KÖTTER SICHERHEITSBRIEF

Exklusive Informationen für Entscheider

Ausgabe 02 | 2026

Risiko Cybercrime: 360-Grad-Resilienz stärkt Unternehmen und Kritische Infrastrukturen

Cybercrime ist global das größte strategische Risiko für Wirtschaft und Kritische Infrastrukturen (KRITIS). Dabei stehen die hiesigen Akteure besonders unter Druck. Weltweit belegt Deutschland Rang vier unter den am stärksten von Internetkriminalität betroffenen Nationen. Gleichzeitig heizt die kriminelle Nutzung von Künstlicher Intelligenz (KI) die Bedrohungslage weiter ganz massiv an: Allein 86 % der Phishingangriffe sind neuesten Studien zufolge mittlerweile KI-gesteuert.

Künstliche Intelligenz fungiert somit als Cybercrime-Beschleuniger, indem sie Kriminellen insbesondere ermöglicht, Angriffe schneller, gezielter sowie massenhaft zu skalieren – und so de facto jedes Unternehmen und jeden KRITIS-Betreiber ins Visier nehmen zu können.

Das dramatische Ausmaß dieser Entwicklung verdeutlichen wiederholte Unternehmens-Insolvenzen infolge erfolgreicher Cyberattacken genauso wie der jüngste „Cyber-GAU“ beim Land Berlin inklusive Erpressungsversuch und anschließender Veröffentlichung erheblicher Mengen an sensiblen Daten im Darknet.

„Angesichts dieser Bedrohungslage muss für Unternehmen und KRITIS-Betreiber klar sein: Cyberresilienz ist ein elementarer Baustein für die eigene Daseinsvorsorge“, sagt Dirk H. Bürhaus, u. a. Geschäftsführer von KÖTTER Cyber Security. „Um mit den Angreifern Schritt zu halten, bedarf es 360-Grad-Schutz plus einem schlagkräftigen Business Continuity Management, das bei einer erfolgreichen Attacke die eigene Handlungsfähigkeit sichert.“

Dies unterstreicht auch KÖTTER Sicherheitsbeirats-Mitglied Prof. Dr. Harald Olschok: „Ganzheitliche Resilienz zielt vor allem darauf ab, dass Firmen und KRITIS-Betreiber auch im Krisenfall den Betrieb aufrechterhalten können. Denn wer Sicherheit immer noch als reine Gefahrenabwehr definiert oder in Insellösungen denkt, gefährdet seine eigene Zukunft oder sogar die Versorgungssicherheit.“

„Wir brauchen Handlungsfähigkeit statt Versicherungsmentalität“

Unternehmens-Insolvenzen und abgesagte Operationen in Kliniken nach Cybervorfällen sowie zuletzt die Attacke auf das Land Berlin inklusive Datenabfluss ins Darknet: Wie massiv ist die Risikolage durch Cybercrime für Firmen und Kritische Infrastrukturen?
Dirk H. Bürhaus: Riesig. Cybercrime ist Risiko Nummer 1 für jedes Unternehmen und jede Kritische Infrastruktur! Das unterstreichen folgende Zahlen: Das Schadensvolumen nimmt stetig zu und beläuft sich gemäß Branchenverband Bitkom aktuell auf bis zu 205 Milliarden Euro. Das sind mehr als drei Viertel aller Schäden durch Wirtschaftskriminalität. Ein signifikanter Anteil trifft KRITIS-Betreiber wie Kliniken, Energieversorger oder Nahrungsmittelproduzenten. Wer bei dieser Zahl noch wegschaut, agiert fahrlässig.

Warum nimmt die Situation so massiv zu?
Prof. Dr. Harald Olschok: Es gibt mehrere Ursachen. Erstens schaffen unsere hochgradig vernetzten Industrie- und Dienstleistungsgesellschaften immer mehr digitale Angriffsziele. Zweitens hat sich Cybercrime, speziell im Bereich der Organisierten Kriminalität, längst professionalisiert. Drittens verschärfen geopolitische Spannungen die Lage. Nicht befreundete Staaten nehmen hiesige Firmen, gerade auch aus der Defence-Industrie, und Kritische Infrastrukturen immer massiver ins Visier.

Das heißt, KI fungiert als Brandbeschleuniger für Internetkriminalität …
Bürhaus: Genau. KI verändert die Spielregeln. Sie senkt die Einstiegshürden und ermöglicht Angriffskampagnen mit einer bislang nicht gekannten Schlagkraft. Entscheidend ist dabei die Skalierbarkeit: Angriffe können schneller vorbereitet, automatisiert und in großer Zahl durchgeführt werden. Damit wird Cybercrime auch für Tätergruppen attraktiv, die früher nicht über entsprechende technische Ressourcen verfügt haben. Das ist aber längst nicht alles. Mit KI-Hilfe sammeln und analysieren Kriminelle z. B. auch immer mehr Informationen über ihre Opfer – das betrifft längst nicht mehr allein Unternehmer oder VIPs, sondern zunehmend auch einzelne Mitarbeiter. Auf dieser Basis entstehen hochgradig personalisierte Angriffe. Sozusagen über den Einzelnen zum großen Ganzen.

