zusammenarbeit mit Sicherheitsunternehmen interessiert, merkt der Polizeipräsident Düsseldorfs, Norbert Wesseler, an. Auch in anderen Bereichen hält er weitergehende Kooperationen für möglich, etwa bei der Wohnungssicherheit. „Die Diskussion läuft." Schwieriger werde es bei hoheitlichen Aufgaben oder der Terrorbekämpfung. „Beim Einbruchschutz schreibt sich die Polizei Erfolge auf die Fahne, es fehlt aber oft der Hinweis, dass wir dazu beigetragen haben", kritisiert Gerstenberg indes.

Versöhnliche Töne klingen aber auch durch. Innenminister Reul regt an, die Branche solle Vorschläge unterbreiten, wo die Polizei Aufgaben abgeben kann. Das nehmen die Unternehmensvertreter natürlich gerne auf. „Diese Runde hier ist dafür der richtige Partner", freut sich Gerstenberg. Thomas Tschersich (T-Systems International GmbH) kann sich

Leser suchen Orientierung

(jgr) Die Frage nach der Sicherheit beschäftigt die Menschen, beobachtet Tom Bender. Der Geschäftsführer der Rheinische Post Verlagsgesellschaft weiß, wovon er spricht – in den Medien kommen die Probleme ja geballt vor, in Form von Schlagzeilen zu Raub, Mord und Cyberkriminalität. „Das Thema hat viele Facetten", fasst Bender zusammen. „Aus den Kontakten mit unseren Lesern wissen wir, wie wichtig es ihnen ist. Kein Thema sensibilisiert derzeit mehr." Daher sei es spannend zu hören, wie die Spezialisten in Sachen Sicherheit die Lage einschätzen, sagt Bender bei der Begrüßung der Forumsteilnehmer. „Sie sind nah dran an den dunklen Ecken, leuchten sie aus. Daher wissen Sie am besten, wie wir uns schützen können. Ihre Antworten werden vielen Menschen Orientierung geben – und auch Mut, sich den Herausforderungen zu stellen."

Tom Bender, Geschäftsführer der Rheinischen Post

Terrorismus: Leben in diffu

(jgr) Zu den großen Bedrohungen der Sicherheit gehören die Gefahren durch Terrorismus – auch dies ein Thema beim RP-Forum „Sicherheit in Deutschland". Das Thema verunsichert Bürger und Politiker gleichermaßen: „Die Politik steht ständig unter der Drohung, es könnte etwas passieren", analysiert der Terrorismusexperte Rolf Tophoven die Lage.

Entscheidungen fielen unter diesen Umständen schwer, erklärt der Direktor des IFTUS-Instituts für Krisenprävention weiter: „Gibt es zu viele Reglementierungen, werden die Bürger unzufrieden. Sind die Maßnahmen zu locker, gibt es Vorwürfe, wenn etwas passiert." Sicherheitsbehörden müssten sich auf alle Szenarien vorbereiten, würden aber – wenn alles gut geht – kritisiert, der Aufwand sei zu hoch.

Gefährdet sind – so Tophoven – insbesondere Großveranstaltungen, wegen der großen medialen Wirkung. Hier hat sich nach Beobachtung von Daniel Schleimer (Securitas) die Einstellung der Menschen verändert, und „viele Veranstaltungen können wegen der Kosten für Sicherungsmaßnahmen nicht mehr stattfinden".

Wichtig sei „Klarheit und Wahrheit gegenüber den Bürgern", meint der Personenschutz-Experte Stefan Bisanz. Dazu gehöre auch die Feststellung, dass es 2016 die meisten Anschläge der Terrororganisation IS in Deutschland gegeben habe.

