Können unsere Städte Katastrophen widerstehen?

Cyberangriffe, eine Zunahme von Extremwetterereignissen, Katastrophen und Aktivitäten fremder Nachrichtendienste zum Nachteil der deutschen Wirtschaft, politische Unruhen und Pandemien werden Staat, Gesellschaft und Wirtschaft in den nächsten Jahren vor große Herausforderungen stellen. Was können Städte und Gemeinden präventiv tun, um diesen Herausforderungen zu widerstehen?

Der Sicherheitsexperte Uwe Gerstenberg fordert genaue Analysen darüber, welche Risiken für jede Stadt bestehen. FOTO: ALOIS MÜLLER

Großbrände und andere Katastrophen bedrohen das Leben der Menschen. Doch auch andere Gefahren lauern, zum Beispiel aus dem Internet. Welche Konsequenzen das für Städte, Gemeinden und ihre Bürger hat, darüber diskutierten Sicherheitsexperten beim RP-Forum. FOTO: GETTY IMAGES/MICHAEL STIFTER

(jme) Uwe Gerstenberg ist Geschäftsführer der consulting plus GmbH, einem etablierten Sicherheitsberater und -dienstleister mit jahrzehntelanger nationaler und internationaler Erfahrung. Und er ist Autor des Booklets „Masterplan Sicherheit. Lösungswege für eine sichere Stadt". In der ersten Diskussionsrunde des 6. RP-Wirtschaftsforums Sicherheit wies er darauf hin, dass viele Risiken wie etwa Extremwetterereignisse oder Pandemien eben nicht mehr nur hypothetisch eintreten können, sondern schon Realität geworden sind.

Er fragt: „Wir alle erleben den Klimawandel und seine Auswirkungen hautnah. Jedes dieser Ereignisse beeinflusst unser gesellschaftliches Leben intensiv und nachhaltig. Was können oder müssen Städte und Gemeinden präventiv unternehmen, wenn es darum geht, eine Stadt durch konkrete Maßnahmen widerstandsfähig, resilient zu machen?"

Zunächst, meint Gerstenberg, müsse analysiert werden, welche Risiken für jede Stadt bestünden. Also bedürfe es zunächst einer Bestandsaufnahme aller Risiken. „Neben den Naturereignissen gehören sicherlich auch menschliches Versagen, Nachlässigkeit und Routine sowie Kriminalität und Terrorismus dazu."

Deutschland, so Gerstenberg, sei das einzige Land, das sich einer doppelten Wende in der Stromerzeugung verschrieben habe. „Einerseits reduzieren wir die fossilen Energieträger zugunsten erneuerbarer Energien. Andererseits steigen wir aus der Kernkraft aus. Die Risiken der Energiewende, die für die Gesellschaft und die Wirtschaft entstehen, sind nicht zu unterschätzen." Wirtschaft und Unternehmen benötigten eine planbare, kontinuierliche und bezahlbare Stromversorgung.

Welche Konsequenzen das für Städte und Gemeinden, also auch für die Bürger, hat, verdeutlicht Gerstenberg am Beispiel der Systemsicherheit. „Wir gehen davon aus, dass der Strom immer fließt. Dabei kommt es zu etwa 12.000 ungeplanten Ausfällen auf der Netzebene der Mittelspannung und zu rund 130 Ausfällen in der Hochspannung im Jahr. Der längste Ausfall zog sich knapp über neun Tage. Neben kurzfristigen Unterbrechungen der Stromversorgung besteht auch die Gefahr eines lang anhaltenden Stromausfalls – eines Blackouts. Dieses Risiko steigt, da mit jedem Tag ein weiteres kleines Kraftwerk aus Wind und Sonnenenergie an das Stromnetz angeschlossen wird."

„Der Staat wird's schon richten"

Experten warnen: Die Deutschen müssen sich auf Großschadenereignisse einstellen – und Eigenvorsorge betreiben. Über diese und andere Bedrohungsszenarien diskutierten Experten beim RP-Forum Sicherheit in den Rudas Studios in Düsseldorf.

Behörden, aber auch die Bürger müssten sich auf Bedrohungsszenarien besser vorbereiten. Das betonten die Diskussionsteilnehmer beim RP-Sicherheitsforum. FOTOS: A. MÜLLER

VON JÖRG MEHL

Was können Behörden, Unternehmen, aber auch die Bürger selbst tun – und wie können sie für einen Notfall vorsorgen? Dr. Christian Endreß (ASW West) sieht starke Defizite in allen Bereichen, sobald es um das Thema Vorbereitung auf eine Katastrophe geht – im behördlichen Bereich wie auch bei Unternehmen, die sich oftmals nicht hinreichend vorbereiten. Ganz besonders aber auch in der Bevölkerung: „Wir leben heute in einer Vollkaskomentalität. Die Menschen gehen davon aus: Der Staat wird's schon richten." Dieses Prinzip habe sich jahrelang bewahrheitet. „Jeder geht davon aus, wenn er die 110 oder die 112 anruft, kommt innerhalb von wenigen Minuten Hilfe."

