SCHWERPUNKT HEFT

G06715

1.12.2023

Nr. 23

sicherheits.berater

Informationsdienst für Sicherheit in Wirtschaft und Verwaltung

446 ›››

Resilienz ist alles

SCHWERPUNKT BUSINESS RESILIENCE

Zweite Seite

Resilienz ist alles

Liebe Leserinnen und Leser,

Resilienz ist in allen Lebensbereichen ein hohes Gut. Selbst mit unserem auf die Sicherheit von Unternehmen und Behörden verengten Blick deckt der Begriff eine enorme inhaltliche Spannbreite ab. Meint man damit noch oder schon oder nur Business Continuity Management?

Da wir Praktiker sind, wenngleich mit dem nötigen theoretischen Unterbau, werden wir uns dem Thema hier im Heft vorzugsweise von der praktischen Seite her nähern, damit Sie daraus einen geschäftlichen bzw. beruflichen Nutzen ziehen können.

Mit Resilienzbestrebungen wird (endlich) nicht nur dem Täter hinterhergehetzt, sondern werden Denkmodelle entwickelt, die auch Entwicklungen antizipieren, seien sie absehbar wie Veränderung klimabedingter Ereignisse, konkret wie das alljährliche Hochwasser, oder nur abstrakt wie Hochwasserkatastrophen im Ausmaß Ahrtal. Es lohnt sich, das, was heute noch als unwahrscheinlich gilt und in einer Risikobetrachtung niedrig gewichtet wird, dennoch zu durchdenken, um vorbereitet zu sein.

Der Autor hat soeben am DACH-Forum der SIMEDIS Akademie in Tirol teilgenommen, auf dem neben Business Continuity und Reaktionspotenzial auf Cyberattacken auch durch künstliche Intelligenz unterstützte Risikoanalysen thematisiert wurden. Sogenannte LLMs (Large Language Models) müssen als Fluch und Segen betrachtet werden. Sie erleichtern, und vor allem, beschleunigen die Analyse von Daten und die Auswertung von Berichten. Dies gilt für Textinformationen ebenso wie für Bilder, wie sie in der Videoanalytik genutzt werden. Die Kehrseite der Medaille stellen Missinterpretationen gelieferter Daten und die ebenfalls unterstützte Generierung von Falschinformationen in zunehmend besserer Qualität dar.

Ich weiß aus Hunderten von Sicherheitsberatungsprojekten: Sie können die Resilienz Ihres Unternehmens oder Ihrer Behörde gezielt stärken, wenn Sie wie bei einem Rosenkranz die Perlenschnur der Sicherheitsstrategie abarbeiten. Aus der Gefährdungsanalyse folgen die dringlichsten Maßnahmen zur Vorbeugung. Business Impact-Analysen (BIA) zeigen die Schmerzstellen im Unternehmen auf. Notfallpläne, Krisenmanagement und Krisenkommunikation unterstützen bei der Bewältigung auftretender Ereignisse. Das Geschäft geht weiter dank eines umfangreichen Business Continuity Management. Die Aufarbeitung der Ereignisse und eine revisionssichere Dokumentation erlauben, aus dem Schaden klug zu werden. Erfahrungen fließen in regelmäßige Trainings von Krisenstäben und Mitarbeiter auf allen Ebenen ein. Und dann startet der Regelkreis (pardon der Rosenkranz) aufs Neue.

Als Sicherheitsverantwortlicher können Sie Ihre Fähigkeiten in Sachen Resilienz und Business Continuity Management auch trainieren bzw. sich weiterbilden. Bei der SIMEDIA Akademie (www.simedia.de), die sich den Flur mit der Redaktion des Sicherheits-Berater teilt, finden Sie z. B. ein Seminar „Die Rolle der Unternehmenssicherheit im Kontext der organisatorischen Resilienz“ und einen Lehrgang „Business Continuity Professional, BdSI“.

Der Autor Peter Stürmann
Diplom-Kaufmann

Herausgeber des Sicherheits-Berater, Geschäftsführer aller Unternehmen der von zur Mühlen-Gruppe mit den Spezialgebieten Sicherheitsstrategie und Security-Audits

SCHWERPUNKT BUSINESS RESILIENCE

GASTBEITRAG

Resilienz statt BCM oder Resilienz durch BCM – das ist hier die Frage

Wesentlicher Baustein?

Das Konzept der Resilienz, auch als organisationale Resilienz oder Business Resilience bezeichnet, ist mittlerweile auch in den Disziplinen des Sicherheitsmanagements angekommen. Ist Business Continuity Management (BCM) jetzt ein Auslaufmodell und organisationale Resilienz das neue BCM? Oder ist BCM vielmehr ein wesentlicher Baustein für ein resilientes Unternehmen neben anderen Bausteinen?

Zwei Normen

Gleich zwei Normen sollen bei der Klärung der Begrifflichkeit und der Umsetzung in Organisationen helfen. Im März 2017 wurde der ISO-Standard ISO 22316:2017 mit dem langen Titel „Security and resilience – Organizational resilience – Principles and attributes" veröffentlicht. Der ISO-Standard wurde durch das Technical Committee ISO/TC 292 Security and resilience erarbeitet, das auch die ISO-Standards rund um den ISO 22301:2019 Business Continuity Management verantwortet. Organisationale Resilienz ist laut ISO 22316 „the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper".

» „Resilience" leitet sich aus dem lateinischen „resilire" ab, „zurückspringen". «

Der englische Begriff „Resilience" leitet sich aus dem lateinischen Begriff „resilire" ab, gleichbedeutend mit „zurückspringen". Der Duden definiert Resilienz als „psychische Widerstandskraft; Fähigkeit, schwierige Lebenssituationen ohne anhaltende Beeinträchtigung zu überstehen".

Bedrohungsszenarien

Unternehmen sind ständig internen und externen Veränderungen ausgesetzt. Veränderungen können positiv für das Unternehmen sein, aber auch zu Bedrohungen für das Unternehmen werden. Bedrohungen können als Störungen, Notfälle, Krisen oder Katastrophen die Produkt- und Serviceerbringung eines Unternehmens beeinträchtigen oder gar unterbrechen. Organisationale Resilienz betrachtet hierbei ein weites Spektrum an Bedrohungsszenarien von graduellen internen und externen Veränderungen bis hin zu

akuten oder abrupten Notfallszenarien. Die zu betrachtenden Szenarien reichen daher von unternehmensinternen Bedrohungsszenarien wie beispielhaft Know-how-Verlust bei Mitarbeitern, Fehlern oder vorsätzlichen Handlungen bis hin zu externen Bedrohungen wie Änderungen in Absatzmärkten, Wettbewerbsumfeld, technologischer Wandel, politische Rahmenbedingungen sowie BCM-Risiken für Geschäftsprozesse, Personal, Gebäude, IT und Dienstleister.

ISO 22316:2017

Diese sehr umfassende Sicht auf Bedrohungen und Risiken macht deutlich, dass nicht eine einzelne Disziplin im Unternehmen für Resilienz verantwortlich sein kann. In der Anlage des ISO 22316:2017 werden daher beispielhaft zwanzig relevante Managementdisziplinen aufgeführt, die zum Erreichen einer Organisatorischen Resilienz beitragen. Zu den aufgeführten Disziplinen zählen alle GRC-Disziplinen (Governance, Risk and Compliance), darüber hinaus aber auch Kommunikations- und Personal-Management sowie Strategische Planung, Qualitätsmanagement und Controlling. Unter den alphabetisch aufgezählten Disziplinen findet sich auch gleich zu Beginn das Business Continuity Management, gefolgt von Krisenmanagement und Cyber Security Management.

» Das Business Continuity Management hat gleich mehrere Werkzeuge im Köcher. «

Resiliente Unternehmen verfügen über die Fähigkeit, Risiken und Chancen frühzeitig zu erkennen und über eine gute Vorbereitung auf negative Veränderungen oder disruptive Schocks. Studien zeigen, dass sich resiliente Organisationen vor allem durch ihre Unternehmenskultur und Kundenorientierung von anderen Organisationen unterscheiden (Vgl. Ostschweizer Fachhochschule, www.provida.ch, Kurzlink https://tinyurl.com/u3en27by). Organisationen, die eine starke Unternehmenskultur besitzen, schnelle organisatorische und strukturelle Veränderungen zulassen, ein hohes Vertrauen in zufriedene Mitarbeiter haben und eine hohe Führungsqualität aufweisen, erweisen sich als widerstandsfähiger bei Unternehmenskrisen. Resiliente Unternehmen zeichnen sich zudem durch eine hohe Kundenorientierung und -bindung aus. Ein starkes Risikomanagement, Compliance und resiliente Mitarbeiter sind ebenfalls – allerdings weniger bedeutende – Merkmale resilienter Unternehmen.

Welchen Beitrag kann das Business Continuity Management (BCM) zu einem resilienten Unternehmen leisten?

Transparenz

Ein wesentlicher Faktor für die organisationale Resilienz ist die Transparenz über Kunden, Produkte, Prozesse, interne und externe, horizontale und vertikale Abhängigkeiten über die gesamte Wertschöpfungskette. Welches sind die kritischen Glieder dieser Wertschöpfungskette, die es gilt vor Unterbrechungen zu schützen und in einem Notfall schnell wiederherzustellen, um das Überleben des Unternehmens zu sichern?

Kritische Assets

Nur auf Basis dieser Transparenz können die kritischen Assets des Unternehmens identifiziert und angemessen geschützt werden. Zu diesem Schutz gehört die Identifikation und Überwachung der Risiken, die präventiven Maßnahmen zum Schutz vor Angriffen, Fehlern und Ausfällen sowie die reaktiven Maßnahmen zur Notfall- und Krisenbewältigung und Wiederherstellung.

Business Impact Analyse

Das Business Continuity Management hat gleich mehrere Werkzeuge im Köcher, um diese Transparenz herzustellen. Die Business Impact Analyse (BIA) hat die Identifikation zeitkritischer Geschäftsprozesse für die Notfallvorsorge zum Ziel. Gleichzeitig vermag sie aber auf Grund der prozessualen Herangehensweise eine hohe Transparenz über die Wertschöpfungsketten des Unternehmens schaffen. Nicht selten führt die BIA zu einer (Wieder-)Belebung des Prozessmanagements im Unternehmen und damit zu einer stärker prozess-, produkt- und serviceorientierten Sicht auf das Unternehmen. Im Rahmen

der BIA werden zudem horizontale und vertikale Abhängigkeiten zwischen Prozessen und deren Ressourcen wie Personal, IT, Gebäude, Anlagen und Dienstleister identifiziert. Dieser Informationsverbund ermöglicht erst die Schaffung eines durchgehenden Sicherheitsniveaus für die kritischen Wertschöpfungsketten.

BCM Risk-Assessment

Im Rahmen des BCM Risk-Assessments werden Single-points-of-failures (SPOF) für die kritischen Geschäftsprozesse identifiziert. Risiken, die bislang nicht erkannt oder nicht richtig eingeschätzt wurden, können hierdurch minimiert werden. Notfall- und Krisenmanagementpläne versetzen das Unternehmen in die Lage, schnell und effektiv das definierte Mindestniveau der Produkte und Services für die Kunden wiederherzustellen.

Zentrale Grundlagen

BCM ist alleine nicht in der Lage, ein Unternehmen resilient und damit widerstandsfähig gegen alle internen und externen Bedrohungen zu machen. BCM schafft jedoch zentrale Grundlagen und ist ein wichtiger Baustein, gemeinsam mit den anderen Disziplinen, um die Widerstandsfähigkeit eines Unternehmens deutlich zu erhöhen und damit robuster gegen interne und externe Störungen zu machen.

Der Gastautor Matthias Hämmerle

Selbständiger Unternehmensberater und Auditor für Business Continuity- und Krisenmanagement sowie Informationssicherheit. Herausgeber der BCM-News (www.bcm-news.de)

Fragen an unseren Gastautor? +49170 7738581
www.haemmerle-consulting.de
mhaemmerle@haemmerle-consulting.de

SCHWERPUNKT BUSINESS RESILIENCE

GESETZESLAGE

Die BIA als Grundlage guter Entscheidungen

EU-Richtlinie 2016/1148

Bereits 2015 wurden die Betreiber kritischer Infrastrukturen (auch KRITIS-Unternehmen genannt) durch das IT-Sicherheitsgesetz (IT-SIG) auf Grund wachsender Cyberbedrohungen verpflichtet, entsprechende Sicherheitsanforderungen nachweislich zu erfüllen. Zudem kam man damit der Umsetzungspflicht zu der seit 2016 geltenden EU-Richtlinie 2016/1148, der sogenannten Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie), nach. Zur weiteren Konkretisierung der Sektoren und Festlegung von Schwellenwerten für den Geltungsbereich dieses Gesetzes für KRITIS-Unternehmen wurde 2017 die BSI-KRITIS-Verordnung mit seiner aktuellen Fassung aus 2022 eingeführt. Hierbei zeigt sich eine juristisch eher untypische Entwicklung dadurch, dass die Gesetzeslage im Bereich der Cybersicherheit der der physischen Sicherheit von KRITIS-Unternehmen deutlich voraus ist. Die CER-Richtlinie (EU) 2022/2557 (Critical Entities Resilience) reguliert auf EU-Ebene seit Inkrafttreten im Dezember 2022 die europaweite Resilienz kritischer Infrastrukturen, um Versorgungssicherheit und wirtschaftliche Stabilität zu gewährleisten.

KRITIS-DachG

Aus dieser Umsetzungspflicht wurde im Juli 2023 der erste Referentenentwurf zum Schutz kritischer Infrastrukturen in Form des sogenannten KRITIS Dachgesetzes (KRITIS-DachG) veröffentlicht, welcher nach aktuellem Stand Oktober 2024 in Kraft treten soll.