Wie soll man mit der Gefahr umgehen? Uwe Gerstenberg von der consulting plus-Unternehmensgruppe verweist auf die Anstrengungen der Städte,

Was tun in Zeiten permanenter Bedrohung beim RP-Forum. Dr. Christian Endreß (ASW

die Stadtmöblierung, also Bushaltestellen, Bänke oder Litfasssäulen, zur Terrorabwehr zu nutzen. „Die Wirtschaft muss hier noch weitere Model-

Ulrich Weynell
ISN Technologies AG

Thomas Tschersich
T-Systems International

Jens Washausen
Geos Germany

Uwe Gerstenberg
consulting plus

Stefan Bisanz
consulting plus

Daniel Schleimer
Securitas Services

Dr. Christian Endreß
ASW NRW

als Partner an

ost die Gelegenheit, dem Innenminister des Landes NRW, Herbert Reul (CDU), einen Ausbau der Sicherheitspartner-

FOTOS: MICHAEL LÜBKE

gut vorstellen, dass sich die drei großen in Düsseldorf vertretenen Telekommunikationsunternehmen in einer Partnerschaft mit der Polizei und der Staatsanwaltschaft über Cyber-Sicherheitsfragen regelmäßig austauschen. „Den formalen Rahmen dafür gibt es ja schon: die Sicherheitspartnerschaft mit dem Digitalverband Bitkom."

Auch Ulrich Weynell (ISN AG) verweist auf die langjährigen positiven Erfahrungen in der Zusammenarbeit mit der polizeilichen Kriminalprävention der Länder und des Bundes. Er empfiehlt seinen Kunden zusätzlich zur eigenen Expertise und der nachfolgenden Umsetzung, sich eine weitere objektive Stellungnahme eben jener Beratungsstellen einzuholen, die bundesweit kostenlos sind.

Als sehr originell erachten die Diskussionsteilnehmer den Vorschlag von Jens Washausen (Geos Germany), ein früher erfolgreiches Fernsehformat aufzugreifen: „Der 7. Sinn" war eine gern gesehene Informationssendung zur Verkehrssicherheit. „Damit könnte man die Bevölkerung auch für Themen der Kriminalität sensibilisieren." „Eine monatliche oder sogar wöchentliche Ausstrahlung im öffentlich-rechtlichen Fernsehen kann für eine zielführende Aufklärung mit dauerhaftem Lerneffekt in der Bevölkerung sorgen, begleitet von Social Media, Youtube und anderen Kanälen", erläutert Weynell. „Der Vorteil hierbei ist eine sehr zeitnahe Information über veränderte Täterverhalte (Life Long Learning), die dadurch zudem sehr dynamisch und bei professioneller Umsetzung zusätzlich unterhaltsam ist."

Reul: Sicherheit kostet einiges

(jgr) Es ist ein hochkarätiges Auditorium, dem sich NRW-Innenminister Herbert Reul (CDU) beim RP-Sicherheitsforum „Sicherheit in Deutschland" stellt – entsprechend ausgiebig nimmt sich der Politiker Zeit, seine Vorstellungen zur Gestaltung der Sicherheitsagentur zu erläutern und darüber mit den Experten aus der Sicherheitsbranche und Vertretern aus Behörden und Kommune zu diskutieren.

Reul präsentiert dabei nicht nur Vorhaben, die bereits bekannt sind – etwa die geplante Einstellung von 2300 Polizisten und 500 Verwaltungsassistenten zur Unterstützung der Polizei –, er gibt auch einen Einblick in sein Verständnis von Sicherheitspolitik. Einige Punkte werden von den Branchenvertretern durchaus auch kritisch hinterfragt, wie die Diskussionen zeigen (siehe nebenstehend sowie Seite 11).

Heute müsse die Polizei auf viele Situationen vorbereitet sein, erläutert der Minister, was auch erkläre, wieso manche Dinge länger dauern oder teurer werden. Als Beispiel nennt er die Anschaffung neuer Helme: „Wollen Sie die besten – oder die zweitbesten, die vielleicht in bestimmten Situationen nicht sicher sind?" Vor allem bei den Liegenschaften der Polizei hat der Minister einen großen Nachholbedarf entdeckt; der Investitionsstau betrage eine Milliarde Euro, „die IT-Infrastruktur ist Steinzeit, nicht Neuzeit".

Doch wer soll das bezahlen? Hier sieht Reul auch die Allgemeinheit in der Pflicht: „Die Gesellschaft wird über die Investitionen entscheiden müssen", aber auch konkreter: Städte müssten ebenfalls mehr tun, sie hätten in der Vergangenheit in den Bereichen Ordnung und Sicherheit oft gespart.