Das treffe im Alltag zu – greife aber nicht bei Großschadenereignissen oder Katastrophen. „Die Menschen müssen sich auf neue Szenarien einstellen, Eigenvorsorge treffen." Gerade bei einem lang anhaltenden Stromausfall, einem Blackout, müsse man davon ausgehen, dass keine Hilfe mehr kommen kann.

Steffen Schimanski (Deutsches Rotes Kreuz) sieht seine Organisation in einer besonderen Rolle – gerade auch als Partner der Behörden. Mit Blick auf die Hochwasserkatastrophe meint er, es dürfe zwar kein „Weiter so!" geben, vieles habe aber auch gut funktioniert. Die Helfer der ersten Stunde seien Nachbarn gewesen, die mit angepackt hätten, betont er. „Wir erleben eine unfassbare Solidarität, wo Sozialraum, Quartiere, Veedel, wie man in Köln sagt, funktionieren." Die allerdings taucht bisher in keinem Notfallplan auf. „Wir haben uns viele Jahre auf Spezialisten, Fachkräfte, hoch spezialisierte Hilfeleistung durch Experten fokussiert, die aber bei großen Ereignissen an ihre Grenzen kommt."

Wenn ein Krankenhaus nur über die Luft evakuiert werden kann, ließen sich in kurzer Zeit vielleicht nicht so viele Hubschrauber organisieren, wie benötigt würden. „Da brauchen wir andere Herangehensweisen und müssen auch schauen: Können die Strukturen vor Ort so gefestigt werden, dass sie so lange durchhalten, bis Hilfe organisiert ist?" Da sei noch viel zu tun, zumal sich zu wenige Behörden, Unternehmen, aber auch Bürger bewusst darüber seien, welche Gefahren potenziell auf sie zukommen.

Stefan Bisanz (consulting plus) meint: „Wir müssen uns zum Thema Sicherheit und Ordnung bekennen." Das finde aber zu wenig statt. „Auf welche Art und Weise bereiten wir uns auf Katastrophen überhaupt vor?", fragt er. „Warum keine Intervention? Wir haben Städte in Nordrhein-Westfalen, wo sich nachts eine Doppelstreife um Ordnung kümmert. Da müssen wir eingreifen, uns bekennen – und entsprechende Gelder bereithalten." In Köln beispielsweise gebe es bei der Berufsfeuerwehr 300 offene Stellen, im Ordnungsamt 180 – und das schon seit Jahren.

Britta Zur, Polizeipräsidentin in Gelsenkirchen, verweist auf den „immensen Personalzuwachs", den die Polizei in Nordrhein-Westfalen seit einigen Jahren habe. „Wir haben sehr gute Einstellungszahlen. Der Polizeiberuf ist attraktiv wie wohl nie zuvor." Sie selber konnte in den vergangenen Monaten mehrere Hundert Polizeianwärter in Gelsenkirchen begrüßen. Dennoch: Gerade im Katastrophenfall sei die Zusammenarbeit enorm wichtig. Man könne nicht Polizei, Feuerwehr oder Stadt isoliert betrachten, „entscheidend sind immer die Kommunikationswege." Und gute Kommunikation müsse schon vor, nicht erst in der Krise sichergestellt werden.

Daniel Schleimer (Securitas Services) wünscht sich gemeinsame Maßnahmenpläne und Konzepte, die alle Kräfte, behördliche wie private Sicherheitsakteure, bei einem Großereignis zusammenführen. Und solche Pläne auch präventiv durchzuspielen, damit „wir im Ereignisfall direkt und gezielt agieren können". Ein Beispiel für gemeinsame Krisenpläne von Behörden, Kommunen und privaten Sicherheitsunternehmen in NRW ist ihm nicht bekannt – „die sollten wir aber auf jeden Fall aufbauen!" Dazu müssten allerdings auch Vorbehalte gegenüber den privatwirtschaftlichen Unternehmen abgebaut werden.

Uwe Gerstenberg sieht ein Hauptproblem in Sachen Prävention, dass sich die Akteure oft gar nicht kennen. Es gebe schlicht keine gemeinsamen Runden von Politik, Verwaltung und Wirtschaft. Dabei müsste jede Gemeinde wissen, welche „Player" es in der lokalen/regionalen Wirtschaft gibt und wie sie in bestimmten Szenarien helfen könnten. Deshalb plädiert er dafür, dass „Städte und Gemeinden sich fragen, was sind die Risiken und wie gehen wir mit ihnen um im Rahmen einer Risikosteuerung". Im Ergebnis werde vielleicht festgestellt, dass ein Bauunternehmer mit Baggern und Lastwagen gebraucht wird oder ein IT-Spezialist, der ein abgesunkenes Rechenzentrum wieder in Betrieb nehmen kann.