Das KRITIS-DachG steht neben den bisherigen Regelungen zum Cyberschutz, hier allerdings mit Blick auf die physische Resilienz von Unternehmen der kritischen Infrastruktur. Es soll erstmalig bundeseinheitlich das Verständnis kritischer Anlagen regeln und Vorgaben für die physische Sicherheit formulieren (vgl. KRITIS-DachG-RefE Begründung, V, Nr. 1). Zu den wesentlichen Inhalten des KRITIS-DachG-RefE gehören die:

Wesentliche Inhalte

- *„Vorgaben zur Identifizierung von kritischen Anlagen und kritischen Anlagen mit besonderer Bedeutung für Europa.*
- *Vorgaben zur Registrierung von kritischen Anlagen.*
- *Etablierung von staatlichen Risikoanalysen und -bewertungen für kritische Dienstleistungen.*
- *Gesetzliche Verankerung wesentlicher nationaler Anforderungen für Resilienzmaßnahmen von Betreibern kritischer Anlagen.*
- *Einführung eines Meldewesens für Störungen.*
- *Umsetzung einer Ausschlussklausel für kritische Anlagen, die einen besonderen Bezug zum Sicherheits- und Verteidigungsbereich aufweisen. Für solche kritische Anlagen gelten dann die jeweils einschlägigen Vorgaben für den Sicherheits- bzw. Verteidigungsbereich.*
- *Einführung von Bußgeldvorschriften.“* (Begründung, A. II. KRITIS-DachG-RefE)

Kritische Anlagen

Mit diesem Referentenentwurf wurde erstmalig auch der Adressatenkreis näher festgelegt, der nach § 7 alle kritischen Infrastrukturen und kritischen Anlagen umfasst, auch solche, die für Europa von Bedeutung sind. Als kritische Anlagen werden alle Anlagen *„aus den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum, öffentliche Verwaltung oder Siedlungsabfallentsorgung“* definiert, die die geltenden Schwellenwerte erreichen oder überschreiten (vgl. § 4 KRITIS-DachG-RefE).

KRITIS-Verordnung

Die bestehende KRITIS-Verordnung (KritisV) gibt bereits heute schon Aufschluss darüber, welche Schwellenwerte zur näheren Bestimmung anzunehmen sind. Gemessen an der bisherigen Entwicklung und Festlegung der Schwellenwerte ist davon auszugehen, dass diese sich weiter verschärfen und Anlagen zukünftig als kritisch zu bewerten sind, auch wenn sie aktuell nicht die angegebenen Schwellen der geltenden KritisV erreichen oder überschreiten. Insbesondere Anlagen, die nahe dieser Schwellwerte liegen, sollten diesen Umstand in Entscheidungen rechtzeitig einbeziehen. Diesbezüglich ist zukünftig eine gemeinsame Regelung zu kritischen Anlagen sowie wichtiger und besonders wichtiger Einrichtungen für das IT-SIG und das KRITIS-DachG geplant (vgl. KRITIS-DachG-RefE Begründung, A, I.).

Resilienzmaßnahmen

§11 KRITIS-DachG-RefE verpflichtet zu sogenannten Resilienzmaßnahmen. Diese müssen einerseits verhältnismäßig sein und sich an den Vorgaben der Risikoanalyse und Bewertung aus §§ 9 und 10 KRITIS-DachG-RefE orientieren und den Stand der Technik einhalten. An dieser Stelle wird auch die tragende Rolle eines funktionierenden Business Continuity Management Systems (BCMS) deutlich, was den aktuellen Stand der Technik in Bezug auf Managementsysteme für Unternehmensresilienz darstellt.

Risikoanalyse
Ein Prozess, bei dem die möglichen Risiken und ihre Ursachen analysiert werden. Mit dem Ziel, ein klares Verständnis der Risiken zu entwickeln.

Wann statt Wie

Problematisch kann es jedoch werden, wenn Organisationen immer noch darüber diskutieren, ob die Einführung eines BCMS zum aktuellen Zeitpunkt erforderlich ist, statt über die Art der Einführung und mögliche Umsetzungen zu sprechen.

Zeitpunkt als Problem

Eine solche Einführung erfordert Vorbereitung, Zeit und Ressourcen – insbesondere dann, wenn Geschäftsprozesse noch nicht dokumentiert wurden oder es sogar am prozessualen Verständnis mangelt. Entscheidend ist zudem, dass ein Business Continuity Management (BCM) nicht als ein generelles und starres System zu verstehen ist, das standardisiert übernommen werden kann.

Angepasstes BCMS

Vielmehr sollte ein für die Organisation angepasstes BCMS implementiert werden, was die Organisation und vor allem die betroffenen Bereiche nicht überfordert. Schließlich ist die Implementierung eines neuen Managementsystems selten ein ressourcenschonendes Unterfangen und auch keine Aufgabe, die als berufliche Nebentätigkeit zu erbringen ist. Daher sollte man sich für eine Einführungsvariante entscheiden, die sich zunächst um die wesentlichen Lücken der Organisation kümmert und im Ergebnis auch einen Mehrwert für das Unternehmen darstellt.

Zielführende Umsetzung

Eine zielführende Umsetzung eines BCMS ermöglicht es den Verantwortlichen auf Basis einer angepassten Business Impact Analyse (BIA), eine valide und reliable Entscheidung zu Resilienzmaßnahmen zu treffen, die im Sinne des KRITIS-DachG-RefE auch eine Bewertung in Bezug auf ihre Verhältnismäßigkeit ermöglichen. Demnach ist eine Maßnahme verhältnismäßig, wenn sie angemessen und geeignet ist, das angestrebte Ziel zu erreichen.

Risikobewertung
Sie beinhaltet die Einschätzung der Wahrscheinlichkeit des Eintretens eines Risikos sowie die Bewertung der potenziellen Auswirkungen. Mit dem Ziel zu bestimmen, welche Risiken akzeptabel sind, um Maßnahmen zu ergreifen die Risiken zu mindern oder zu managen.

Gleiches gilt für die nach einer BIA erforderliche Risikobeurteilung. Die Risikoanalyse und Risikobewertung bilden die Grundlage für eine effektive Risikobeurteilung, die Organisationen dabei hilft, valide Entscheidungen zu Risikomanagementstrategien und -maßnahmen zu treffen.

Elemente des BBK

Hierbei sind die gem. § 9 Abs. 2 KRITIS-DachG-RefE vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zur Verfügung gestellten Elemente für die Risikoanalyse und -bewertung zu berücksichtigen. Auf Grundlage dieser Ergebnisse wäre eine Überprüfung auf vorhandene Resilienzmaßnahmen in bereits existierenden Resilienzplänen möglich, um diese falls erforderlich zu ergänzen oder auch neue Pläne zu erstellen. Anschließend können diese Maßnahmen im Rahmen von Übungen und Test auf deren Ziele geprüft werden.

Bewusste Entscheidungen

Im Ergebnis wäre dann auch eine Bewertung möglich, ob die Resilienzmaßnahmen angemessen und geeignet sind, das angestrebte Ziel zu erreichen. Demnach können

Entscheidungen zu möglichen Resilienzmaßnahmen nur bewusst und valide getroffen werden, wenn die Grundlagen, auf die sie zurückzuführen sind, auch stringent nachvollziehbar sind und sich die geltenden Pläne in vorherigen Tests und Übungen bewährt haben. Gleiches sollte auch bei den Pflichten aus § 11 Abs. 6 ff. KRITIS-DachG-RefE in Bezug auf die zweijährige Nachweispflicht zu Resilienzplänen und Resilienzmaßnahmen gegenüber dem BBK oder einem Auditor berücksichtigt werden.

Neun Monate nach Registrierung

Weiterhin sind gem. § 11 Abs. 3 unter anderem angemessene Reaktionen auf Vorfälle und die Wiederherstellung der Geschäftskontinuität zu gewährleisten. Gem. §10 Abs. 1 KRITIS-DachG-RefE ist bereits neun Monate nach Registrierung bei einer vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gemeinsam eingerichteten Registrierungsstelle (vgl. § 8 Abs. 1 KRITIS-DachG-RefE) eine Risikobeurteilung durchzuführen.

Angemessene Schulungsanforderungen

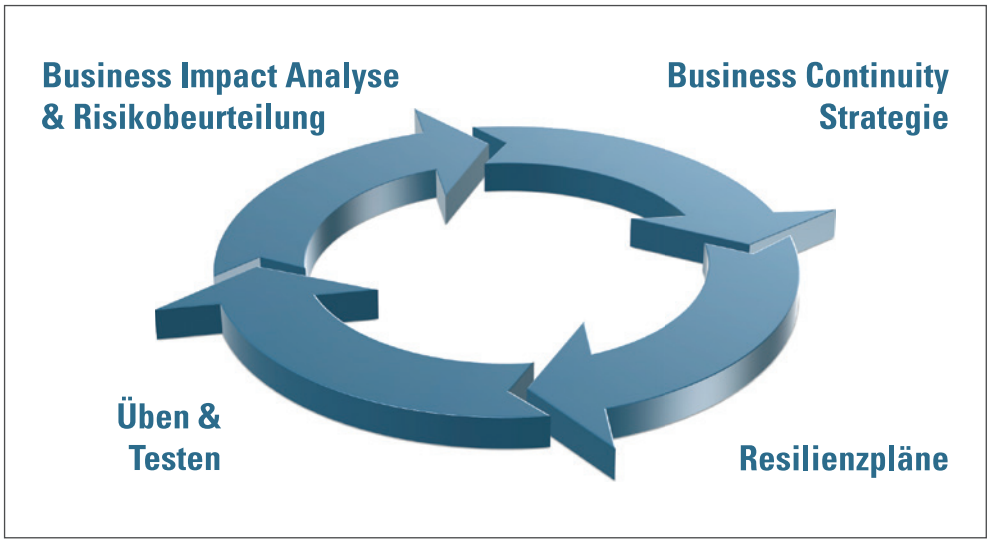
In Bezug auf das verantwortliche Personal ist zu gewährleisten, dass diese durch Übungen und Schulungen sensibilisiert werden. Ebenso werden angemessene Schulungsanforderungen und Qualifikationen an verantwortliches Personal gestellt, die sich nach Auslegung des Autors auch auf die verantwortlichen Geschäftsführer erstrecken und eine persönliche Teilnahme an derartigen Maßnahmen erfordern (vgl. Anhang 1 nach § 11 Abs. 1 KRITIS-DachG-RefE).

»Auch das verantwortliche Personal ist zu schulen.«

Ungeachtet der noch bis Anfang 2026 ausbleibenden Pflichten aus §§ 6 bis 8 und §§ 10 bis 12 des KRITIS-DachG-RefE und ebenso der erst Januar 2027 in Kraft tretenden Bußgeldvorschriften gem. § 19 KRITIS DachG Ref. E. stellt sich die vorgelagerte Herausforderung, eine entsprechende Grundlage zu schaffen, um diese Pflichten, wie unter anderem eine Risikobeurteilung, überhaupt durchführen zu können. Das bedeutet, dass unter anderem Geschäftsprozesse allumfänglich zu dokumentieren sind.

BIA-Assessment

Zudem sind zeitkritische Prozesse durch ein sogenanntes BIA-Assessment zu identifizieren und anschließend eine BIA für die zeitkritischen Prozesse durchzuführen. Um einerseits einen auditfähigen und auch ernst gemeinten Reifegrad der Organisation zu erreichen, sind mehrere Durchläufe eines BCM-Lebenszyklus erforderlich. Daher ist davon auszugehen, dass eine Einführung eines BCMS erst mit Gültigkeit des KRITIS-DachG im Oktober 2024 die Einhaltung der oben genannten Pflicht zur Vorlegung einer Risikobeurteilung und Resilienzplänen als auch Umsetzung von Resilienzmaßnahmen innerhalb der angegebenen Fristen deutlich erschweren kann.



Bildquelle: ah/VZM GmbH

Wohl keine Repressionen

Repressionen sind in Bezug auf eine direkte gesetzliche Pflicht aus dem KRITIS-DachG mangels Gültigkeit nicht zu erwarten. Mögliche Ansprüche aufgrund einer vernachlässigten Sorgfaltspflicht und Verantwortlichkeit von Geschäftsführern gem. § 93 Aktiengesetz (AktG) mangels ergriffener Resilienzmaßnahmen haben aus Sicht des Autors jedoch eine hohe Relevanz und sollten bei der strategischen Entscheidung zur organisationalen Resilienz berücksichtigt werden.

Fazit

Iteratives Vorgehen

Aus Sicht des Autors ist daher ein iteratives (schrittweises) Vorgehen einer meist überambitionierten ganzheitlichen Einführung vorzuziehen, um die dafür erforderlichen Ressourcen zu schonen. Daher sollten Unternehmen, die auf Grundlage der aktuellen Gesetze den Unternehmen kritischer Infrastruktur zuzuordnen sind, sich bereits heute mit der Einführung eines BCMS auseinandersetzen.

Der Autor Christian Horres
Kriminologie, Kriminalistik und Polizeiwissenschaft M. A.

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater mit den Spezialgebieten Business Continuity Management und Risk Management

SCHWERPUNKT BUSINESS RESILIENCE

COACHING

Resilienz durch ein lebendiges BCMS

Dieser Artikel soll Führungskräfte und Sicherheitsverantwortliche ermutigen, über die technischen und organisatorischen Aspekte von BCM (Business Continuity Management) hinauszudenken und die menschliche Komponente in den Mittelpunkt ihrer Resilienzstrategien zu stellen.

In einer Zeit, in der Unternehmen zunehmend komplexen und vielfältigen Risiken ausgesetzt sind, ist es entscheidend, nicht nur auf Krisen zu reagieren, sondern sie vorausschauend zu managen. Das Business Continuity Management System (BCMS) bietet hier einen strukturierten Ansatz, um Unternehmen widerstandsfähiger zu machen. Jedoch stellt die Einführung eines BCMS, z. B. durch einen externen Berater, lediglich den ersten Schritt dar. Um wirklich wirksam zu werden, muss sich die Einführung in eine tiefer verwurzelte Resilienzkultur verwandeln.