Gesellschaftlich umstrittene Themen packt Reul an, wenn er auf die Gesetzeslage und Pläne der Landesregierung etwa für das neue Polizeigesetz verweist. Immerhin positioniert er sich hier deutlich und verteidigt Vorhaben wie die automatische Kennzeichenerfassung. Zumindest in dieser Runde hält sich der Widerstand dagegen in engen Grenzen. Dass eine automatische Kennzeichenerfassung nicht erlaubt sein soll, hält Reul für „absurd" – von Hand dürften Polizisten doch Nummern aufschreiben, wundert sich der Minister. Und auch die Mautbetreiber dürften die Nummern für die Abrechnungen aufzeichnen.

Ob bei diesem Thema oder anderen wie Vorratsdatenspeicherung – Reul gibt sich gesprächs- und kompromissbereit: „Wie weit man dabei geht, darüber kann man immer reden, das ist alles lösbar." Bei der Verwendung des Begriffs Null-Toleranz-Strategie sieht er sich im Übrigen in Teilen auch missverstanden: „Ich möchte nur, dass die Sicherheitskräfte konsequent sind." Und dass sich etwas ändere. Reul sieht das Problem, dass ansonsten die „Bürger am Staat zweifeln". Hundertprozentige Sicherheit könne niemand versprechen, „wir wollen aber möglichst viel erreichen".

NRW-Innenminister Herbert Reul (links neben RP-Geschäftsführer Tom Bender) stellt sich den Forderungen der Sicherheitsbranche .

Abwehr gegen Messerattacken

(jgr) Immer wieder sorgen in jüngster Zeit Messerattacken für Schlagzeilen. Es ist schwer, sie zu verhindern: Messer kann man an jeder Ecke kaufen, und wenn es ein – auch ziemlich großes – Brotmesser ist.

Kann man sich gegen eine solche Attacke wehren? Wie? Beim RP-Wirtschaftsforum „Sicherheit in Deutschland" demonstrieren zwei Spezialisten vor RP-Lesern, was möglich ist: die Trainerin Ellen Tokur, die auch Krav Maga, eine israelische Selbstverteidigungsmethode, lehrt, und der Personenschützer Dennis Helgers aus Roermond.

Eines muss Ellen Tokur vorausschicken: „Bei einer Messerattacke wird man sehr wahrscheinlich verletzt, auch wenn man sich geschickt wehrt. Aber es geht ums Überleben." Wird eine zentrale Ader getroffen, verblutet man womöglich schneller, als dass Hilfe käme. Und: „Messerattacken sind gefährlicher als Angriffe mit Schusswaffen." Auch weil Täter eben einfacher an Messer als an Pistolen kommen. Und man hört keinen Schuss, der zumindest andere mögliche Opfer warnt.

In ihren Kursen erklären die beiden Verteidigungsprofis, wie man in einer Gefahrensituation zu ersten Einschätzungen kommen kann: Emotional handelnde Angreifer haben meist keinen Plan. Sie zeigen ihre Angriffslust, daran kann man sie früher erkennen als Angreifer, die gezielt handeln. Die verstecken ihr Messer oft und zücken es erst unmittelbar vor dem Angriff. Doch auch dafür haben die Profis Tipps.

Die Verteidigungsprofis Ellen Tokur und Dennis Helgers demonstrieren, wie man sich gegen eine Messerattacke wehren kann.

ıser Bedrohung

durch Terroranschläge? Auch darüber diskutierten die Sicherheitsexperten
NRW, 3. v. links) fordert eine Kooperation aller Beteiligten.

le entwickeln." Die Gesellschaft könne sich aber keine „Vollkaskomentalität" mehr leisten, „jeder muss mitwirken".

Das betont auch Günter Calaminus vom Sicherheitsunternehmen W.I.S.: „Die Menschen müssen sich mehr mit dem Thema beschäftigen und sehr aufmerksam beobachten, auf welchen Veranstaltungen sie sich sicher fühlen können."