Axel Schmidt (Salto Systems) ist selbst von der Hochwasserkatastrophe betroffen. Wasser bis ins Erdgeschoss, Stromausfall, Telefonnetzüberlastung: „Wir haben über einen Tag gebraucht, um die 112 anrufen zu können", schildert er seine Erlebnisse. Wasser, Hebepumpen, Heizung – alles fiel aus, über Wochen. Obwohl er gut vorbereitet war – nur ein Notstromaggregat hatte er nicht. Nachbarn waren die ersten, die halfen, lange bevor professionelle Kräfte eintrafen. „Es war schon ergreifend zu sehen, wie viele Leute mit angepackt haben – bevor dann die Feuerwehr das Wasser abgepumpt hat." Es fehle an der Priorisierung der Notfälle. Es sei eben ein Unterschied, ob jemand zehn Zentimeter Wasser im Keller stehen hat, oder ob das Erdgeschoss schon überflutet ist.

Oliver P. Kuhrt (Messe Essen) sieht die Sicherheit eines Unternehmens wie seines, einen Versammlungsort vieler Menschen, gleich mehrfach bedroht – durch Terror, Naturkatastrophen wie Hochwasser oder auch Cyber-Attacken. „Wir sind deshalb maßgeblich angewiesen auf eine intensive Kommunikation mit den handelnden Akteuren – bei der Stadt, bei Institutionen. Aber ohne die Privaten geht es auch nicht. Für ein Unternehmen unserer Größe ist es wichtig, dass Pläne erstellt werden, die sicherstellen, dass wir sehr schnell auch autark handeln können."

Unterschätzte Risiken – können wir uns noch selber helfen?

Nicht nur die Hochwasserkatastrophe hat gezeigt: Wir alle müssen uns zunehmend auf Extremwetterereignisse, Naturkatastrophen und Cyberangriffe einstellen. Das hat Auswirkungen auf die Versorgungsstrukturen der Bundesrepublik Deutschland.

(jme) Dr. Christian Endreß ist Geschäftsführer des Wirtschaftsschutzverbandes Allianz für Sicherheit in der Wirtschaft West (ASW West), der die Kriminalprävention in der Wirtschaft fördert. In der zweiten Diskussionsrunde des 6. RP-Wirtschaftsforums Sicherheit ging er der Frage nach, ob die Strukturen der Inneren Sicherheit und speziell des Zivil- und Katastrophenschutzes in Deutschland heutigen und zukünftigen Ereignissen noch gerecht werden können. Nahezu paradox erscheint Dr. Endreß, dass einerseits der größte Anteil der Kritischen Infrastrukturen, also die Unternehmen, die die lebensnotwendige Versorgung der Bevölkerung sicherstellen, privatwirtschaftlich betrieben wird, andererseits eine Einbindung in staatliches Krisenmanagement nicht erfolgt. „Häufig werden komplexe Risiken in den Unternehmen und Behörden nicht hinreichend wahrgenommen. Unsere Versorgungsinfrastrukturen sind enorm anfällig und nur einzelne Branchen sind zur Notfallvorsorge verpflichtet. Dabei sollte eine angemessene Notfallvorsorge nicht die Kür, sondern die Pflicht aller Unternehmen und Behörden sein."

Dr. Christian Endreß, Geschäftsführer ASW West FOTO: A. MÜLLER

Wie anfällig die Versorgungsstrukturen sind, skizziert Dr. Endreß am Beispiel der Lebensmittelversorgung. „Der Einkauf, also die Versorgung der Bevölkerung mit Lebensmitteln im Alltag, ist in Deutschland so selbstverständlich, dass – mit Ausnahme der Lebensmittelsicherheit – dieses Feld weder in der Bevölkerung noch in der Wirtschaft oder der Politik viel Beachtung findet", mahnt er. Bei genauerer Betrachtung zeige sich, dass das privatwirtschaftlich organisierte System der Lebensmittelversorgung durchaus krisenanfällig sei. Da auch in der Bevölkerung ein geringes Risikobewusstsein für Ausfälle existiere, hat Dr. Endreß Zweifel, ob es im Zusammenspiel aller relevanten Akteure möglich wäre, im Krisenfall eine ausreichende Lebensmittelversorgung zu gewährleisten."