Der Kern des BCM: Ziele und Notwendigkeiten

Wiederherstellung der Betriebsfähigkeit

Business Continuity Management (BCM) zielt darauf ab, die Auswirkungen von Unterbrechungen und Krisen auf die Geschäftstätigkeit zu minimieren und eine schnelle Wiederherstellung der Betriebsfähigkeit zu ermöglichen. Die Hauptziele von BCM sind:

- Identifikation potenzieller Bedrohungen und Schwachstellen der zeitkritischen Prozesse
- Sicherstellung einer effektiven Reaktion im Krisenfall durch geübte und getestete Wiederanlaufpläne

- Aufrechterhaltung zeitkritischer Geschäftsprozesse unter allen Umständen
- Minimierung von Ausfallzeiten und finanziellen Verlusten
- Schutz des Unternehmensimages und der Kundenbeziehungen

Strategische Notwendigkeit

Die Implementierung eines BCMS ist weit mehr als eine gute Geschäftsentscheidung: Sie ist eine strategische Notwendigkeit. Ein professionell etabliertes BCMS unterstützt Unternehmen maßgeblich dabei, systematische und robuste Verfahren zu konzipieren und einzuführen. Dieses Vorgehen ist entscheidend, um auch in Zeiten schwerwiegender Betriebsstörungen die Aufrechterhaltung essenzieller Geschäftsprozesse und somit die kontinuierliche Handlungsfähigkeit des Unternehmens sicherzustellen.

Über die formale Einführung hinaus: das Schaffen einer Resilienzkultur

Unternehmenskultur

Ein BCMS wird jedoch nur dann sein volles Potenzial entfalten, wenn das gesamte Unternehmen die Notwendigkeit von Resilienz verinnerlicht und aktiv lebt. Es geht nicht darum, Checklisten abzuarbeiten, sondern um die Entwicklung einer Unternehmenskultur, in der jeder Mitarbeiter sich der Bedeutung von BCM bewusst ist und im Einklang damit handelt.

Die Bedeutung von Überzeugung und Coaching

Wichtigkeit und Verständnis

Damit ein BCMS nicht nur auf dem Papier existiert, müssen die Verantwortlichen mehr als nur fachliche Experten sein. Sie müssen in der Lage sein, die Geschäftseinheiten von der Wichtigkeit der Business Continuity zu überzeugen. Das erfordert ausgeprägte kommunikative Fähigkeiten und ein tiefes Verständnis für die innerbetrieblichen Abläufe und Kulturen.

Fähigkeiten fördern

Zielgerichtetes Coaching kann an dieser Stelle ansetzen, indem es nicht nur die fachlichen Inhalte von BCM vermittelt, sondern auch die Fähigkeit fördert, diese Inhalte praxisnah in die Unternehmenskultur zu integrieren. Dies beinhaltet:

- Unterstützung bei der Erstellung einer praxistauglichen BCM-Roadmap
- Moderationsbegleitung bei der Durchführung der ersten Business Impact Analysen (BIA)
- Systemisches Coaching der BCM-Organisation und ihrer Verantwortlichen.

Überzeugende BCM-Verantwortliche

Die Implementierung eines BCMS als nachhaltige Lösung zur Erhöhung der Unternehmensresilienz ist ein umfassender Prozess, der weit über die reine formale Einführung hinausgeht. Es bedarf einer resilienten Unternehmenskultur und überzeugungskräftiger BCM-Verantwortlicher, die durch zielgerichtetes Coaching in die Lage versetzt werden, diese Kultur im Unternehmen zu verankern. Nur dann kann ein BCMS zu einem lebendigen und effektiven Teil der Unternehmensführung werden, der im Krisenfall seinen wahren Wert beweist.

Die Autorin Susanne Kufeld
Master of Arts – M. A. , BCCM Business Coaching und Change Management

Sicherheitsberaterin, Redaktionsmitglied des Sicherheits-Berater mit dem Spezialgebiet Business Resilience, CISO bei der Messe Berlin

Schwerpunkt Business Resilience

BCM

Krisenmanagement – wer braucht das schon?

Beispiel Haftpflichtversicherung

Haben Sie eine Haftpflichtversicherung? Wann haben Sie diese zum letzten Mal genutzt? Auch wenn es schon ein paar Jahre her ist, hatten Sie dann jemals den Gedanken, die Police zu kündigen? Oberflächlich betrachtet macht sie ja keinen Sinn, da sie nur Geld kostet, aber im Alltag keinen messbaren Nutzen für Sie bringt. Mit dem Jahresbeitrag könnte man vielleicht doch was Schöneres machen, z. B. mal wieder ins Konzert gehen oder seinem Partner etwas schenken.

Notfallvorsorge

Mit an Sicherheit grenzender Wahrscheinlichkeit haben Sie diese Option nie ernsthaft erwogen. Mit einem überschaubaren finanziellen Einsatz „erkaufen" Sie sich ein Stück persönlicher Sicherheit. Sie sorgen für einen Notfall vor und dass das Sinn macht, würde niemand ernsthaft in Frage stellen.

Vogel-Strauß-Politik

Im unternehmerischen und behördlichen Bereich sieht es seltsamerweise anders aus. Hier scheint eine Vogel-Strauß-Politik vorzuherrschen. Man handelt nach dem Prinzip: „Wenn ich nur die Augen vor möglichen Risiken fest genug schließe, werden sie auch nicht eintreten."

Klassische Krisenfälle

Keine Sorge, der Sicherheits-Berater wird jetzt nicht wieder in epischer Breite die klassischen Krisenfälle (Hoechst, Exxon Valdez, Brent Spar, Elch-Test, ADAC usw.) aufzählen, die Sie sicherlich schon zur Genüge kennen. Wir ziehen auch nicht die Geschichte aus der Schublade, nach der x Prozent der Unternehmen, die keinen professionellen Krisenstab hatten, 18 Monate nach dem Ereignis vom Markt verschwunden waren. Diese durch nichts gestützte Aussage geistert seit Ewigkeiten im Krisenmanagementbereich umher, wird aber auch durch zigfaches Wiederholen und Steigerung der Prozentzahl nicht wahrer.

Hoher Schaden

Aber auch wenn Unternehmen, die von einem krisenhaften Ereignis betroffen sind, nicht gleich in die Insolvenz gehen oder vom Wettbewerb geschluckt werden, erleiden sie dennoch oft einen hohen Schaden, sowohl materiell als auch immateriell.

Welchen Beitrag kann ein vorbereitetes Krisenmanagementsystem zum Unternehmenserfolg beitragen?

1. Prävention:

BCM

Die beste Krise ist die, die gar nicht erst eintritt. Im Rahmen des Business Continuity Management (BCM) ist zunächst einmal zu ermitteln, welchen potenzielle Krisen sich das Unternehmen gegenübersieht und wie diese überhaupt entstehen können. Man mag gar nicht glauben, wie wenige Unternehmen eine solche Analyse durchgeführt haben. Sogar große High-Tech-Konzerne verschließen sich davor, mit teilweise gravierenden Folgen. So entstand die „Festplatten-Krise" 2011 nur deswegen, weil 80 Prozent der weltweiten Produktion von Festplatten-Controllern in dem thailändischen Landstrich erfolgt, der seinerzeit überflutet wurde. Eine vorher durchgeführte Analyse hätte ergeben, dass ein erhebliches Risiko darin besteht, sämtliche Zulieferer aus der gleichen Region zu wählen. Das Backup-RZ legt man ja auch nicht direkt neben das Hauptrechenzentrum.

Kommunikationsabteilung

Die Kommunikationsabteilung kann ebenfalls einen erheblichen Beitrag zur Prävention leisten. Entgegen landläufiger Meinungen kommen Krisen nämlich nur selten unerwartet und plötzlich. Viel häufiger sind sie das Ende eines langen und beobachtbaren Prozesses. Im Zeitalter der sozialen Medien kann man auf den einschlägigen Seiten und Apps sehr gut ablesen, wie das eigene Unternehmen in der Öffentlichkeit wahrgenommen wird und vor allem, wie sich dieses Bild entwickelt. Firmen, die schon im Normalbetrieb kritisch beäugt werden oder über die in der Vergangenheit (aus welchem Grund auch immer) negativ berichtet wurde, laufen bei einem an sich harmlosen Ereignis Gefahr, aufgrund dieser Tendenz in eine krisenhafte Situation abzugleiten.

» Die beste Krise ist die, die gar nicht erst eintritt. «

Beobachten der Berichterstattung

Durch das gezielte Beobachten der Berichterstattung können frühzeitig (kommunikative) Maßnahmen ergriffen werden, um das Bild des Unternehmens in der Öffentlichkeit positiver zu gestalten. Sollte dennoch einmal ein krisenhaftes Ereignis eintreten, hat man zumindest schon einmal eine positiv eingestellte Presse, was sehr viel wert ist.

2. Notfallmanagement

Bundesanstalt für Sicherheit in der Informationstechnik

Wichtig ist zunächst, das Notfall- vom Krisenmanagement zu unterscheiden. Nach BSI-Standard 100-4 („Notfallmanagement") ist ein Notfall *„ein Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wieder hergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt […]."*

Deutsche Gesetzliche Unfallversicherung

Ein Notfall ist also im Vergleich zur Krise niedrigschwelliger, erfordert aber dennoch eine gesonderte Notfallbewältigungsorganisation. Die DGUV 1 („Grundsätze der Prävention") fordert in § 22 (1) die Vorbereitung auf solche Fälle: *„Der Unternehmer hat entsprechend § 10 Arbeitsschutzgesetz die Maßnahmen zu planen, zu treffen und zu überwachen, die insbesondere für den Fall des Entstehens von Bränden, von Explosionen, des unkontrollierten Austretens von Stoffen und von sonstigen gefährlichen Störungen des Betriebsablaufs geboten sind."*

Notfallpläne

Die Aufgabe des Notfallmanagements ist die operative Bewältigung des Schadensereignisses (z. B. die unmittelbare Brandbekämpfung oder die Räumung von Gebäuden). Vorbereitete Notfallpläne helfen in den zu erwartenden Stresssituationen, keine wesentlichen Maßnahmen zu übersehen, und helfen so, aus einem Notfall erst gar keine Krise werden zu lassen.

3. Krisenmanagement

Abweichende Situation

Laut dem bereits erwähnten BSI-Standard ist unter einer Krise *„eine vom Normalzustand abweichende Situation verstanden, die trotz vorbeugender Maßnahmen im Unter-*

nehmen bzw. der Behörde jederzeit eintreten und mit der normalen Aufbau- und Ablauforganisation nicht bewältigt werden kann. […].“

IATA

Eine noch prägnantere Definition bietet die IATA (International Air Transport Association): *„Any situation which has the potential to affect long-term confidence in a company, or its products, or which can interfere with its ability to continue operating normally.“*

Reputation

Wichtig ist dabei zu verstehen, dass eine Krise nicht nur durch materielle Schäden entstehen kann. Eine Verletzung der Reputation eines Unternehmens oder einer Behörde kann genauso schwerwiegende Konsequenzen nach sich ziehen. Eine Krise im hier gemeinten Sinn kann aus drei Gründen entstehen:

Krisengründe

- Ereignisse, die einen bestimmten vordefinierten Schwellenwert überschreiten (z. B. angenommene Schadenshöhe, verletzte Mitarbeiter oder längerer Ausfall wichtiger Prozesse)
- Ereignisse, die nicht vordefiniert waren und für die kein Notfallplan existiert
- Ereignisse, für die die Notfallplanung nicht mehr ausreicht

Krisenstab

Im Gegensatz zum Notfallmanagement befasst sich der Krisenstab nicht mit der operativen Bekämpfung des Ereignisses, sondern steuert das Gesamtunternehmen mit dem Ziel, den Geschäftsbetrieb soweit wie möglich aufrecht zu erhalten und das Unternehmen schnell wieder in den Normalzustand zurückzuführen. Er handelt also auf einer strategischen Ebene und sorgt unter anderem dafür, dass dem Notfallmanagement die notwendigen Ressourcen auch über einen längeren Zeitraum zur Verfügung gestellt werden.

» Auf dem Papier brauchbar, in der Praxis schnell undurchführbar. «

Krisenmanager sind sich einig, dass in einer solchen Situation rasch und entschlossen reagiert werden muss. Unternehmen, die nicht vorbereitet sind, sondern einem Ereignis „aus dem Stand“ begegnen wollen, verlieren mit organisatorischen Maßnahmen wertvolle Zeit, die sie nicht mehr aufholen können.

Gemeinsames Überlegen

Weithin verbreitet ist beispielsweise die Idee, dass man sich in einem Krisenfall im Kreis der Geschäftsführung und Fachabteilung zusammenfindet und sich gemeinsam überlegt, wie man die Situation löst. Was auf dem Papier vielleicht noch brauchbar klingt, wird in der Praxis schnell undurchführbar. Weiß der Notfallmanager z. B., wann er wen informieren muss (und wie dessen Nummer lautet)? Dies gilt besonders, wenn das Ereignis nachts oder an Feiertagen eintritt (und Krisen haben die seltsame Tendenz, genau das zu tun).

Automatisiertes Alarmierungssystem

Sollte er tatsächlich die benötigten Informationen haben, wird er erhebliche Zeit am Telefon verbringen, um den Personen zu erklären, was passiert ist und dass sie zum Standort kommen sollen. Diese haben bestimmt Rückfragen und verlängern damit noch das Gespräch. Man geht bei einem nicht automatisierten Alarmierungssystem davon aus, dass pro Anruf mindestens drei bis fünf Minuten vergehen. Zeit, die der Notfallmanager nicht hat, denn er soll ja eigentlich das Ereignis bekämpfen und nicht telefonieren.