„Poller allein reichen nicht", ist Jens Washausen von der Sicherheitsfirma Geos Germany überzeugt. „Terror ist letztlich nur mit politisch-moralischen Mitteln zu bekämpfen." Notwendig sei aber eine „vernünftige, schnelle und schlagkräftige Sicherheitsarchitektur".

Dr. Christian Endreß vom Verband Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen (ASW NRW) warnt indes vor zu großer Besorgnis: „Es ist ja nicht die Regel, dass etwas passiert." Behörden und Sicherheitswirtschaft würden sich heute anders aufstellen. Wichtig sei hier eine bessere Kooperation aller Beteiligten, der intelligente Einsatz von Instrumenten und eine gute Ausbildung der Mitarbeiter.

IS: Geschlagen, aber nicht besiegt

(jgr) Die anhaltenden Verluste der Terrororganisation „Islamischer Staat" (IS) im Irak und in Syrien weckten Hoffnungen. Doch der Terrorismusexperte Rolf Tophoven warnt: „Nationale und internationale Sicherheitsbehörden sowie Geheimdienste weltweit sind sich einig: Der Fall von Mossul und Rakka bedeutet nicht das Ende des ‚Islamischen Staates'." Sicher sei für die Experten, „dass der IS als Guerilla-Armee weiter funktionieren wird, denn er kontrolliert zwar nur noch geringe, vor allem ländliche Flächen im syrisch/irakischen Feld. Aber der IS wird Untergrund-Kommandos bilden."

Auch für Europa und Deutschland bleibe die Gefahrenlage kritisch: Der IS habe sich „im Laufe seiner relativ kurzen Geschichte zu einer internationalen Organisation entwickelt", sagt Tophoven. So hätten Antiterror-Experten zum Beispiel „eindeutige Verbindungen von Terroranschlägen in Europa IS-Akteuren in Libyen zugeordnet".

Ebenso besorgniserregend: „Der ‚Kult' des Selbstmordterrorismus ist unter der Ägide des Islamischen Staates weiter gestiegen", stellt der Experte fest. Die Anzahl der Selbstmordangriffe durch den IS nach Ausrufung des „Kalifats" habe alle anderen Dschihadisten-Gruppen übertrumpft, einschließlich al Qaida.

Eine Gefahr geht auch nach wie vor von IS-Söldnern aus, die in ihre Heimatländer zurückkehren. Für Deutschland gehen Sicherheitsbehörden, so Tophoven, von 970 Personen aus, die nach Syrien und in den Irak gereist sind, um sich dort dem IS anzuschließen. Nach Erkenntnissen der Sicherheitsbehörden seien bereits 320 von ihnen zurückgekehrt. 255 davon stammen aus Nordrhein-Westfalen. „Viele von ihnen verfügen über Kampferfahrung oder zumindest eine Waffe und Sprengstoffausbildung", sagt der Experte.

Sein Fazit: „Trotz der Niederlage des Islamischen Staates und des ‚Kalifats' auf dem eigentlichen ‚Geburtsfeld' Nahost ist die Gefahr durch die indoktrinierten und kampferprobten Kämpfer der Organisation noch lange nicht gebannt."

Der Terrorismusexperte Rolf Tophoven warnt davor, den so genannten „Islamischen Staat" nicht mehr als Gefahr ernstzunehmen.

CYBERKRIMINALITÄT

Die unheimliche Bedrohung aus dem Netz

Die Angriffe kommen meist unbemerkt über die Computerleitungen. Cyberkriminalität zählt zu den an meisten unterschätzten Gefahren. Die Schäden sind aber enorm: Rund 54 Milliarden Euro sind es allein in deutschen Unternehmen – pro Jahr!

VON JOSÉ MACIAS

So manchem der Besucher des RP-Sicherheitsforums „Sicherheit in Deutschland“, die am Nachmittag in das Konferenzzentrum der Rheinischen Post gekommen waren, stockte der Atem: Da hatte sich soeben der IT-Spezialist der Münsteraner Firma ISN Technologies, Lukasz Wrobel, mit ein paar Klicks einen Überblick über die Serverstrukturen bei einer Stadtverwaltung verschafft. Auf einen echten Angriff hat dabei der Spezialist an diesem Tag verzichtet, macht aber klar, dass für Hacker die Überwindung der Sicherheitsmechanismen keine wirkliche Herausforderung darstellt.