Aktuelle Studien schätzen zudem die Wahrscheinlichkeit eines großflächigen Stromausfalls innerhalb der nächsten fünf Jahre als hoch ein. Dr. Endreß: „Die Frage ist nicht, ob es zu einem großflächigen Stromausfall kommen wird, sondern wann." Der Experte sieht dringenden Handlungsbedarf: „Nur durch gemeinsame Anstrengungen von Behörden und Unternehmen können komplexe Ereignisse bewältigt werden. Durch eine funktionierende Zusammenarbeit mit der Wirtschaft können Versorgungsengpässe vermieden werden." Wichtig sei, dass sich alle Akteure, staatlich wie privat, vor dem Eintritt einer Krise abstimmen und Notfallpläne entwickeln.

Wenn aus dem Hahn kein Wasser mehr kommt

Weggeschwemmte Leitungen und Rohre im Ahrtal: Eine Katastrophe wie die Flut im Juli kann die Versorgung der Bevölkerung gefährden. Um sich auf solche Fälle vorzubereiten, müsse mehr getan werden, sagen Experten. FOTO: DPA

Im Katastrophenfall geht mitunter nichts mehr – kein Strom, kein Telefonnetz, keine Lebensmittel, kein frisches Trinkwasser. Ist die Bevölkerung Deutschlands ausreichend auf solch einen Notfall vorbereitet?

VON JÖRG MEHL

Die Bevölkerung, findet Steffen Schimanski (Deutsches Rotes Kreuz), muss sensibilisiert werden für das Thema Risiko. „Sauberes Wasser, das ich erhitzen kann, das ich trinken kann, ist lebensnotwendig. Aber das Bewusstsein, dass das Wasser plötzlich nicht mehr aus dem Hahn kommen könnte oder ungenießbar, ja vielleicht gefährlich ist, weil es mit Krankheitskeimen versetzt ist, scheint verlorengegangen zu sein. Da ist Aufklärung und Kommunikation nötig." Insgesamt seien wir in Deutschland gut auf Katastrophenfälle vorbereitet – schwierig werde es aber, wenn sie sich großflächig ausbreiten, „wenn das Hochwasser eben nicht mehr im Keller steht, sondern im zweiten Stock". Deshalb sei es „unfassbar wichtig, solche Szenarien von Anfang bis zum Ende zu denken. Und da müssen alle an einen Tisch, die wir dafür brauchen." Er plädiert dafür, gesamtgesellschaftliche Ressourcen in Risikoanalysen und die Bevölkerungsschutzplanung einzubinden und vor allem Bewusstsein zu schaffen – zum Beispiel durch Aufklärungskampagnen zu Bevölkerungsschutz und Prävention sowie Integration in den Schulunterricht.

Mehr im Video

RP-Forum Sicherheit in den Rudas Studios in Düsseldorf: Schauen Sie sich alle Diskussionen im Video an.
www.rp-forum.de/sicherheit
(oder QR-Code scannen)

Daniel Schleimer (Securitas Services) hat zu Hause ein Regal, in dem sich die notwendigen Dinge befinden, um zehn Tage in einem Katastrophenfall zu überstehen. „Höchste Bedeutung hat dabei das Wasser", sagt der erfahrene Sicherheitsexperte. Das Bundesamt für Katastrophenschutz hat eine „Persönliche Checkliste" herausgebracht, die aufführt, welche Lebensmittel in welcher Menge man vorrätig haben sollte, um im Falle einer Katastrophe wie Hochwasser, Stromausfall oder Sturm zehn Tage ohne Einkaufen überstehen zu können. Sie ist im Internet abrufbar unter www.bbk.bund.de. Der Haushaltswaren-Discounter Kodi geht hier mit positivem Beispiel voran und hat 2,5 Millionen Haushalte mit der Empfehlungsliste für Notfälle versorgt.

Christian Kromberg, Ordnungsdezernet der Stadt Essen, berichtet, dass die Stadt nicht auf ein solches Zehn-Tages-Szenario vorbereitet ist – was auch auf alle anderen Großstädte in Deutschland zutreffe. Im Katastrophenfall bedürfe es Hilfe von außen. Wobei im Ruhrgebiet der Strom schon wegen der „Ewigkeitslasten" des Bergbaus funktionieren muss: Die Pumpsysteme unter der Erde müssen weiterlaufen, damit das Grubenwasser in ausreichender Tiefe gehalten werden kann – ansonsten würde es zu massiven Überschwemmungen kommen. Allerdings strebt Essen die „resiliente Stadt" an und ist auf verschiedene Szenarien vorbereitet. So werden in Essen beispielsweise Straßenbäume gepflanzt, die auch Stürmen trotzen können. Oder es wird durchgespielt, was nach einem Cyberangriff auf die Stadtverwaltung passiert. Auch das Hochwasser ist im Stadtrat ein großes Thema. Kromberg räumt aber auch ein: „Das Ungewisse bleibt, und damit auch die Notwendigkeit zu improvisieren. Auf alle Szenarien werden wir nicht vorbereitet sein können." Wobei jede Kommune selbst die Verantwortung für den Katastrophenschutz trägt.