Improvisieren

Ist der Personenkreis dann endlich eingetroffen (hoffentlich waren alle zu Hause und sind gleich beim ersten Versuch erreicht worden), geht das Improvisieren weiter. In welchen Raum gehen wir? Haben wir Arbeitsmittel? Wer führt denn Protokoll? Ich kann mich nicht in den PC einloggen, ist denn hier niemand, der sich damit auskennt? Die Liste der Dinge, mit der wichtige Zeit vertrödelt wird, ließe sich endlos fortsetzen.

Fachleute und Assistenzteam

Dagegen der vorbereitete Krisenstab: Der Notfallmanager weiß, wann er den Leiter des Krisenstabs informieren muss. Hält dieser die Einberufung des Stabes für notwendig, gibt er einen Code in das automatische Alarmierungssystem ein. Dieses ruft parallel alle benannten Mitglieder des Krisenstabs an und lässt sich bestätigen, dass sie an den Standort kommen und wie lange sie dafür benötigen. Mit der Meldung haben die angerufenen Personen auch die Information erhalten, welches der beiden vorab vorbereiteten Lagezentren aktiviert wird. Nach einer ersten kurzen Besprechung, in der sich der Kernkrisenstab (vier bis fünf Personen) ein Bild von der Lage gemacht und entschieden hat, dass das Unternehmen in den Krisenmodus wechselt, wird der Stab um Fachleute und das Assistenzteam erweitert. Diese haben regelmäßig geübt und kennen ihre spezifischen Aufgaben.

Unterschied zur Bilanzpressekonferenz

Auch die Kommunikation unterscheidet sich in einem Krisenfall deutlich von der bei einer Bilanzpressekonferenz. Der Pressesprecher und die Geschäftsleitung sollten diesen Sonderfall regelmäßig mit Spezialisten trainieren. Beiden muss bewusst sein, dass ihre Zielgruppe emotionalisiert ist und sie ihnen nicht zuhören wird, wenn nur technische Fakten mitgeteilt werden (wer Näheres dazu wissen möchte, sollte sich einmal das Vier-Seiten-Modell des Kommunikationswissenschaftlers Schulz von Thun ansehen). Ein plastisches Beispiel hierfür ist die Kommunikation im Rahmen der geplanten Versenkung der „Brent Spar“ 1995, einem schwimmenden Öltank, der den Firmen Shell und Esso gehörte. Die Öffentlichkeit sorgte sich um möglicherweise noch vorhandene Giftstoffe und war hoch emotionalisiert (in Deutschland wurden Shell-Tankstellen boykottiert), die Kommunikationsabteilung von Shell beschränkte sich aber auf die Aussage, dass man die Erlaubnis zur Versenkung habe.

Regelmäßiges Üben

Natürlich ist die Implementierung und das regelmäßige Üben eines Krisenstabs mit Kosten verbunden. Diese sind erfahrungsgemäß aber sehr überschaubar, denn im Wesentlichen muss das Unternehmen organisatorische Maßnahmen ergreifen (Benennung der Mitglieder, Erstellung von Handlungsanweisungen etc.).

Wert Ihres Unternehmens

Zugegeben, der Einsatz eines Krisenstabs wird äußerst selten erfolgen (und der Sicherheits-Berater wünscht Ihnen, dass Sie ihn überhaupt nie brauchen werden), aber denken Sie an die eingangs erwähnte Haftpflichtversicherung und ihren Beitrag zu Ihrer persönlichen Sicherheit. Ihr Unternehmen sollte Ihnen genauso viel wert sein.

Kein „Sonderstab“

Zu guter Letzt noch ein Hinweis: Krisenstäbe dürfen auch so heißen. Ereignisse ändern nicht ihre Bedeutung, nur weil die Unternehmens- oder Behördenleitung meint, dass man die Organisation besser „Stab für außergewöhnliche Ereignisse“ oder „Sonderstab“ nennt, um Mitarbeiter oder Bevölkerung nicht zu verschrecken.

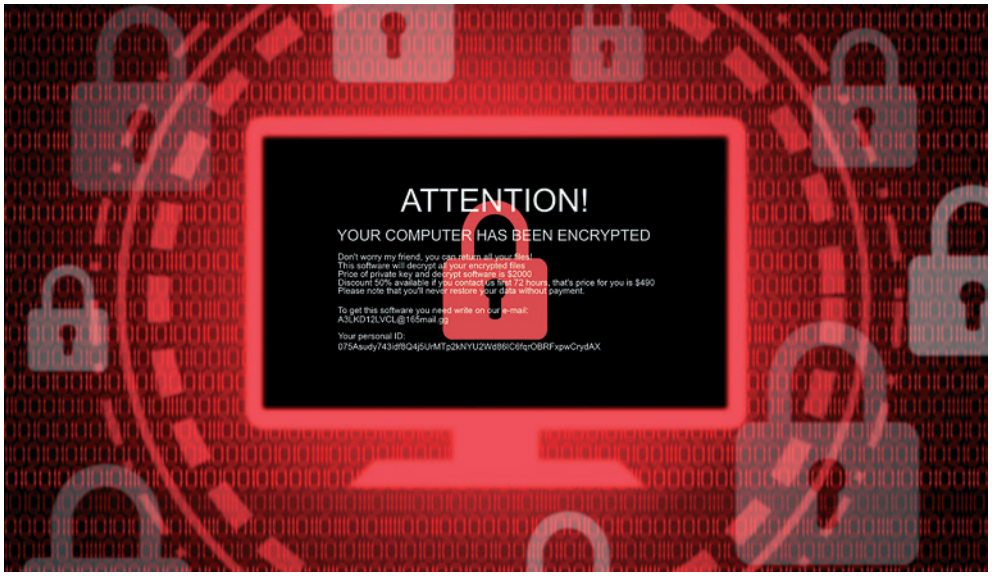
Der Autor Stephan Leukert
Dipl.-Staatswissenschaftler (univ.)

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 2011) mit den Spezialgebieten personelle Sicherheitsdienstleistungen, Sicherheitskonzepte sowie Notfall- und Krisenmanagement

Schwerpunkt Business Resilience

IT-SICHERHEIT

Mit COW an Windows vorbei gegen Ransomware-Angriffe



Gravierende Unterbrechung

Das größte Risiko, eine gravierende und lange dauernde Unterbrechung des Geschäftsbetriebes zu erleiden, besteht darin, Opfer eines Ransomware-Angriffs zu werden, also eines gezielten Angriffs auf die Funktionsfähigkeit der Unternehmens-IT.

Windows-Landschaft

Voraussetzung für einen erfolgreichen Ransomware-Angriff ist im Normalfall die fast überall genutzte Windows-Landschaft. Die Kombination von Windows-Clients und -Servern, den zugehörigen Office-Produkten und der Verwaltung des Ganzen durch das Windows Active Directory bildet ein tödliches Trio. Alle beteiligten Windows-Produkte sind enorm komplex und entsprechend fehlerhaft. Die Folge solcher Komplexität ist, dass Angreifer immer neue Sicherheitslücken finden, die es ermöglichen, einem Benutzer irgendein Stück Software unterzuschieben, das die Angreifer als Einfallstor für ihr weiteres Vorgehen nutzen können.

Schadsoftware auf PCs und Servern

Die Folge eines ersten erfolgreichen Einbruchs ist im Normalfall die durch Windows-Interna gut unterstützte Verbreitung von Schadsoftware auf weiteren PC und vor allem auf Servern des betroffenen Unternehmens. Anschließend folgen gegebenenfalls die Kopie, der Abzug von „interessanten“ Daten und zum Abschluss die Verschlüsselung aller Daten.

Wertlose Datensicherung

Eine schlimme Erfahrung, die viele Unternehmen machen mussten, die einem Ransomware Angriffs ausgesetzt waren, war die Erkenntnis, dass die Datensicherung nichts wert war. Entweder enthält auch die Sicherung durch Ransomware beschädigte Daten, ihre Verwaltung ist ebenso verschlüsselt wie alle anderen Daten oder sie funktioniert ohne das nunmehr unbrauchbare Windows Active Directory nicht.

Windows Registry

Wirklich gut gemachte und wirkungsvolle Ransomware wird nicht etwa nur Office-Dateien und Datenbanken unbrauchbar machen, sondern auch IT-interne Informationen – zuvorderst zum Beispiel die Windows Registry auf allen befallenen Systemen – falls möglich aber auch die Konfiguration von Firewalls, Netzen und als Krönung die des Backups.

Dass an eine Datensicherung heute höhere Anforderungen als in den Vor-Ransomware-Zeiten gestellt wird, ist auch in den Top-10 Ransomware-Maßnahmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgeführt:

BSI-Forderung

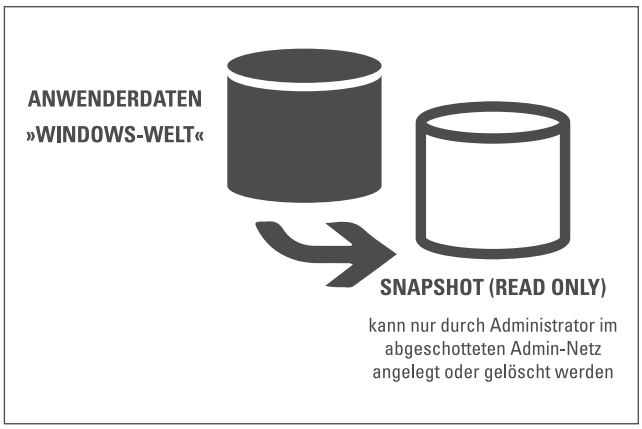
„Daten müssen in einem Offline-Backup gesichert werden. Diese Backups werden nach dem Backupvorgang von den anderen Systemen des Netzwerkes getrennt und sind daher vor Angriffen und Verschlüsselung geschützt.“ (www.bsi.bund.de, Kurzlink https://tinyurl.com/252wp7ar)

Backup-Administrator

Selbst diese Forderung ist aber noch nicht ganz vollständig. Während des Backupvorgangs sind die Daten sehr wohl gefährdet. Ein geschickter Angreifer könnte zum Beispiel die Rolle des Backup-Administrators einnehmen und durch ein kleines Stück „Zusatzsoftware“ die komplexen Datenstrukturen des Backups so beschädigen, dass eine Wiederherstellung von Daten nicht mehr möglich ist.

Außerhalb der Gefahrenzone

Zum Schutz gegen Ransomware wird also ein System benötigt, bei dem Manipulation und die Zerstörung von Daten durch einen feindlichen Anwender nicht möglich ist und das von einem Administrator verwaltet wird, der außerhalb der Gefahrenzone agiert. Der Administratoraccount des Backups muss außer Reichweite eines Angreifers liegen.



Bildquelle: wme/VZM GmbH

Copy-On-Write-System

Grundlage für die benötigte Unverwundbarkeit des Speichers ist ein Copy-On-Write-System (COW). COW-Speichersysteme wie das von NetApp (www.netapp.com) entwickelte „ONTAP“ oder das als Open Source vorliegende „ZFS“ (openzfs.org) überschreiben bei Änderungen nichts auf dem Speichermedium, sondern schreiben Änderungen der Daten stets in einen neuen Datenblock. Zudem werden bei jedem Speichervorgang auch alle internen Verwaltungsinformationen aktualisiert. Vorteil des Copy-On-Write ist, dass der Speicher und damit darauf vorhandene Dateisysteme immer konsistent sind und dass es sehr einfach und billig ist, Kopien – „Snapshots“ genannt – großer Datenmengen bis hin zur Kopie des gesamten Systems anzufertigen.

„Schnappschüsse“ mit minimalem Aufwand

Die unveränderlichen „Schnappschüsse“ von produktiven Verzeichnissen oder ganzen Dateisystemen lassen sich mit minimalem Aufwand und in hoher Frequenz anfertigen. Damit gibt es Datensicherungen, die konstruktionsbedingt nicht überschrieben werden können und die im Falle eines Falles helfen, die durch Ransomware zerstörten Daten aus der garantiert schreibgeschützten Kopie zügig wiederherzustellen. Wohlgemerkt ersetzen Snapshots keine weiteren Datenkopien, denn bei Schäden am Speichermedium oder bei Zerstörung oder Verlust des Geräts ist der Snapshot genauso unbenutzbar wie das Original.

Rigorose Trennung

Eine solche unveränderliche Datenkopie muss dadurch abgesichert werden, dass das Speichersystem in einem Netz betrieben wird, dessen Administration gänzlich und dauerhaft von der Administration der sonstigen IT getrennt ist. Entscheidend ist die rigorose Trennung von der Windows-Welt. Damit soll gewährleistet sein, dass auch bei einem qualifizierten Ransomware-Angriff auf das (Windows-)Netz die Kontrolle des Speichersystems außer Reichweite eines Angreifers bleibt.

„Immutable Backup“

Diese Kombination aus geschützter Administration und nicht manipulierbaren Snapshots stellt dann eine unveränderliche Sicherung, auf neudeutsch ein „Immutable Backup“ dar. Das Immutable Backup erweitert die altbekannte 3-2-1-Regel der Datensicherung. Das 3-2-1 Prinzip verlangt drei Kopien aller relevanten Daten auf zwei verschiedenen Medien, von denen eines räumlich ausgelagert ist. Diese Auslagerung soll die Datensicherung vor Schäden am Gerät und durch Auslagerung auch vor Feuer, Wasser oder Naturkatastrophen schützen.

3-2-1-1-T-Prinzip

Angesichts der Bedrohung durch Ransomware muss das 3-2-1 Prinzip zu 3-2-1-1-T erweitert werden. Die weitere 1 steht dabei für eine unveränderliche Datenkopie (Immutable Backup) und das T für regelmäßige Tests aller Ausfertigungen der Datensicherung. Nur realitätsnahe Tests können Mensch und Material helfen, im Ernstfall eine fehlerfreie Wiederherstellung sicherzustellen.