Thomas Tschersich von T-Systems International nimmt auch bei diesem Thema kein Blatt vor den Mund: „Bei Cyberangriffen tendiert der technische Aufwand für die Angreifer gegen null – zumal Hacker mittlerweile sogar eigene Suchmaschinen wie Shodan nutzen, die anfällige Netze automatisch aufspüren. Und das Entdeckungsrisiko ist für sie sehr gering, wenn man es nicht gerade mit einem Anfänger zu tun hat.“

Erschreckend sind vor allem die Dimensionen der Hacker-Angriffe, vor allem auf Firmen. Dr. Christian Endreß vom NRW-Verband „Allianz für Sicherheit in der Wirtschaft“ (ASW) berichtet, dass allein an Rhein und Ruhr über 400.000 Unternehmen bereits digital angegriffen wurden: „Das sind über 50 Prozent der Unternehmen – und die Dunkelziffer der tatsächlich betroffenen Firmen ist hoch.“

Auch der Wirtschaftsanwalt Klaus M. Brisch (DWF Germany Rechtsanwaltsgesellschaft) legt ernüchternde Zahlen vor: „Die Schäden durch Cyberangriffe belaufen sich in Deutschland jährlich auf rund 54 Milliarden Euro, europaweit kommen wir auf 327 Milliarden Euro. Wir wissen etwa, dass in Großbritannien inzwischen über 50 Prozent der Unternehmen schon mal Opfer eines Cyberangriffes geworden sind.“ Bedeutet das etwa, dass die anderen britischen Firmen, die bislang noch nicht Schäden gemeldet haben, nicht betroffen sind? Die Antwort des international gefragten Juristen ist ernüchternd: „Die anderen Unternehmen glauben nur, sicher zu sein – sie sind es aber nicht. Wir brauchen daher auch in Deutschland eine Cybersicherheitsstruktur für Unternehmen.“

Wie dramatisch die Folgen einer Cyberattacke sein können, macht Hans-Wilhelm Dünn vom Cyber-Sicherheitsrat Deutschland anhand von Zahlen deutlich: „Bei einem Ausfall der IT-Infrastruktur bekommen mittelständische Unternehmen im Durchschnitt nach zwei Tagen Liquiditätsprobleme.“ Viele Firmen merken indes nicht einmal, dass man aus ihren Computern wichtige Informationen absaugt. „Die Unternehmen merken im Schnitt erst nach 218 Tagen, dass sie infiltriert sind.“

Die Messe Essen, die mit der Sicherheitsmesse Security Essen immer wieder wichtige Impulse für die Sicherheitsbranche liefert, kennt die Problematik genau: „In diesem Jahr werden wir deshalb mit fachlicher Unterstützung des BSI (Bundesamt für Sicherheit in der Informationstechnik) eine gesonderte Konferenz zu Cybersecurity anbieten“, bekräftigt Geschäftsführer Oliver P. Kuhrt. T-Systems-Experte Thomas Tschersich sieht aber nicht im Mangel an IT-Spezialisten das Hauptproblem, sondern beklagt die generelle „digitale Ignoranz“: „Die meisten Menschen etwa benutzen ihre Smartphones wie Telefone – dabei sind das Computer, auf die ebenfalls ein Virenschutz gehört. Die meisten Sicherheitslücken entstehen in diesem Bereich, weil die Anwender schlichtweg ihre Betriebssysteme nicht regelmäßig updaten.“

Für Cyberkriminelle ist es in vielen Fällen leicht, an Passwörter heranzukommen. Die durch Internetkriminalität erzeugten wirtschaftlichen Schäden gehen in die Milliarden. FOTO: THINKSTOCK/JORUBA