Die Polizei sei auf mehrtägige Szenarien wie die Hochwasserkatastrophe ebenfalls nicht vorbereitet, sagt Britta Zur, Polizeipräsidentin in Gelsenkirchen. „Wir bekommen aber in solchen Fällen immer Unterstützung von umliegenden Kreispolizeibehörden." Fällt der Notruf aus, werden die Anrufe automatisch an eine andere Polizeibehörde geleitet.

Natürlich sei auch die Polizei sehr stark von einer funktionierenden Stromversorgung abhängig und müsse sich der Frage stellen, was passiert, wenn der Strom über eine längere Zeit ausfällt. Allerdings sind Notstromaggregate vorhanden, Hilfe von anderen Behörden würde ebenfalls kommen. „Die Polizei von Gelsenkirchen wäre also auf keinen Fall von der Außenwelt abgeschnitten!"

Stefan Bisanz, consulting plus, fordert, dass Risikogruppen in Katastrophenszenarien betrachtet werden – was kann passieren, was darf nicht passieren? „Ich glaube, das passiert nicht, weil wir in vielen Bereichen unseres Lebens immer schnelllebiger werden. Informationen werden als Ware gehandelt. Und so ist das auch mit den Risikoszenarien – das Leid ist offenbar nicht groß genug, dass Risiken Präsenz haben." Prävention werde nicht betrieben, „wir reagieren nur." Wenn eine Region von einer Krise betroffen sei, bekämen das andere „maximal noch über die Nachrichten mit".

Dr. Christian Endreß meint: „Wir müssen die Bevölkerung noch viel stärker für solche Szenarien sensibilisieren." Man müsse zudem Selbsthilfefähigkeiten und Nachbarschaftshilfe stärken. Wichtig sei, die Bevölkerung als Partner und selbstständigen Akteur innerhalb der Sicherheitsstrukturen zu betrachten und sie in die Notfallplanung einzubeziehen.

Insgesamt seien wir „in Deutschland sehr reaktiv. Es gelingt uns nicht, vor die Lage zu kommen, Risiken zu antizipieren." Derzeit etwa mache man sich Gedanken darüber, wie man Menschen bei Schadenslagen rechtzeitig per SMS warnen könne. „Dieses System – unter cell broadcasting bekannt – gibt es seit Jahren – und es ist in anderen Ländern bereits erfolgreich in das nationale Warnsystem implementiert."

Axel Schmidt, Salto Systems, berichtet, dass die Notstromversorgung mangelhaft ist – Notstromaggregate seien kaum verbreitet. Gelernt hätten vor allem die, die von einer Katastrophe betroffen waren. „Die nicht betroffen waren, werden ohne die notwendige Sensibilisierung in die nächste Katastrophe hineinlaufen." Und was Sirenen angeht: „Außer auf Facebook fragt keiner: Was ist denn los? Müssen wir irgendetwas machen?'"

Meist herrsche bei Probealarm der Gedanke vor „Wird schon nix passieren" – und falls es wirklich wichtig ist, wird schon jemand anrufen. Bei Evakuierungsübungen blieb jedenfalls bisweilen die Hälfte der Belegschaft in ihren Büros …

Bedrohungen im Fokus

(jgr) Im vergangenen Jahr stand das RP-Forum Sicherheit noch ganz unter dem Vorzeichen von Corona. In diesem Jahr gehöre die Pandemie-Bekämpfung schon zum Alltag, sagte Matthias Körner, Geschäftsführer der Rheinische Post Medien GmbH, bei der Begrüßung der Gäste. Andere Themen seien nun wieder stärker in den Blick gerückt. Als Beispiele nennt Körner die Frage nach der sicheren Stadt, aber auch die Folgen des Klimawandels mit Extremwetterlagen. Der geplante Anschlag auf die Synagoge in Hagen zeige zudem, dass auch die Bedrohung durch Terrorismus nach wie vor aktuell sei. „Es gibt also viele Themen für dieses Forum."

Zum sechsten Mal trafen sich Sicherheitsexperten sowie Vertreter von Organisationen, die mit Sicherheitsfragen befasst sind, um im Forum die Fragen zu diskutieren, die auch die Menschen beschäftigen. „Jedes Mal hat es sich gezeigt, wie wichtig es ist, diesen Kreis zusammenzubringen", sagte Körner. Das Forum biete die Gelegenheit für einen „vitalen Austausch mit konkreten Ergebnissen". „Wir freuen uns, die Plattform für diesen Dialog zur Verfügung stellen zu können", sagte Körner.