Erste Schritte

In der Praxis wird es kaum möglich sein, in kurzer Zeit die gesamte Unternehmens-IT auf unveränderliche Backups umzustellen. Erste Schritte sollten aber darin bestehen, die Informationen, die zur schnellen Wiederherstellung einer funktionierenden und vertrauenswürdigen IT-Infrastruktur benötigt werden, auf diese Weise zu sichern. Das sind (ohne Vollständigkeit der Auflistung):

- Die Benutzer- und Rechteverwaltung (Active Directory oder LDAP-Datenbank)
- Die Konfigurationsdaten des eigenen DNS
- Konfigurationsdaten von Switchen und Routern
- Firewall-Regeln und weitere Konfigurationsdaten
- „Goldene Kopien“ von virtuellen Maschinen, Software (Binärdateien) und Firmware
- Konfigurationen und Einstellungen von Infrastrukturkomponenten (z. B. der Admin-PC)
- IT-Notfallpläne und die IT-Dokumentation

» Entscheidend ist die rigorose Trennung von der Windows-Welt. «

Operational Technology

Auch für andere IT-Umgebungen, die im Ernstfall eine schnelle Rekonstruktion benötigen, wie z. B. die „Operational Technology“ (OT) eines Gebäudes, also die IT des technischen Gebäudebetriebs, der Überwachung und der Sicherheitstechnik eines Gebäudes oder einer Liegenschaft, liegt der Einsatz eines Immutable Backup nahe.

Vertrauenswürdiges Backup

Sowohl bei der IT-Basis als auch bei der OT geht es weniger um enorme Datenmengen, als um eine Vielzahl von Konfigurationsinformationen, deren Vollständigkeit und Konsistenz benötigt wird, um einen IT-Basisbetrieb oder die wichtigsten Funktionen der Gebäudetechnik und der Gebäudesicherheit wiederherzustellen. Ein solches vertrauenswürdiges Backup „vor Ort“ ermöglicht, schnell eine Basis zu schaffen, auf der zumindest ein Notbetrieb wieder möglich ist und das Unternehmen oder das Gebäude nicht völlig „am Boden liegen“.

Der Autor Werner Metterhausen
Diplom-Informatiker

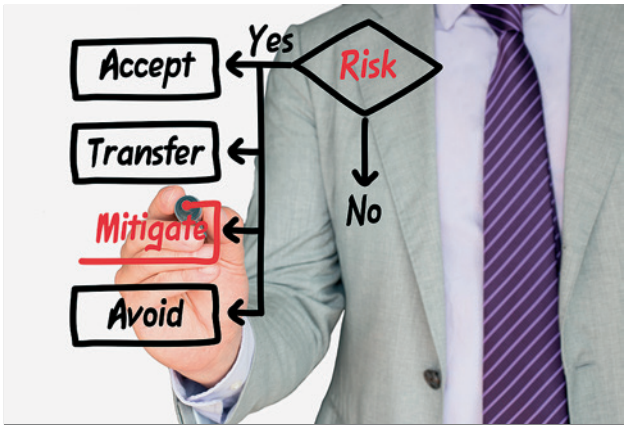
Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 1997) mit den Spezialgebieten RZ-Zertifizierung, Datenschutz, Informationssicherheit (ISO 27001 Lead-Auditor)

Schwerpunkt Business Resilience

SICHERHEITSKONZEPT

Gefährdungsanalyse – Risiken erkennen und gezielt mitigieren

Risikobehaftete Veränderungen



Veränderungen im Unternehmen können risikobehaftet sein, beispielsweise die Wahl der neuen Standortfläche im Rahmen der Expansion. Die Einschätzung möglicher Gefährdungen am potenziellen Standort erfolgt meist im Rahmen einer Gefährdungsanalyse. Betrachtet werden vielfältige Szenarien, wie Einflüsse durch Elementarkräfte (Wind, Feuer, Wasser), risikobehaftete Nachbarbetriebe, Großereignisse wie auch die Verfügbarkeit und Ausfallsicherheit von Medien, wie Stromversorgung, Datenkonnektivität etc. Aber auch interne Prozesse, die im Unternehmen selbst begründet sind, können risikobehaftet sein, beispielsweise bei Fehlentscheidungen des Managements, durch den Weggang von Schlüsselpersonen oder produktionsbedingt durch Produktmängel, oder bei Ausfall von Personal und Maschinen ...

Abschätzen und berechnen

Etabliert hat sich für den ganzen Prozess – bestehend aus Risikoidentifikation, -analyse und -evaluation – der Begriff Gefährdungsanalyse oder auch Risikoanalyse. Zur Gefährdungseinschätzung und -bewertung benötigt man klar definierte Szenarien mit daraus resultierenden Auswirkungen, um das mögliche Schadenpotenzial einschätzen zu können. Dieses ergibt sich aus dem Produkt von Eintrittswahrscheinlichkeit und Auswirkung und weist im Ergebnis den Handlungsbedarf auf.

Handlungsbedarf

Bei der Maßnahmenplanung ist zu entscheiden, wie mit Risiken, die Handlungsbedarf erfordern, umgegangen werden soll. Eine generelle Empfehlung für Unternehmen kann nicht geben werden, da viele individuelle Aspekte betrachtet werden müssen. Insbesondere hängt die Risikobehandlungsstrategie stark vom Risikoappetit des jeweiligen Unternehmens ab.

„Risk Mitigation“

„Risk Mitigation“ bedeutet Risikominderung. Als Strategie, um Gefahren abzuwehren, bieten sich dem Unternehmen verschiedene Ansätze:

Handlungsoptionen

a) die Risiken zu akzeptieren

b) Risiken zu reduzieren und kontrollieren

c) auf Risiken nicht einzugehen und sie vermeiden

d) andere für Risiken verantwortlich zu machen

Parametereinschätzung

Für welche der vorstehenden Optionen (auch Kombinationen sind möglich) sich das Unternehmen letztlich entscheidet, wird auch beeinflusst durch die Einschätzung folgender Parameter:

- die Häufigkeit des Eintretens
- das Schadenausmaß im Falle des Geschehnisses
- direkte Auswirkung auf die im Szenario beschriebene Situation
- indirekte Auswirkung

Priorisieren

Die Erledigung aller risikobehafteten Szenarien anzustreben ist löblich – mit Priorität sollten jedoch zunächst die Punkte in den Fokus genommen werden, für die ein (sehr) hoher Handlungsbedarf ermittelt wurde, um einen möglichen Ausfall des Unternehmens auszuschließen.

Option Risikoakzeptanz

Bewusst übernehmen

Leicht fällt die Entscheidung, wenn die Risikoanalyse für ein Szenario sowohl eine niedrige Eintrittswahrscheinlichkeit als auch eine geringe Auswirkung bzw. einen geringen Schaden zeigt. Das Risiko ist in einem solchen Fall akzeptabel und kann zu einem späteren Zeitpunkt beseitigt werden.

Option Risikoreduktion

Gezielt minimieren

Als zweite Option besteht die Möglichkeit, das Risiko zu minimieren oder es zu modifizieren. Wenn das Unternehmen das Risiko einschätzen kann und die kritischen Prozesse kennt, können mögliche Fehler abgestellt und Einflussfaktoren so verändert werden, dass mit ergänzenden Sicherheitsmaßnahmen die Gefahr gesenkt bzw. ihr entgegengewirkt wird. Beispielhaft kann dies durch den Aufbau von Redundanzen geschehen, durch Schulungsmaßnahmen und Wissensverteilung beim Personal etc. Möglicherweise hilft auch eine qualitative oder quantitative Einschränkung im Prozess und trägt so zur Risikoreduktion bei.

»Die Risikobehandlung hängt stark vom Risikoappetit des Unternehmens ab.«

Option Risikovermeidung

Risiken meiden

Nimmt man das eingangs genannte Szenario „Standortsuche zum Zweck der Unternehmensexpansion“ und es stellt sich heraus, dass die gewünschte Fläche in einem Gebiet mit Hochwassergefährdung und seismischer Aktivität liegt oder im Untergrund Altlasten vorhanden sind, ist es eine Risikovermeidung, wenn dieser Standort nicht weiter betrachtet wird. Auch interne Umstrukturierungsmaßnahmen können dazu beitragen, Risikoursachen auszuschließen.

Option Risikotransfer

An Dritte übertragen

Der Risikotransfer bietet sich an, wenn das Unternehmen sich beispielsweise auf bestimmte eigene Kernkompetenzen konzentrieren möchte und risikobehaftete Prozesse an Dritte transferiert. Das kann z. B. das Auslagern der IT an einen RZ-Collocation-Betreiber sein, weil Know-how oder IT-Mitarbeiter fehlen. Bei möglichen Schäden rein finanzieller Art bietet sich der Abschluss einer entsprechenden Versicherung an. Denkbar ist die Übertragung des Risikos auf Partnerunternehmen, wenn sie aus technischen oder wirtschaftlichen Gründen besser in der Lage sind, mit dem Risiko umzugehen.

Chancen nutzen

Das Ergebnis des Risikoscorings der Gefährdungsanalyse ist nicht durchweg als negativ zu sehen, sondern der sich ergebende Handlungsbedarf kann auch als Chance betrachtet werden. Gegebenenfalls werden durch eine Prozessänderung oder -neudefinition Ressourcen frei, die anderswo genutzt werden können.

::: Cornelia Last :::

Schwerpunkt Business Resilience

PRAXIS

Wasserschutzkonzept: Paradebeispiel für Resilienzbemühungen

Mindestanforderung

Lange Zeit blieb das Thema Wasserfluten gleichbedeutend mit Hochwasser, wurde also schnell Anrainern von Flüssen und Meer zugewiesen. Nicht nur Rheinanlieger wissen ein Lied davon zu singen, dass in den letzten Jahren gehäuft Hochwasserereignisse mit ungewöhnlich hohen Pegeln auftraten. Als Bezugs- oder auch Gefahrengröße wurde und wird ein theoretischer statistischer Wert herangezogen, nämlich das 100- bzw. 200-jährige Hochwasser. Solch statistische Werte sind zum Teil fehlerbelastet, weil vor 200 Jahren die Messgenauigkeit fehlte, können aber als Mindestanforderung herangezogen werden, ab wann und wie weit man sich Gedanken machen muss.

Steigende Pegelstände

Steigende Pegelstände treten aber auch an Flussläufen auf, denen die Statistik bislang keine Aufmerksamkeit zuwandte – und hier sprechen wir nicht nur von Ahr und Oder. Wer im Sommerurlaub breite Flussbecken überquert, in denen das Rinnsal an Bach kaum auszumachen ist, muss nur im Frühjahr zur Schneeschmelze wiederkommen. In den Bergen gilt schon lange jedes Unwetter als große Gefahr wegen auftretender Wassermassen und abrutschender Hänge.

Starkregenereignisse

Starkregenereignisse treten vermehrt auf und überfordern Kanalisation und Regenrinnen, weil beide auf Normalmaß, also die üblichen Umstände in Deutschland, dimensioniert wurden. Der Deutsche Wetterdienst bietet mit CatRaRE (Catalogue of Radar-based Rainfall Events) eine Übersicht der Starkregenereignisse seit 2001. Auf der Webseite kann man über ein Dashboard, das uns allen spätestens seit den täglichen Covid-Inzidenzmeldungen ein Begriff ist, die Ereignisse regional zugeordnet betrachten. Folgender Kurzlink führt zum Ergebnis von NRW: https://tinyurl.com/mura7eze (auf https://Wetterdienst.maps.arcgis.com). Immerhin 20 Prozent der Top 100 Niederschlagsmengen waren der Kategorie „extremer Starkregen“ zuzuordnen.

Interview mit dem CRO Amsterdams

In Heft 21/2019 führte der Sicherheits-Berater ein Interview mit dem CRO (Chief Resilience Officer) Rotterdams, Jean Molenar, dessen Aufgabe in „nichts anderem“ besteht als bei der Stadtplanung dahingehend einzugreifen, dass neue Wohnungen und Unternehmensbauten dort errichtet werden, wo auch in 100 Jahren noch nicht das Meer Einzug gehalten hat.


21
2019
403 BERUFSBILD
sicherheits.berater
BERUFSBILD
R wie Resilience: Was macht ein CRO?
Der CRO von Rotterdam
Haben Sie schon einmal einen CRO kennengelernt – einen Chief Resilience Officer? Wahrscheinlich gibt's in Deutschland noch gar keinen. Arnoud Molenaar dagegen kennt mindestens 99, die diesen Titel tragen. Er ist selbst CRO – und zwar der von Rotterdam, der zweitgrößten Stadt in den Niederlanden. Dort arbeitet er im Urban Development Department. Ausgerechnet am 20. September, dem Global Climate Strike For Future, fragten wir ihn, wie man das wird und welche Aufgaben die Position mit sich bringt:
Molenaar war im Prinzip bereits CRO, bevor er es offiziell wurde. Im Jahr 2014 schrieb die Rockefeller Foundation einen weltweiten Wettbewerb 100RC aus (www.100resilientcities.org). Sie suchte 100 resiliente Städte, die bereit sind, einen CRO einzustellen und versprach, deren Salär zu übernehmen.

Auszug aus Heft 21/2019

Regelmäßige Risikoanalyse

Ähnlich vorausschauend kann und muss ein Wasserschutzkonzept sein. Es muss Erfahrungswerte aufnehmen, vorbeugende Maßnahmen beinhalten, Reaktionspotenzial aufzeigen und ständig auf Aktualität überprüft werden. Im Rahmen einer Risikoanalyse, die mindestens jährlich fortgeschrieben wird, müssen Schäden aus auftretenden Wassermassen und Maßnahmen zur Mitigation dieser Risiken regelmäßig erfasst werden. Dabei sind Hochwasser, Starkregenereignisse, aber auch Wasserschäden aus Defekten oder gar Sabotageakten gleichermaßen zu thematisieren.