Klaus M. Brisch (DWF, links) diskutiert mit Dr. Michael J. Kaldasch (Aimedis, 2. v.r.) und Hans-Wilhelm Dünn, Präsident des Cyber Sicherheitsrates Deutschland (rechts) vor RP-Lesern über Cybersicherheit und Internetkriminalität. Michael Krons (Phoenix) moderierte die Diskussionsrunden. FOTO: MICHAEL LÜBKE

Lukasz Wrobel (ISN Technologies) demonstriert ein Gerät, das es in China für 200 Euro gibt, mit dem man Sicherheitskarten kopieren kann. FOTO: MICHAEL LÜBKE

Bedrohungsfelder werden aber in den nächsten Jahren vor allem mit neuen, internetfähigen Geräten wie Kühlschränken und anderen Smarthome-Geräten eröffnet: „Hier ist es nur eine Frage der Zeit, wann es zur Kastastrophe kommt.“

Terrorismus-Experte Rolf Tophoven weist darauf hin, dass Terroristen Bomben und Sprenggürtel bislang vor allem dafür nutzen, um Aufmerksamkeit für sich zu schaffen. „Das wird sich in der Zukunft noch stärker in Richtung Cyberguerilla ändern und erweitern.“

„Ich bin deshalb davon überzeugt, dass Cybersicherheit in den nächsten Jahren zu einem der herausfordernden Themen für die Sicherheit in Deutschland werden wird“, ergänzt Endreß. Er verweist dabei nicht nur auf Angriffe, die vor allem aus dem russischen Raum kommen, sondern auch auf das Darknet: „Dort lässt sich problemlos nahezu alles bestellen, vom Betäubungsmittel bis zur Schusswaffe. Der moderne Bankräuber braucht allerdings keine Schusswaffe mehr, dafür reichen ein Computer und das Wissen um digitale Sicherheitslücken.“

Auch Jens Washausen (Geos Germany) warnt vor den systemischen Risiken, insbesondere für Firmen: „Die Qualität der Software ist vor allem im deutschen Mittelstand erschreckend schlecht – das kann für viele Unternehmen desaströse Folgen haben. Aber solange Vorstände ausschließlich ihre IT-Abteilung fragen, werden sie die Risiken nicht erkennen – hier gibt es nahezu immer dieselbe Antwort, dass alles in Ordnung sei.“

Uwe Gerstenberg und Stefan Bisanz von Consulting Plus sehen deshalb vor allem das Management in der Pflicht. „Entscheider haben oft keine Ahnung vom Thema Cybersicherheit. Sie vertrauen hier den Menschen, aber ohne zu kontrollieren – und natürlich gibt es in Deutschland zudem zu wenig Fachkräfte, die sich mit dem Thema auskennen“, so Gerstenberg. „Außerdem bekämpfen wir vorrangig die Computerviren anstelle der Menschen, die diese entwickeln. Gleichzeitig sind es die Menschen, die vor den Computern sitzen, die die Fehler machen. Unser Ansatz ist es daher, uns schwerpunktmäßig um die Menschen auf beiden Seiten zu kümmern“, erläutert Bisanz.

Klaus M. Brisch plädiert ebenfalls für einen Denkwechsel in den Unternehmen. „Das Management sieht Cybersecurity immer noch als Kostenfaktor – dabei ist es ein Nutzenfaktor. Denn in Zukunft werden Firmen ihren Vertragspartnern nachweisen müssen, dass ihre IT sicher ist – sonst wird es nicht zum Vertragsabschluss kommen.“

Viele Angriffe über E-Mail

(rps) Wenn Cyber-Kriminelle Unternehmen attackieren, ist am häufigsten eine E-Mail der Türöffner: 59 Prozent der erfolgreichen Cyber-Angriffe auf kleine und mittlere Firmen erfolgten über Anhänge oder Links in der elektronischen Post. Das ist das Ergebnis der Studie „Cyberrisiken im Mittelstand“, die der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) kürzlich vorgelegt hat.

„Bei der IT-Sicherheit kommt es eben nicht nur auf Technik an. Auch Mitarbeiter müssen für die zahlreichen Gefahren sensibilisiert werden“, sagt Peter Graß, Cyberversicherungsexperte des Verbandes.