Einiges ist diesmal neu: Die Experten diskutierten in den Rudas Studios im Düsseldorfer Hafen. Die Ergebnisse werden auf vielen Kanälen publiziert – in dieser Sonderveröffentlichung, online – und zusätzlich können die Diskussionen auf Video angesehen werden.

Matthias Körner, Geschäftsführer der Rheinische Post Medien GmbH FOTO: RP


Wolfgang Straßer
@-yet


Dr. Christian Endreß
ASW West


Uwe Gerstenberg
consulting plus


Stefan Bisanz
consulting plus


Steffen Schimanski
DRK


Oliver P. Kuhrt
Messe Essen


Sabina Großkreuz
Messe Essen

Mehr im Video

www.rp-forum.de/sicherheit/


Britta Zur
Polizeipräsidentin GE


Axel Schmidt
Salto Systems


Daniel Schleimer
Securitas


Christian Kromberg
Stadt Essen


Pia Kemper
Rheinische Post


Matthias Körner
Rheinische Post

Experten fordern mehr Sensibilität für IT-Sicherheit

Sicherheitsexperten diskutierten in den Rudas Studios, Düsseldorf, über Bedrohungen unterschiedlicher Art und wie ihnen begegnet werden kann. FOTOS: ALOIS MÜLLER

Wie umgehen mit den Cyber-Gefahren? Sicherheitsspezialisten haben da klare Vorschläge, und Praktiker können auf einige Erfahrungswerte verweisen. Das zeigen die Diskussionen beim 6. RP-Wirtschaftsforum Sicherheit.

VON JÜRGEN GROSCHE

Bei der Diskussion zum Thema IT-Sicherheit kommen beim RP-Forum einige Fälle aus der Praxis zur Sprache. Oliver P. Kuhrt (Messe Essen) erinnert an einen Vorfall aus seiner Branche vor zwei Jahren. 2019 wurde die Messe Stuttgart durch einen Hackerangriff über zwei Wochen komplett lahmgelegt. Der Schaden sei immens gewesen. „So etwas lässt sich versicherungstechnisch kaum abdecken“, sagt Kuhrt. „Für uns ist das ein essenzielles Thema“, bilanziert der Messeexperte. Denn Messen seien bis tief in die Systeme mit vielen Partnern vernetzt, über die solche Angriffe auch in die eigenen Systeme eingeschleust werden können.

Dr. Christian Endreß (ASW West) bringt die Bedrohung auf eine einfache Formel: „Alles, was digitalisiert werden kann, das wird heute digitalisiert. Alles was digitalisiert ist, wird angegriffen.“ Unternehmen, Behörden und alle Nutzer brauchen zuallererst einen Basisschutz. „Doch selbst das funktioniert bei vielen nicht“, bedauert Endreß. Er zitiert aus dem Lagebild Wirtschaftsschutz NRW aus dem Jahr 2019, nach dem insbesondere kleine und mittelgroße Unternehmen noch „deutlich Luft nach oben“ hätten. Oft seien die Mitarbeiter nicht ausreichend sensibilisiert.

„Hundertprozentige Sicherheit gibt es nicht“, sagt Wolfgang Straßer (@-yet). Aber die Sicherheitslevels seien allgemein oft zu niedrig. Immer mehr Geschäfts- und Fertigungsprozesse werden digitalisiert. „Sie werden häufig angegriffen.“ Selbst Infrastrukturbereiche seien viel zu einfach zu attackieren. Die Sicherheitsexperten seines Unternehmens seien auch schon mehrfach zu denselben Unternehmen gefahren, die offenbar trotz negativer Erfahrungen ihre Sicherheitssysteme nicht ausgebaut hatten.

Ein ähnliches Beispiel nennt Axel Schmidt (Salto Systems). In Österreich habe ein Hotel trotz mehrfacher Angriffe seinen Basisschutz nicht erhöht. Mehr als einmal hätten die Zimmer-Schließanlagen nicht funktioniert. Immerhin das sei der Uniklinik Düsseldorf im vergangenen Jahr nicht passiert. „Das Zutrittskontrollsystem funktionierte weiter. Es war getrennt vom Rest.“

Christian Kromberg (Stadt Essen, Sicherheitsdezernent) beschreibt die Probleme und Gefahren aus kommunaler Sicht. Auf der einen Seite sollen Städte und Gemeinden ihre Prozesse immer weiter digitalisieren und den Bürgern digitale Zugänge verschaffen. Auf der anderen Seite zählen viele Abläufe zur kritischen Infrastruktur. Kromberg nennt als Beispiele den Notruf oder die Auszahlung von staatlichen Hilfen. Werden sie blockiert, schafft das immense Probleme. Für Kommunen bedeutet dies eine doppelte Herausforderung: „Wir müssen viel Geld in die IT-Sicherheit investieren. Aber wenn trotzdem etwas schiefgeht, müssen wir unsere Dienstleistungen im Zweifel auch wieder analog anbieten können.“