Maßnahmen

Standortwahl

1. Maßnahmen zum Schutz vor Hochwasser und Starkregen fangen bei der Standortwahl an, so man denn noch die Wahl hat. Dazu ein paar Parameter:
   a. kein Standort in der Nähe von offenen Gewässern (Seen, Flüsse, Bäche, Küste)
   b. Vermeidung von ausgewiesenen Überflutungsgebieten
   c. keine Hanglage
   d. kein Grundstück, dessen Grasnarbe knapp über dem Grundwasserspiegel liegt
   e. kein Standort in der Nähe bzw. im Einflussbereich von Bauwerken der Wasserwirtschaft (Talsperren, Wasserbehälter etc.)

Baulich-technische Maßnahmen

2. Lässt sich ein solcher Standort nicht vermeiden, so sollten baulich-technische Maßnahmen bereits in der Bauphase realisiert werden. Bei Baumaßnahmen in Hochwassereinzugsgebieten ist daher zunächst ein Richtwert zu definieren, der für alle folgenden Hochwasserschutzmaßnahmen einzuhalten ist, beispielsweise der Hochwasserwert 200.

Weiße Wanne

3. Standard für solche Bauten ist heute die sogenannte weiße Wanne, bei der der Beton mit Zuschlagstoffen wasserfest(er) gemacht wird. Ergeben Bodenproben im Umfeld des Baukörpers einen erhöhten Sulfatgehalt, müssen spezielle Zemente, die kalkarm sind, eingesetzt werden. Außerdem muss der Beton möglichst dicht sein. Das Problem bei Sulfatgehalt im Erdreich ist die auftretende treibende Wirkung. Es bildet sich Ettringit, wodurch der Beton von innen zerstört werden kann.

Schutzmaßnahmen für Gebäudeöffnungen

4. Überall dort, wo Öffnungen in ein Gebäude die Wanne durchbrechen, müssen ausreichende Schutzmaßnahmen vorgenommen werden. Kellerabgänge, Lichtschächte u. ä. sind mit druckwasserdichten Schotten oder Türen abzudichten. Besser noch ist es, das Wasser erst gar nicht in Schächte oder Kellerabgänge hineinzulassen, indem diese Öffnungen überdacht werden und das Wasser gezielt abgeleitet wird.

Mobile Schutzelemente

5. Sollten mobile Schutzmaßnahmen errichtet werden, müssen diese ausreichend fundamentiert werden, damit sie nicht durch die Wucht des Wassers weggespült werden können. Werden mobile Schutzelemente, Sandsäcke oder Sperrbalken, unmittelbar vor Gebäudezugängen platziert, ist darüber nachzudenken, dass hinter diesen Schutzmaßnahmen – also im Eingangsbereich des Gebäudes – Sickerwasser auftreten kann. Dieses muss entsorgt werden können.

Schadenpotenzial

6. In vielen Gemeinden werden zum Schutz vor Hochwasser Schutzwände installiert. Dies legt die Vermutung nahe, dass hinter der Schutzwand unbeschadet weitergelebt werden kann und erst bei Überschwappen des Wassers über die Schutzwand ein Schadenpotenzial auftritt. Dieser Gedanke ist jedoch schlichtweg falsch. Hochwasser von Flüssen führt auch zu einer zeitlich versetzten Erhöhung des Grundwasserpegels, dieser zum Phänomen des so genannten Qualmwassers. Dabei drückt das Wasser aus dem Erdreich, es bildet sich ein Teich ohne erkennbaren Zulauf. Dieser Effekt kann häufig auf Wiesen im Nahbereich von Flüssen ausgemacht werden, vollzieht sich aber in ähnlicher Form auch um Bauwerke herum, die hinter einer Hochwasserschutzmauer im Grundwasser stehen. Auch bei nicht mit einer Bodenplatte gesicherten Innenhöfen muss mit diesem Phänomen gerechnet werden.

> »Der Gedanke, die Schutzwand schütze bis zum Überschwappen des Wassers, ist schlichtweg falsch.«

Gefragte Statiker

7. Hochwasserschutz darf sich nicht allein auf Gebäude konzentrieren, sondern muss auch Bauteile erfassen, die keine ausreichende Masse als Gegengewicht zu den Auftriebskräften von Grundwasser besitzen. Als Beispiel seien hier unterirdisch verlegte Medienkanäle zu nennen. Hier ist der Statiker zum Schutz solcher Bauteile besonders gefragt.

Nachbesserung durch Injektionen

8. Bei weißen Wannen zeigt sich in den ersten Jahren nach Inbetriebnahme, an welchen Stellen noch Undichtigkeiten auftreten, die dann durch Injektionen nachgebessert werden müssen. Doch solche Leckagen treten auch noch Jahre nach Bauabschluss auf. Entsprechend sollten keine hochwertigen technischen Einrichtungen, z. B. ein Rechenzentrum, unmittelbar an die Außenhaut des Gebäudes gelegt werden.

Entdeckung von Undichtigkeiten

9. Um die Entdeckung auftretender Undichtigkeiten zu vereinfachen, ist es hilfreich, die Außenwände weiß zu tünchen, weil einsickerndes Wasser zur Braunfärbung führt. Außerdem sollten Inspektionen durch eine Minimierung von Installationen an den Außenwänden vereinfacht werden.

Resistentes Dichtmaterial

10. Klassische Punkte zum Wassereintrag im Gebäude sind die für die Zuführung von Einspeisungen ins Gebäude erforderlichen Durchbrüche in den zuvor aufgebauten weißen oder schwarzen Wannen. Die Zuführungen müssen penibel abgedichtet werden. Das Dichtmaterial ist auf Resistenz gegen eventuell vorhandene Schadstoffe im Umfeld zu prüfen bzw. seinerseits mit einem Schutzanstrich zu versehen. Die Einführungen sind durch Zugentlastungen oder vergleichbare bauliche Maßnahmen so zu gestalten, dass mechanische Einwirkungen (durch Wasserauftrieb bzw. Absacken von Grund) keine Auswirkungen auf die Dichtung haben können.

Geschlossene Innenhöfe

11. Beliebtes architektonisches Element sind geschlossene Innenhöfe, die ansprechend begrünt den Mitarbeitern in den daran gelegenen Büros einen angenehmen Ausblick verschaffen. An dieser Stelle kommen zwei Gefährdungsmomente zusammen. Zum einen sorgen die eingesetzten Pflanzen mit ihren Wurzeln dafür, dass Dichtungsmaßnahmen zerstört werden können. Wurzelwerk kann Abdichtplanen, aber auch Beton direkt angreifen – entsprechend ist eine geeignete Auswahl der Bepflanzung vorzunehmen.

Wartung der Drainageleitung

12. Bei sintflutartig auftretenden Regenfällen sind Innenhöfe geeignet, zum Schwimmbecken zu mutieren, weil die Drainage des Innenhofes entweder nicht ausreichend dimensioniert wurde oder sich im Laufe der Jahre durch Erdreich, Rindenmulch, aber auch Pflanzenwurzeln zugesetzt hat und damit

einen Teil ihrer Kapazität verloren hat. Hier ist eine regelmäßige Wartung der Drainageleitung, aber auch eine wassersperrende Ausprägung der Umfassungsbauteile erforderlich.

Ab- und Zuluftöffnungen

13. Innenhöfe werden unter Sicherheitsaspekten auch gerne zur Aufstellung von Zuluftöffnungen oder großvolumigen Abluftöffnungen genutzt. Diese müssen selbstredend gegen direktes Eindringen von Niederschlag geschützt werden. Hilfreich ist hier eine Art Deckel oder Haube, die in ausreichendem Abstand montiert werden, um den Luftschluss nicht zu behindern. Zudem ist die Oberkante dieser Bauwerke oberhalb des Erdniveaus im Innenhof möglichst hoch anzusiedeln, um bei volllaufendem „Schwimmbecken" keinen natürlichen Überlauf ins Gebäude hin zu kreieren.

Absaugung des Wassers

14. Sofern Mensch oder Technik das Volllaufen eines Innenhofes erkennen, sollte eine unterstützende Absaugung des auftretenden Wassers vorgenommen werden. Die Führung der Wasserabpumpleitung durch das Gebäude stellt sicherlich eine suboptimale Lösung dar, entsprechend müssen andere Wege gefunden werden. Förderpumpen müssen entsprechend der zu erwartenden Förderhöhe ausgelegt werden. Je nach Lage des Innenhofes innerhalb eines Baukörpers sind sehr große Leitungswege zu berücksichtigen, sodass sich die Vorhaltung von Schläuchen mit entsprechender Länge lohnt.

Pumpensümpfe

15. Wenn wegen der Größe des Gebäudes mehrere Pumpensümpfe eingerichtet werden, schafft man Redundanz der Pumpkapazität durch Verbindung der Sümpfe untereinander unter Ausnutzung des Prinzips der kommunizierenden Röhren.

„Wassermeldekabel“

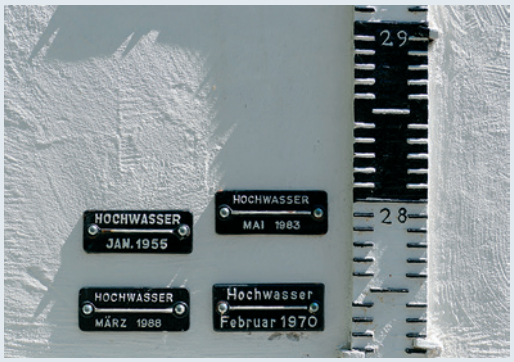
16. Eine Detektion von Wasser muss erfassen, was man nicht verhindern konnte. Es sind, um die Detektionssicherheit optimal auszulegen, möglichst Linienmelder einzusetzen. Die "Wassermeldekabel“ müssen dabei quer zur erwartenden Eindringrichtung des Wassers verlegt werden oder mäandrisch, um eine Flächenüberwachung zu erreichen.

Dachöffnungen

17. Dachöffnungen, aber auch zur Lüftung antriebsgesteuerte Fensteranlagen müssen mit Sensorik ausgestattet werden, die nicht nur Sturm, sondern auch Regen und Hagel erkennen kann. Die Lüftungsöffnungen müssen dann automatisch zugefahren werden.

Definition von Grenzwerten

18. Wasserschutz ist auch auf der organisatorischen Ebene zu treffen. Sofern sich Betriebsgebäude im Hochwassereinzugsbereich befinden, ist zu definieren, bis zu welcher Hochwassermarke ein geordneter Betrieb vollzogen werden kann und ab wann reduzierte Betriebszustände anstehen. Bei der Definition dieser Grenzwerte ist nicht allein die Lage des jeweiligen Betriebsgebäudes zu betrachten, sondern auch die Erreichbarkeit des Betriebsgebäudes für die Mitarbeiter mit öffentlichen Verkehrsmitteln und über Straßen. Wenn das Betriebsgebäude



sich innerhalb des Hochwassereinzugsbereiches am höchsten Punkt befindet, aber sämtliche Straßen sozusagen bereits abgesoffen sind, kann nicht erwartet werden, dass alle Mitarbeiter mit Booten zum Betriebsgebäude geschafft werden.

19. Organisatorische Gegenmaßnahmen müssen unverzüglich anlaufen. Ein Alarmplan muss präzise zu jedem erfassten Risiko Maßnahmen vorgeben, die der Ereignisbekämpfung und Schadenminderung dienen. Dazu gehören z. B. neben dem Aufbau von Wassersperren auch deren regelmäßige Kontrollen sowie Überprüfung der Situation vor Ort, um sofort schadenminimierend eingreifen zu können. Denn wenn mobile Schutzelemente, Sandsäcke oder Sperrbalken aufgebaut werden, ist es nicht auszuschließen, dass hinter diesen Schutzmaßnahmen Sickerwasser auftreten kann. Dieses muss entsorgt werden können.

Alarmplan

» Organisatorische Gegenmaßnahmen müssen unverzüglich anlaufen. «

20. Für eine Frühwarnung ist es hilfreich, Erfahrungswerte aus Hochwasserständen höhergelegener (stromaufwärts) Messstationen zu Rate zu ziehen, um die Kritikalität eines auf ein Unternehmen zukommenden Hochwassers beurteilen zu können.

Frühwarnung

21. Hilfreich bei der Bewertung der Hochwassergefährdung sind auch die jeweils zuständigen städtischen Behörden, die beispielsweise mit Hochwasserkarten die Situation der jeweiligen Hochwasserstände darzustellen in der Lage sind. Oft ist dies Entscheidungshilfe bei der Bewertung, ab welchem Zeitpunkt der Betrieb in einem Gebäude eingestellt geschlossen werden muss, weil beispielsweise keine öffentliche Zuwegung mehr gegeben ist.

Entscheidungshilfe

22. Zumindest eine kleine technische Mannschaft sollte auch im Falle eines Hochwassers das Gebäude noch so lange wie möglich weiter betreiben. Für diese Technikcrew, die möglicherweise über einige Zeit durch Wasser eingeschlossen arbeiten muss, sind ausreichend Räumlichkeiten für den Aufenthalt (Ruhe und Schlafmöglichkeiten), Verpflegung, Kommunikationsmittel etc. vorzuhalten.

Technische Mannschaft

23. Wohl dem, der einen Ausweichstandort hat. Die Forderungen des Bundesamtes zur Sicherheit in der Informationstechnik, BSI, zur Georedundanz von kritischer Infrastruktur kommen nicht von ungefähr. Besser als irgendwelche starren Kilometerangaben zur Distanz zwischen zwei Standorten ist die Vorgabe bei der Standortselektion, dass ein Ereignis nicht beide Standorte gleichermaßen schädigen können darf. Ein Produktionsstandort in Koblenz, der zweite in Köln, beide in Rheinnähe erfüllen nicht den mit der Forderung angestrebten Effekt.