Nur bei jedem vierten Angriff (26 Prozent) drangen Hacker über die Netzwerk-Systeme ein. Sogenannte Ddos-Attacken oder Schädlinge auf Datenträgern wie USB-Sticks (jeweils drei Prozent) spielen kaum eine Rolle.

Drei Viertel der Angriffe (74 Prozent) haben sich laut der Studie erst in den vergangenen zwei Jahren ereignet. Am häufigsten mussten Betriebe nach einem Angriff Kosten für die Aufklärung und Datenwiederherstellung in Kauf nehmen (59 Prozent). In vier von zehn Fällen (43 Prozent) legten die Angriffe die betroffenen Firmen sogar zeitweise lahm.

Es war ein hochkarätig besetztes Forum, das bei der Rheinischen Post über Themen der Sicherheit diskutierte und dabei der Politik auch kritische Fragen mitgab. NRW-Innenminister Herbert Reul (CDU, Mitte) zeigte sich offen für Vorschläge aus der Sicherheitsbranche, wie und wo man besser zusammenarbeiten könnte. FOTO: MICHAEL LÜBKE

VERANSTALTUNGEN

Branche wünscht bessere Zusammenarbeit

Veranstaltungen ziehen nicht nur viele Besucher an, sondern auch Terroristen. Denn als so genannte weiche Ziele sind sie leicht anzugreifen. Sicherheitsunternehmen bieten ihre Dienste an, sehen sich aber von den Ordnungsbehörden nicht genug eingebunden.

VON JÜRGEN GROSCHE

Natürlich geht es in den Diskussionen beim RP-Sicherheitsforum „Sicherheit in Deutschland“ auch um Veranstaltungen und Großereignisse mit vielen Besuchern. Sie gelten als weiche Ziele für Terroristen und stehen daher im Fokus der Sicherheitsbehörden. In Düsseldorf sei die Veranstaltungskultur „sehr ausgeprägt“, sagt Polizeipräsident Norbert Wesseler. „Wir müssen uns auf kritische Situationen vorbereiten.“ So dienen die Lkw-Sperren dazu, Risiken zu minimieren.

In Düsseldorf gebe es eine gute Zusammenarbeit zwischen Stadt und anderen Sicherheitsträgern, betont Wesseler. Vor Veranstaltungen werde genau besprochen, wer welche Aufgaben übernimmt. „Wir prüfen das professionell.“ Zudem tausche man sich regelmäßig beim Düsseldorfer Sicherheitsgipfel aus.

„Die Unternehmen sind nur Auftragnehmer, die Anordnungen ausführen“

Neben der Terrorgefahr gebe es natürlich noch weitere Gefahren, merkt Gerstenberg (Geschäftsführer der consulting plus Beratung) an, zum Beispiel Naturereignisse. Und was eine Massenpanik auslösen kann, zeigten dramatisch die Ereignisse bei der Love Parade in Duisburg. „Bei Veranstaltungen müssten Informationsblätter verteilt werden, die erklären, wie man sich im Gefahrenfall verhalten soll“, regt Gerstenberg an. Im Gegensatz zu Wesseler kritisiert Gerstenberg, dass private Sicherheitsunternehmen meist nicht in die Sicherheitsplanungen vorab einbezogen seien. „Die Unternehmen sind nur Auftragnehmer, die Anordnungen ausführen. Wir könnten mit unseren Erfahrungen viel mehr einbringen.“ Zudem gebe es Schnittstellen, die bislang nicht beachtet werden und sich damit als Schwachstellen erweisen. Als Beispiel nennt Gerstenberg Depots auf Kirmesveranstaltungen, in denen Gasflaschen deponiert sind. „Wer bewacht die?“

„Es wäre schön, bei der Sicherung von Großereignissen ein gewisses Maß einzuführen“

Informationsblätter zu verteilen könne zur Aufklärung beitragen, aber auch verunsichern, meint Christian Zaum, Ordnungsdezernent in Düsseldorf. In der Landeshauptstadt seien private Dienste im Übrigen immer in die Kooperationsgruppe im Rathaus eingebunden. „Und ich bin offen dafür, sich im Vorfeld noch mehr auszutauschen.“ Mit Interesse beobachten Zaum und andere Sicherheitsexperten derzeit ein Projekt in München – dort soll eine Veranstaltungs-App zahlreiche Informationen auch zur Sicherheit bieten.