„Die Digitalisierung schafft große Abhängigkeiten“, sagt Uwe Gerstenberg (consulting plus). Die Konsequenzen von Ausfällen sieht er auf einem ähnlichen Niveau wie bei Stromausfällen und zitiert einen Vorfall aus New York im Jahr 2003. Dort war flächendeckend die Stromversorgung gestört. Zwar gab es Notstromaggregate. Doch der Sprit für sie musste angeliefert werden. Tankwagen konnten nicht beladen werden, weil sie dafür ihrerseits auf Strom angewiesen waren. „Wir müssen in der Lage sein, wichtige Abläufe analog umsetzen zu können.“ Generell müsse die Sensibilität für das Thema erhöht werden, sowohl in der Geschäftsführung wie auch bei den Mitarbeitern in Unternehmen und Behörden.

„Auch die Medienbranche ist von Cyberangriffen nicht verschont geblieben“, berichtet Matthias Körner (Rheinische Post) und erwähnt einen Vorfall Ende des vergangenen Jahres. In einem großen Medienhaus in NRW sei die Infrastruktur zeitweise lahmgelegt worden. „Bei uns ist das Thema ganz oben auf der Agenda angesiedelt“, sagt Körner. Er bestätigt die Einschätzung der Experten, dass auch die Mitarbeiter immer wieder für das Thema sensibilisiert werden müssten.

Zu den kritischen Infrastrukturen gehören auch der Bevölkerungsschutz und die Rettungsdienste, die zum Beispiel vom Roten Kreuz geleistet werden. Die Organisationen könnten die Kosten für IT-Sicherheit oft nicht aus eigenen Kräften, zum Beispiel Spenden, finanzieren, sagt Steffen Schimanski (Deutsches Rotes Kreuz). Er sieht darin ein Grundsatzthema: „Wir brauchen fast einen Systemwechsel bei der Finanzierung, zum Beispiel im Gesundheitswesen, wenn wir die kritische Infrastruktur sicher gestalten wollen.“

Ebenfalls in diesem Bereich ist natürlich die Polizei zu verorten. „Die Polizei in NRW hat das Thema Sicherheit im Blick“, sagt Britta Zur, Polizeipräsidentin in Gelsenkirchen. Die Polizei habe massiv in die IT-Sicherheit investiert und Fachkräfte eingestellt. Selbst wenn ein Angriff erfolgreich wäre, sei die Polizei handlungsfähig. Andere Behörden und/oder das Innenministerium würden ausgefallene Funktionen übernehmen. Dennoch stimmt auch die Polizeipräsidentin der Forderung der Sicherheitsexperten zu: „Wir müssen uns noch stärker mit der Frage beschäftigen: Was wäre, wenn …“

Sicherheit müsse in einfachen Grundsätzen erklärbar sein, fordert Stefan Bisanz (consulting plus Sicherheit). „Der erste Satz lautet: Das eine tun, das andere nicht lassen“ – also in Sicherheit investieren, aber analoge Prozessabläufe parallel beizubehalten. Bisanz erinnert an die Flutkatastrophe. Im Ahrtal hätten manche ältere Bewohner Unterlagen in Aktenkoffern parat gehabt, während einige Jüngere auf wichtige Daten keinen Zugriff gehabt haben, weil sie nur digital gespeichert waren, aber die Netze nicht funktionierten.

Cyberangriffe haben nicht nur wirtschaftliche Schäden zur Folge. Kromberg nennt als Kommunalvertreter auch politische Aspekte. Viele Angriffe hätten zum Ziel, das Vertrauen der Bürger in die Infrastruktur zu erschüttern und damit die Demokratie an sich zu destabilisieren. Britta Zur verweist auf weitere Bedrohungen aus dem Netz, zum Beispiel Kinderpornografie. Zur Bekämpfung habe die Polizei viele Spezialisten ausgebildet. Außerdem habe man die Präventionsarbeit ausgebaut. Vertreter der Polizei besuchen Schulen, „um ein Bewusstsein dafür zu schaffen, wie gefährlich Smartphones in Kinderhänden sein können“.