Ausweichstandort

Fazit

Allein dieses Beispiel Wasserschutzkonzept mit seinen zahlreichen Maßnahmenoptionen zeigt, wie vielschichtig und anspruchsvoll die Aufgabe eines Resilienzmanagements sein kann.

Resilienzmanagement

::: Peter Stürmann :::

Schwerpunkt Business Resilience

FORSCHUNG

Resilienz-Reifegrad – gut vorbereitet für den Ernstfall(?)

Folgenminimierung

Hat eine Organisation eine hohe Widerstandsfähigkeit – hinlänglich als Resilienz bezeichnet – so können die Folgen eines kritischen Ereignisses (Cyberangriffe, Naturkatastrophe, Feuer/Explosionen etc.) minimiert werden: Sowohl die unmittelbaren Auswirkungen wie Betriebsunterbrechungen oder Datenverluste als auch die mittelbaren Folgen wie Reputationsverlust werden geringer sein – und deshalb betreiben Organisationen durchaus einigen Aufwand. Soweit die Theorie …

Wissenschaftliche Studie

Doch wie sieht es in der Praxis aus? Zahlt sich die Investition in Präventionsmaßnahmen tatsächlich aus? Sind Unternehmen, die sich gut auf den Ernstfall vorbereitet fühlen, tatsächlich im Stande, in kurzer Zeit Krisen deutlich besser zu bewältigen als dies mit moderater Vorbereitung gelänge? Was sind bewährte Praktiken für Resilienz, und inwieweit trägt das digitale Potenzial zum Erreichen organisationaler Resilienz bei? Das war die zentrale Fragestellung der Untersuchung, die im Rahmen einer breit angelegten Studie wissenschaftlich betrachtet wurde: Unter Leitung von Prof. Dr. Stefan Vieweg (Dr. Vieweg Consulting und Institut für Compliance & Corporate Governance der Rheinischen Fachhochschule Köln) wurde nicht nur der derzeitige Resilienzgrad der Studienteilnehmer ermittelt (an der Umfrage unter leitenden Angestellten mit Entscheidungsbefugnissen nahmen über 200 Personen teil), sondern ebenso ein Resilienz-Reifegradmodell (RRM) entwickelt, mit dem der eigene Status schnell bestimmt und daraus Verbesserungsansätze abgeleitet werden können.

Resilienz-Reifegradmodell

Das RRM ist ganzheitlich und betrachtet sowohl die strategische Vision als auch die operative Umsetzungskompetenz.

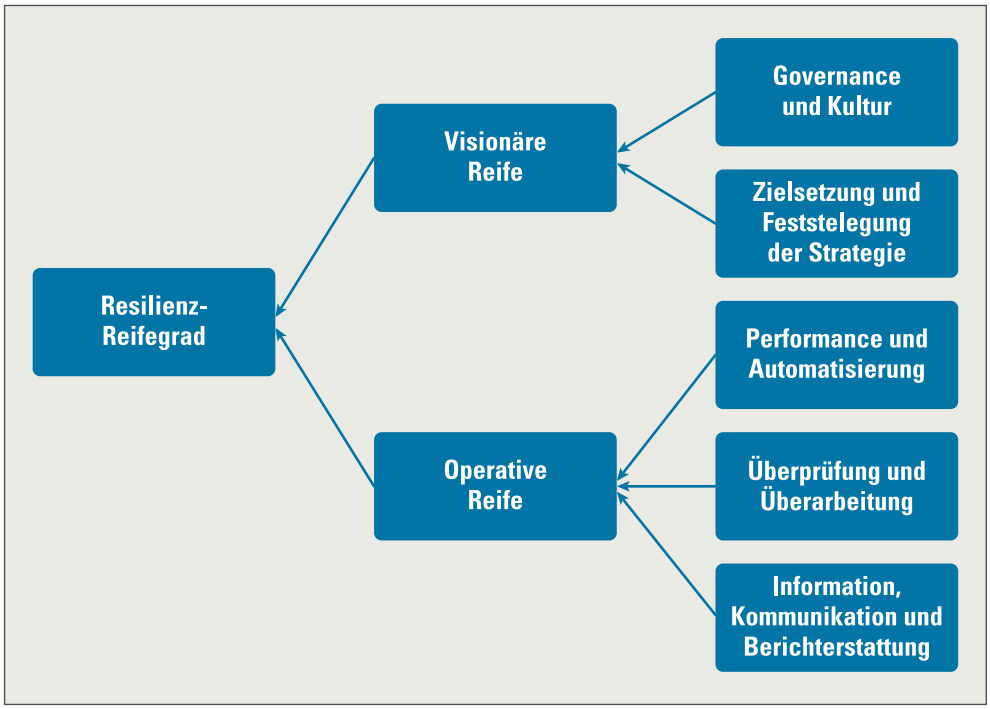


Abbildung 1: Prinzip des Resilienz-Reifegradmodells (RMM)

Bildquelle: Prof. Vieweg

Umfrageergebnisse

Die Umfrage ergab, dass kritische Ereignisse erhebliche negative monetäre Auswirkungen haben, dass trotz einer zumindest mäßigen Vorbereitung nicht viel Schaden abgewendet werden kann und dass die Wiederherstellung Monate dauert und wiederum die Opportunitätskosten erhöht:

Negative Auswirkungen

Top 3 kritische Ereignisse	Negative finanzielle Auswirkungen	Grad der Bereitschaft	Höhe des abgewendeten Schadens	Zeit bis zur Wiederherstellung
1. Pandemie (Covid-19) *2. Cybervorfälle* *3. Marktentwicklungen*	**51 %** *des Gegenwerts des Jahresumsatzes*	**45 %** *fühlten sich zumindest „mäßig vorbereitet"*	**25 %** *des abgewendeten Schadens (gewichteter Durchschnitt)*	**67 %** *brauchten „Monate" oder "Wochen" (anstatt „Tage" oder „Stunden"), um sich zu erholen*

Abbildung 2: Wichtigste Ergebnisse der Umfrage
Bildquelle: Prof. Vieweg

Zur genaueren Analyse wurden Best Practices (Top Performer) gegenüber anderen Teilnehmern abgegrenzt. In acht Bereichen können die Erkenntnisse der Studie zusammengefasst werden:

Best Practices

1. Die Widerstandsfähigkeit hat erhebliche Auswirkungen auf das Endergebnis:
   Top-Performer erleiden einen Verlust von umgerechnet 7 Prozent des Jahresumsatzes, fast 20-mal weniger als Nachzügler (145 Prozent des Jahresumsatzes).

   Verlust Jahresumsatz

2. Geld steht nicht im Vordergrund für die Widerstandsfähigkeit:
   Die Top-Performer gaben weniger für Investitionen in die Resilienz aus, was Unternehmen aus dem dritten Quartil entsprach.

   Weniger Investitionen

3. Reden scheint einfacher zu sein als zu handeln:
   Visionäre Reife ist einfacher als operative Reife, die letztlich für Performance sorgt.

   Visionäre Reife

4. Es gibt einen Grund für die Widerstandsfähigkeit von Top-Performern:
   Bei den Top-Performern übertrifft der Reifegrad der Widerstandsfähigkeit in Bezug auf Vision und Ausführung alle anderen.

   Top-Performer

5. Ein Übermaß an Ausgaben hilft nicht wesentlich weiter:
   Zwischen dem Reifegrad der Resilienz (d. h. ihrer Umsetzung) und der Finanzierung der Resilienz besteht eine klare Nichtlinearität.

   Nichtlinearität

6. Der Sweet Spot der Resilienz-Investitionen:
   Der optimale finanzielle Aufwand liegt bei 10 bis 25 Prozent des Umsatzes und erlaubt eine Schadensvermeidung von etwa 30 Prozent; kleinere Unternehmen (<50 k FTE) schneiden etwas besser ab.

   Optimaler Aufwand

7. Digitalisierung und Automatisierung sind wichtig:
   Je höher der Grad der Digitalisierung, desto höher die wahrgenommene Bereitschaft (obwohl die wahrgenommene Bereitschaft kein guter Indikator für die Resilienzleistung ist).

   Digitalisierungsgrad

8. KI-basierte Modelle helfen, Verbesserungsbereiche zu erkennen:
   Bereits vergleichsweise einfache überwachte Algorithmen bieten eine angemessene Vorhersagekraft, um Verbesserungen der Widerstandsfähigkeit umzusetzen.

   Einfache Algorithmen

QR-Code führt zur App RMM Check

Interessenten können sich gerne einen ersten Überblick über den eigenen Resilienzgrad verschaffen, indem sie elf Fragen in der App RMM Check der Dr. Vieweg Consulting („sustainable transformations in the digital age“) beantworten und auch einen Vergleich zu Industrie-Benchmarks erhalten. Die Dr. Vieweg Consulting bietet u. a. Beratung, Coaching und Trainings in den Bereichen, Resilienz, Cybersicherheit, agiles Management und Nachhaltigkeitsmanagement: https://drvieweg.net.

Beispiel für die Resultateanzeige der App

Der Gastautor Prof. Dr. Stefan Vieweg, CFA

Gründer der Dr. Vieweg Consulting, Direktor des Instituts für Compliance & Corporate Governance der Rheinischen Fachhochschule Köln und dort u. a. Leiter des LL.M. – Studiengangs Compliance & Corporate Security.

Fragen an unseren Gastautor? info@drvieweg.net

Schwerpunkt Business Resilience

SICHERHEITSPLANUNG

Lassen Sie sich durch Drohungen nicht verunsichern!

Destabilisierung

In diesen herbstlichen Tagen fällt mit Blick auf die Nachrichten in Deutschland auf, dass vermehrt Drohungen „auflaufen“: Informationen über verdächtigte Personen und Sprengstoff in Zügen, gleichzeitige Drohmails an Schulen in mehreren Bundesländern, Drohungen gegenüber einem Fernsehsender sowie auch Bedrohungen gegen regionale Unternehmen. Als Außenstehender hat man das Gefühl, zusätzlich zu den sichtbaren Aktionen auf Straßen und an und in Gebäuden wird gezielt versucht, die allgemeine Situation zu destabilisieren. Hendrik Zörner benennt auf der Webplattform des Deutschen Journalistenverbands einige konkrete Fälle anonymer Bombendrohungen und kommentiert: „Wer auch immer die Täter sind, sie wollen das öffentliche Leben in Deutschland stören, der Infrastruktur schaden. Und vor allem wollen sie Angst schüren.“ (www.djv.de, Kurzlink https://tinyurl.com/mm8anmwt)

Einige Aspekte

Es ist aber festzustellen, dass die zuständigen Polizeistellen zusammen mit den übergeordneten Behörden eine sehr gute Arbeit leisten, um präventiv, aktuell und gezielt jede einzelne Straftat aufzuarbeiten. Unabhängig davon benötigen aber diese hoheitlichen Kräfte Unterstützung in den Unternehmen und öffentlichen Einrichtungen. Nachfolgend einige Aspekte, welche man möglicherweise im eigenen Haus überprüfen sollte:

1. Das Thema „Umgang mit Bedrohungen“, sei es durch Anrufe, Mails oder durch einen persönlichen Angriff, wurde in den letzten Jahren oft vernachlässigt. Gibt es bei Ihnen die entsprechenden Prozessabläufe zur Aufnahme und Abarbeitung solcher Vorkommnisse? Sind die entsprechenden Formulare vorhanden? Sind die Mitarbeiter auf solche Situationen durch Einweisungen, Schulungen und Training vorbereitet?

Vorbereitung

2. Funktionieren die Aktionen nach einem solchen Bedrohungsereignis? Was nützen Ihnen Meldeketten, wenn die zuständigen und verantwortlichen Personen im Urlaub oder krank sind und es keine bzw. unzulänglich eingewiesene Vertreter gibt?

Funktionieren

3. Führen Sie regelmäßig Evakuierungsübungen durch? Nutzen Sie durchaus die Spielräume von unterschiedlichen Eintrittsszenarien. Eine Gebäuderäumung nach Brandalarm dürfte nichts anderes sein als eine Räumung nach Bombendrohung! Bei einer spontane Amoklage sieht es dann schon anders aus. Und stellen Sie dabei auch Überlegungen an, dass durch eine solche „chaotische Situation“ bei bewusster Sabotage (vorsätzliche Auslösung Ereignis) das Eindringen von Tätern möglich sein kann. Müssen ggf. taktische Anpassungen in und außerhalb von Betriebszeiten, bei der Wahl von Betriebsmitteln und Personalressourcen vorgenommen werden?

Evakuierungsübungen

» Sicherheitsmanagement ist heute eine verantwortungsvolle Tätigkeit. «

Auswertung

4. Werten Sie Ereignisse und Vorfälle ebenso wie vorgenannte Übungen aus. Lassen Sie die Erkenntnisse, um die Mitarbeiter, ggf. auch zeitweise Nutzer von Gebäuden (in öffentlichen Einrichtungen), in Unterweisungen einfließen. Informieren Sie transparent. Ein sich der Sicherheitsmaßnahmen bewusster Mitarbeiter wird situationsunabhängig im Sinne des Allgemeinwohls und seiner eigenen Situation handeln. Das Thema Sicherheit ist gerade in der jetzigen Zeit ein wichtiges Thema, das nicht einem Selbstzweck dient, sondern das Ziel hat, jede einzelne Person bestmöglich zu schützen.

Ausbildung

5. Dies bedeutet im Umkehrschluss aber auch, dass die verantwortlichen Mitarbeiter in der Unternehmenssicherheit entsprechend ausgebildet sind und Wertschätzung im Haus erfahren. Wie oft hört man auch noch heute: „Dort können wir die Mitarbeiter beschäftigen, die ihre ursprünglichen Tätigkeiten aus körperlichen bzw. seelischen Gründen nicht mehr ausüben können." Oder „Bedienen wir uns Dienstleistern, die uns preiswert zu den Themen beraten und unterstützen können." Die Umsetzung eines unternehmensspezifischen Sicherheitsmanagements mit all seinen Facetten ist heute eine verantwortungsvolle Tätigkeit, die ein hochwertiges und breites Fachwissen voraussetzt. Und aus praktischer Sicht die Resilienz des Unternehmens sicherstellt.