Für einige Teilnehmer der Diskussionsrunde stellt sich darüber hinaus die Frage nach der Sinnhaftigkeit mancher Sicherungsmaßnahmen. Oliver P. Kuhrt (Messe Essen) hält es für „schwer erklärbar“, dass zur Sicherung von Großereignissen viele Kapazitäten gebunden werden, die an anderer Stelle dann fehlen. „Es wäre schön, hier ein gewisses Maß einzuführen“, regt der Messechef an.

Hier könne die Privatwirtschaft im Übrigen für eine Entlastung der öffentlichen Sicherheitskräfte sorgen, betonen andere Gesprächspartner, zum Beispiel Jens Washausen (Geos Germany): „Eine Partnerschaft wäre gut“; sie könne viele Bereiche umfassen. So könne man in einem gemeinsamen Lagezentrum aktuelle Internet-Aktivitäten auswerten, die vielleicht Hinweise auf Gefahren geben. „Denn die Fähigkeiten der Sicherheitskräfte hängen davon ab, wie gut die Informationen in der gesamten Sicherheitsarchitektur sind.“

Wie Gerstenberg bemängelt Daniel Schleimer (Securitas), dass private Dienstleister „trotz ihrer Leistungsfähigkeit am Rande der Sicherheitsbesprechungen“ stehen, oft nicht dabeiseien, obwohl sie operativ intensiv beteiligt sind. „Wir sind vor allem nachts oft die Augen und Ohren.“ Aber in kritischen Fällen könne man häufig nicht effektiv helfen, da man nicht ins Sicherheitskonzept eingebunden sei. Aus Sicht der Sicherheitsbranche bleibt also der Gesprächsbedarf hoch.

NRW-Innenminister Herbert Reul (Mitte) zeigte sich beim RP-Wirtschaftsforum „Sicherheit in Deutschland“ offen für Vorschläge aus der Sicherheitsbranche (links Wolfang Bosbach, rechts RP-Geschäftsführer Tom Bender). FOTO: MICHAEL LÜBKE

Zahlreiche RP-Leser informierten sich beim RP-Sicherheitsforum über unterschiedliche Gefahren und Gegenmaßnahmen. FOTO: MICHAEL LÜBKE

Praktische Tipps zur Sicherheit

(jgr) Einen ganzen Tag lang befassten sich Sicherheitsexperten und Politiker beim RP-Forum „Sicherheit in Deutschland“ mit dem Thema. Am Nachmittag informierten die Experten RP-Leser über Gefahren im Internet, auf der Straße oder im eigenen Wohnumfeld und wie man sich zur Wehr setzen kann. Erfreuliche Nachricht trotz aller Bedrohungen: Es gibt zahlreiche Instrumente. Man muss sich nur auf dem Laufenden halten.

Cyber Security halten viele Unternehmen für einen Kostenfaktor. Ein verhängnisvoller Irrtum. In Wirklichkeit ist Sicherheit ein unermesslicher Nutzenfaktor.
Allein im Jahr 2017 verursachten Cyber-Attacken in Deutschland einen Schaden von 54 Mrd. Euro. In der EU belief er sich sogar auf 340 Mrd.
Dabei bleibt ein großer Anteil der Cyber-Attacken unbemerkt. Denn deren Ziel ist der fortwährende Abfluss von Know-how.

Im Jahr 2020 werden weltweit rund 50 Milliarden Dinge digital miteinander verknüpft sein.
Jedes einzelne kann ein Einfallstor für die Raubritter 4.0 sein.
Keine Frage: Sicherheit erfordert mehr denn je eine ganzheitliche Herangehensweise. Das erfordert Kompetenzteams, die das Problem und das Geschäft verstehen.

Wir tun das.

www.dwf.law