Da Digitalisierung überall stattfinde, müsste das Thema schon in der Schule behandelt werden, meint auch Wolfgang Straßer. Zum Beispiel, wie die Kinder mit Einladungen von Unbekannten umgehen sollten. Generell fordert er: „IT-Sicherheit darf nicht nur als Kostenfaktor betrachtet werden. Sich mit dem Thema zu befassen, ist zentraler Bestandteil eines Risikomanagements – nicht nur der Industrie, auch der Gesellschaft.“

Die Teilnehmer

Wolfgang Straßer
@-yet GmbH, Geschäftsführender Gesellschafter
Dr. Christian Endreß
Allianz für Sicherheit in der Wirtschaft West e.V. (ASW West) Geschäftsführer
Uwe Gerstenberg
consulting plus GmbH, Geschäftsführer
Stefan Bisanz
consulting plus GmbH, Geschäftsführer
Steffen Schimanski
Deutsches Rotes Kreuz, Landesverband Nordrhein e. V., Abteilungsleiter Nationale Hilfsgesellschaft
Oliver P. Kuhrt
MESSE ESSEN GmbH, Geschäftsführer
Sabina Großkreuz
MESSE ESSEN GmbH, Geschäftsbereichsleiterin Marketing
Britta Zur
Polizeipräsidium Gelsenkirchen, Präsidentin
Axel Schmidt
SALTO SYSTEMS GmbH, Geschäftsführer
Daniel Schleimer
SECURITAS Services GmbH, Geschäftsführer
Christian Kromberg
Stadt Essen, Ordnungsdezernent
Pia Kemper
Rheinische Post Forum, Leitung Finanz- und Wirtschafts-Extras
Matthias Körner
Rheinische Post Medien GmbH, Geschäftsführer

Moderation
José Macias, Rheinland Presse Service GmbH, Uwe Gerstenberg

Cyberattacken: Unterschätzte Gefahr aus dem Internet

Angriffe aus dem Internet auf Firmen-, Privat- und Behördenrechner richten Milliardenschäden an, lähmen ganze Bereiche. Und dennoch mangelt es an Risikobewusstsein. Ein nachdrücklicher Impuls für die Expertendiskussion.

(jgr) Wolfgang Straßer weiß, wovon er spricht. In der dritten Diskussionsrunde des 6. RP-Wirtschaftsforums Sicherheit geht es um Cyberattacken und andere Probleme rund um die IT-Sicherheit. Straßer wird mit seinen Spezialisten des Leichlinger Unternehmens für IT-Sicherheit @-yet immer wieder quasi als Nothelfer in Unternehmen gerufen, wenn diese erfolgreich angegriffen wurden. „Allein seit Oktober 2019 haben wir 126 Fälle bearbeitet, durchschnittlich einen pro Woche – vom Konzern mit mehr als 30.000 Mitarbeitern bis hin zu Start-ups mit kleiner zehn“, berichtet Straßer in seinem Impulsvortrag für die Gesprächsrunde.

Die Schäden für Unternehmen durch Hackerangriffe sind immens. Auf 223 Milliarden Euro im Jahr schätzt der Branchenverband Bitcom das Volumen in Deutschland. In Nordrhein-Westfalen seien 630.000 Unternehmen betroffen mit einer Schadenssumme von 46,6 Milliarden Euro, schätzt Straßer. Ein prominentes Beispiel aus der Region ist der Angriff auf die Düsseldorfer Uniklinik vor einem Jahr. Ein Großteil der Rechner war von einer Verschlüsselungssoftware gesperrt worden. Eine Patientin starb in der Folge. Gerade solche Attacken mit Ransomware (Erpressersoftware) häufen sich. Die Erpresser verlangen Geld für den Schlüssel, mit dem die Computer wieder entsperrt werden können.


Wolfgang Straßer warnt im Impulsvortrag vor Cyberattacken.

„IT ist heute überall“, sagt Straßer, „in Behörden, privaten Haushalten, Unternehmen und in der Infrastruktur“. Wenn die IT ausfällt, sei das mehr als einmal eine Katastrophe – ähnlich wie ein Stromausfall. Neben dem Stillstand von Unternehmen, Krankenhäusern, Bahnen oder Ampeln führen insbesondere in der Wirtschaft, aber auch beim Staat, Spionageangriffe zu großen Schäden. Oft werden sie erst nach Jahren bemerkt. „Das Unternehmen kommt erst drauf, wenn es seine gerade in der Entwicklung befindlichen Produkte plötzlich bei der Konkurrenz sieht“, schildert Straßer Begebenheiten, die häufig vorkommen. Auch ein beliebter Trick: In gefälschten Mails verlangt der angebliche Geschäftsführer oder Abteilungsleiter die Begleichung von Rechnungen. Mitarbeiter fallen darauf herein – das Geld ist weg.

Haben denn die Schadensmeldungen Konsequenzen, wird mehr auf Sicherheit geachtet? „Die Angriffe sind immer noch zu leicht möglich“, bedauert der Sicherheitsspezialist. Er vermisst ein Risikobewusstsein nicht nur bei Mitarbeitern, sondern vor allem ganz oben in den Chefetagen. „Die IT ist oft zu schlecht ausgestattet.“