Netzwerken

6. Und eine Anmerkung zum Schluss: Nutzen Sie Ihr Netzwerk bzw. lassen Sie sich vernetzen. Im Oktober 2023 fand in Hamburg das 3. Netzwerktreffen SIMEDIA Akademie für Site-Security-Verantwortliche statt, das eine bisher einzigartige Resonanz erhielt. Das nächste Treffen ist bereits für den 25. und 26.06.2024 in Wolfsburg geplant. Ich kann Ihnen diese Veranstaltung aus Überzeugung nur empfehlen: www.simedia.de, Kurzlink https://tinyurl.com/2fmdjnbe

Der Autor Rochus Zalud
Diplom-Ingenieur konstruktiver Ingenieurbau (TH)

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 1991) mit den Spezialgebieten Sicherheitskonzepte/-planungen, Rechenzentrums- und Leitstellenplanung, bauliche Sicherheit, Türenplanung und Zutrittsorganiation

Nachrichten

4. SIMEDIA-Netzwerktreffen zur Standortsicherheit. Bereits zum vierten Mal treffen sich am 25. und 26. Juni 2024 erneut Sicherheitsverantwortliche aus Wirtschaft und Verwaltung zum gemeinsamen Erfahrungs- und Wissensaustausch beim Netzwerktreffen „Site Security" der SIMEDIA Akademie in Wolfsburg. Auch in diesem Jahr hält das Programm für die Teilnehmer einen hochaktuellen, informativen und praxisorientierten Mix aus Fachvorträgen und Erfahrungsberichten zu unterschiedlichsten Themen der Standort- und Objektsicherheit bereit. Neben dem Vortrags- und Rahmenprogramm bleibt wie gewohnt zudem viel Zeit zu persönlichem Austausch unter Kollegen und intensiver Netzwerkpflege. www.netzwerktreffen-sitesecurity.de.

Zertifiziertes Wissen zur Sicherheitstechnik. Ab dem 30. Januar 2024 startet die insgesamt neuntägige Zertifikatslehrgangsreihe zum „Security Engineer, BdSI" der SIMEDIA Akademie neu. In fünf Lehrgangsmodulen wird Grundlagen- und Planungswissen zu den Themen Perimeterschutz, Gefahrenmelde- und Videotechnik, Zutrittskontrolle, Brandschutz, Türenplanung, Leitstellentechnik vermittelt. Der dreitägige Abschlusslehrgang führt die einzelnen Gewerke zu einem funktionierenden Gesamtsicherheitskonzept zusammen. Ein zusätzliches Hochschulzertifikat der Hochschule Furtwangen kann sich daran anschließen. Wegen des starken Zuspruchs in diesem Jahr wird dieser Lehrgang sehr wahrscheinlich in der zweiten Jahreshälfte 2024 nochmalig angeboten. securityengineer.simedia.de.

Schmutzwasser in Katastrophengebieten umweltschonend säubern. Die Deutsche Bundesstiftung Umwelt DBU berichtet, dass sie ein Projekt des Startups Disaster Relief Systems (DRS) und der Universität Leipzig fördert. Darin geht es um die Entwicklung einer Anlage, die aus Schmutzwasser bis zu 2.500 Liter sauberes Trinkwasser pro Stunde herstellt. Sie soll bei Naturkatastrophen, Krieg oder Epidemien ohne Chemikalien funktionieren, regenerativ angetrieben werden können und recyclebar sein. Die Anlage kann in Katastrophengebieten notfalls auch unbeschadet aus einem Flugzeug abgeworfen werden. Die DBU bzw. der Projektleiter betonen die Umweltfreundlichkeit der Anlage. Bisher seien solche Rohwasseraufbereitungsanlagen oft ökologisch problematisch, weil dabei z. B. Chemikalien zur Flockung von Schwebstoffen eingesetzt würden. www.dbu.de, Kurzlink https://www.dbu.de/news/wie-schmutzwasser-trinkbar-wird/

DEB rät zu Neubewertung der Sicherheitslage bei Großevents. In einer (nicht im Internet veröffentlichten) Pressemitteilung an die Redaktionen rät der Deutsche Expertenrat Besuchersicherheit DEB aufgrund der jüngsten Terroranschläge der Hamas auf den Staat und die Bewohner von Israel sowie die andauernden Gewaltkundgebungen mit Ausschreitungen und Drohungen von Hamas- und Palästinenser-Anhängern zu erhöhter Wachsamkeit und intensiven Sicherheitsmaßnahmen bei Großevents. Die Sicherheit zur Durchführung solcher Veranstaltungen sei demnach vorurteilsfrei neu zu prüfen und die Sicherheitslage entsprechend zu bewerten. www.expertenrat-besuchersicherheit.de

BfDI kritisiert Nachrichtendienstgesetze. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Professor Ulrich Kelber, sieht bei den Neuerungen der Gesetze der Nachrichtendienste noch datenschutzrechtliche Mängel. In einer Pressemitteilung schreibt er, der Bundesnachrichtendienst solle (laut neuem Gesetz) Informationen zur politischen Unterrichtung der Bundesregierung auch nachgeordnete Behörden des Bundes und Behörden der Länder übermitteln dürfen. Nach den Vorgaben des Bundesverfassungsgerichts sei dies, so Kelber, jedoch nur im Fall einer unmittelbar bevorstehenden Gefahr für ein überragendes Rechtsgut erlaubt. Trotz einiger Verbesserungen im Gesetzesentwurf sehe er Unsicherheiten und Lücken. www.bfki.bund.de, Kurzlink https://tinyurl.com/mrvswj3t

Antisemitische Vorfälle melden. Der Bundesverband RIAS (Recherche- und Informationsstellen Antisemitismus) e. V. dokumentiert als Dachverband zivilgesellschaftlicher Meldestellen für antisemitische Vorfälle ebensolche mit Bezug zu den Terrorangriffen auf Israel zwischen dem 7. und 15. Oktober 2023. Im Vergleich zum entsprechenden Vorjahreszeitraum hätten diese Vorfälle um 240 Prozent zugenommen. Der RIAS fordert Zeugen antisemitischer Vorfälle auf, diese unter www.report-antisemitism.de zu melden. Die 22-sei-

Impressum

49. Jahrgang

Herausgeber
Rainer von zur Mühlen
Peter Stürmann

TeMedia Verlags GmbH
Ein Unternehmen der VZM-Gruppe
Alte Heerstraße 1, 53121 Bonn
Telefon: 0228 96293-80
Telefax: 0228 96293-90

Redaktion
redaktion@sicherheits-berater.de
www.sicherheits-berater.de
direkt.sicherheits-berater.de
Bernd Zimmermann
(Chefredaktion, V.i.S.d.P.)
Telefon: 0228 96293-81
chefredaktion@sicherheits-berater.de

Jörg Schulz, Peter Schmidt,
Rochus Zalud

Media-Beratung
Alice M.W. Hoffmann
Telefon: 0228 96293-21
anzeigen@sicherheitsberater.de

Leserservice
info@sicherheits-berater.de
Telefon: 0228 96293-80

Erscheinungsweise
Zweimal monatlich

Preise
Einzelheft: 17,50 € plus Versand
Jahresabo: 294,00 € inkl. Porto
Semesterabo: 25,00 € inkl. Porto
Auslandsabo: 280,00 € zzgl. MWSt. gem. UStG und Versand
Luftpostgebühren auf Anfrage

Abonnementskündigungen sind mit einer Frist von vier Wochen zum Ende des berechneten Bezugszeitraumes möglich.

Im Falle höherer Gewalt (Streik oder Aussperrungen) besteht kein Belieferungs- oder Entschädigungsanspruch. Nachdruck, auch auszugsweise, nur mit Genehmigung des Verlages.

Druck: Unitedprint.com Vertriebsgesellschaft mbH, 01445 Radebeul

Bildquellen:
S. 445, 446 ©fotomaster,
S. 447 ©Robert Kneschke,
S. 450 ©fotomek, S. 453 ©MrJeans,
S. 455 ©Warakorn, S. 458 ©andyller,
S. 459 ©structuresxx, S. 462 ©beebright,
S. 464 ©Gina Sanders, S. 468 ©SiRo,
S. 474 ©kebox
– alle stock.adobe.com

ISSN 0344-8746

NACHRICHTEN

tige Dokumentation ist ebenfalls auf der genannten Webseite zu finden (Kurzlink https://tinyurl.com/2sap66mv)

Habeck sieht digitale Technologien als „Sicherheitskriterium". In einem knapp fünfzehnminütigen Interview, geführt von Bitkom-Präsident Dr. Ralf Wintergerst, äußert sich Bundeswirtschaftsminister Robert Habeck zum Wert der Digitalisierung. So möchte er die Künstliche Intelligenz als nächste Stufe der Digitalisierung möglichst stark machen. Digitale Technologien spielten laut Habeck „eine gigantische Rolle" beim Klimaschutz – selbst dann, wenn sie in den Rechenzentren für steigenden Energieverbrauch sorgten. Diese Energie wolle man aber als Wärme den Kommunen zur Verfügung stellen. Mit digitalen Techniken könne die Effizienz der Verbräuche deutlich gesteigert werden. Vom Smarthome bis zu Beleuchtungssystemen, zur Netzsteuerung und zur Verkehrsführung nütze uns die Digitalisierung und erst recht eine AI in der Digitalisierung. Laut Schätzungen, so Habeck, könnten die Energieverbräuche – privat durch Smart Meter und staatlich über digital geführtes Monitoring – bis zu 30 Prozent gesenkt werden. Habeck plädiert für Investitionen in die Chipindustrie in Deutschland, weil sie ein Ökosystem schafften, das hochattraktiv für weitere Unternehmen sei, die sich ebenfalls ansiedeln wollten. Habeck bezeichnet das als „Honigtopf, zu dem die Bienen kommen." Die derzeitige Abhängigkeit von asiatischen Märkten sieht Habeck als Problem, eine gewisse Grundkompetenz bei der Digitalisierung dagegen als „Sicherheitskriterium" oder „Wirtschaftsrobustheit". Diese sollte uns durchaus etwas kosten. Zudem fordert Habeck mehr Mut zum unternehmerischen Risiko. Bis 2024 möchte er eine „vernünftige KI-Verordnung hinbekommen", „im Venture Capital eine richtige Welle auslösen", „ Datenverfügbarkeit steigern" und zugleich das „Dateninstitut richtig operationabel" machen. Das Interview ist in dem Podcast „Wintergerst trifft … " auf der Webseite des Branchenverbandes Bitkom zu hören. www.bitkom.org, Kurzlink https://tinyurl.com/ynfu4swr

Propagandaschrift von Osama Bin Laden findet neue Fans. Einem Bericht der WELT-Redaktion (und anderen Zeitungen) zufolge entwickelt sich eine Propagandaschrift des tausendfachen Massenmörders Osama Bin Laden aus dem Jahre 2002 zum TikTok-Hit. Darin rechtfertige Bin Laden die Anschläge auf die USA vom 11. September 2001. Seine terroristische und antisemitische Argumentation findet offenbar bei vielen jungen Lesern aus den USA Anklang. Diskussionen werden auf TikTok unter dem Hashtag #lettertoamerica erstaunlich oft im Sinne Bin Ladens geführt. TikTok hat damit begonnen, solche Beiträge zu löschen. www.welt.de, Kurzlink https://tinyurl.com/y7txfepn

Chefs als Albtraum für Security-Teams. In einem Beitrag von www.computerwoche.de (Kurzlink https://tinyurl.com/3ktuzncv) heißt es auf Basis eines „Executive Security Spotlight Report von Ivanti", Führungskräfte könnten „für die Security-Teams ein wahrer Albtraum sein". Denn Chefs seien häufig mit umfangreichen Zugangsrechten ausgestattet. Und sei dies nicht der Fall, würden sie Sicherheitsvorgaben einfach umgehen. In der genannten Studie sollen dafür zahlreiche Belege zu finden sein.

Köln zufrieden mit privaten Sicherheitsdienstleistern. Laut Kölner Stadt-Anzeiger zeigt sich die Stadt Köln zufrieden mit der Zusammenarbeit mit privaten Sicherheitsdiensten am 11.11.2023. Bis auf zwei Fälle seien auf Grund intensiver Überprüfungen der Sicherheitsdienste keine Probleme mit dem Sicherheitspersonal entstanden. In einem Fall habe ein Mitarbeiter offenbar angeboten, Menschen gegen eine Geldzahlung Zugang zum Feierareal gewährt zu haben. Die insgesamt 750 Personen sollen bei 67 Sicherheitsunternehmen angestellt gewesen sein. Das Subunternehmer-System sei auf drei Ebenen beschränkt gewesen. www.ksta.de, Kurzlink https://tinyurl.com/2dtn34ja

Verkehrssicherheit und Sicherheitsempfinden erforscht. Die Unfallforschung der Versicherer (UDV) im Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat eine Studie zur „Verkehrssicherheit in Deutschland 2023" veröffentlicht und mit den Ergebnissen von Vorgängerstudien aus den Jahre 2010 bis 2019 verglichen. Dazu wurden über 2.000 Personen ab 18 Jahren online befragt. Demnach fühlen sich Männer (64 Prozent) grundsätzlich deutlich sicherer als Frauen (49 Prozent). Die Studie enthält unter anderem Fragen zur wahrgenommenen Verkehrssicherheit, zur Verkehrssicherheit als politisches Thema, zu befürworteten Verbesserungsmaßnahmen, zu gefährlichem Verkehrsverhalten und zum regelkonformen Verhalten von Autofahrern (auch von Fahrrad- und Pedelec-Fahrern). www.udv.de, Kurzlink https://tinyurl.com/y8z6rxcm