Können Wirtschaft und KRITIS-Betreiber mit dieser kriminellen Energie Schritt halten?
Olschok: Sie müssen. Denn die Folgen eines erfolgreichen Angriffs können Firmen in die Insolvenz treiben und bei Kritischen Infrastrukturen noch weitreichender die gesamtgesellschaftliche Versorgungssicherheit gefährden. Deshalb brauchen wir deutlich stärkere Allianzen zwischen Unternehmen, Politik und Sicherheitswirtschaft. Die Initiative Wirtschaftsschutz ist hier ein wichtiger Ansatz. Gleichzeitig können spezialisierte Dienstleister insbesondere mittelständische Betriebe unterstützen, die nicht über die Ressourcen großer Konzerne verfügen. Das zentrale Stichwort lautet 360-Grad-Sicherheit. Anders ausgedrückt: Unternehmen und KRITIS-Betreiber müssen aufhören, Sicherheit in einzelnen Silos zu denken.

Prof. Dr. Harald Olschok, Mitglied des KÖTTER Sicherheitsbeirates und früherer Hauptgeschäftsführer des Bundesverbandes der Sicherheitswirtschaft.

> **„Der Staat muss Vorbild bei Cyber Security sein und Kooperationen ausbauen.“**
> Prof. Dr. Harald Olschok

Wie funktioniert ganzheitlicher Schutz konkret?
Bürhaus: Eine 360-Grad-Lösung muss ganz individuell zum Unternehmen beziehungsweise zur Kritischen Infrastruktur passen. Am Anfang steht dabei immer eine assetbasierte Risikoanalyse. Sie definiert die relevanten Gefahren, darauf aufbauend lassen sich vorhandene Schutzmaßnahmen optimieren sowie neue physische, technische und IT-basierte Maßnahmen integrieren. Ein Security Operations Center, kurz SOC, bildet einen wesentlichen Baustein für den digitalen Schutz: Es ermöglicht die kontinuierliche Überwachung und Bewertung sicherheitsrelevanter Ereignisse sowie eine schnelle Reaktion – idealerweise rund um die Uhr.

In welcher Weise kann KI dabei die Verteidigung stärken?
Bürhaus: KI bietet auf der Verteidigungsseite enorme Vorteile. Sie kann große Mengen an Sicherheitsdaten korrelieren und analysieren, Lagebilder zusammenführen und dadurch ein wesentlich umfassenderes Gesamtbild erzeugen. Ebenso ist sie in der Lage, Anomalien in Prozessen und Netzwerken zu erkennen und damit Auffälligkeiten sichtbar zu machen, die Menschen allein nur schwer oder zu spät erkennen würden. Diese Möglichkeiten sollten Unternehmen und KRITIS-Betreiber noch intensiver nutzen.

Olschok: Und zugleich immer den Faktor Mensch mitnehmen. Denn Technologie allein schafft keine Sicherheit. Mitarbeiter müssen für Cybercrime und Social Engineering sensibilisiert sowie regelmäßig geschult werden.

Ergänzende Infos zu ganzheitlicher Cyber Security finden Sie hier:

Und der Blick auf die Politik. Was müsste diese noch mehr tun?
Olschok: Der Staat muss Vorbild bei der Cyberabwehr sein – von Gemeinden, Städten und Kreisen über die Länder bis zum Bund. Der Angriff auf die Berliner Senatsverwaltung und die Veröffentlichung einer Riesenzahl sensibler Daten im Darknet haben die bestehenden Defizite mehr als deutlich gemacht. Wir brauchen also noch mehr Investitionen in den Schutz öffentlicher Institutionen plus effektive Strukturen für die Zusammenarbeit im Krisenfall. Das gilt zwischen den staatlichen Ebenen unter Überwindung der „Kleinstaaterei" ebenso wie gegenüber Wirtschaft und Sicherheitswirtschaft. Zudem benötigt Letztere mehr politische Anerkennung als Teil der nationalen Sicherheits-, Cyber-Security- und Resilienzarchitektur.

Trotzdem nachgefasst: Wie stark kann 360-Grad-Schutz in einer Zeit sein, in der ein angegriffener Zulieferer genauso gefährlich ist wie eine Schwachstelle im eigenen Rechenzentrum?
Bürhaus: Genau das ist das Thema. Deshalb darf 360-Grad-Sicherheit nicht bei der eigenen IT oder am eigenen Betriebsgelände enden. Integrativer Schutz bedeutet, Cyber Security mit organisatorischer, physischer und technischer Sicherheit zu verbinden. Denn Cyberattacken können analoge Angriffe begünstigen – und umgekehrt können physische Vorfälle digitale Systeme gefährden. Zusätzlich gehört die Lieferkette einbezogen. Ein Unternehmen kann die eigene IT hervorragend schützen und trotzdem über einen kompromittierten Zulieferer angegriffen werden.

Es braucht folglich zusätzlich umfassende Resilienz-Lösungen?
Bürhaus: Unbedingt. Denn angesichts der beschriebenen Gesamtsituation hat sich beim Thema Cyber Security auch die zentrale Fragestellung entscheidend verändert. Es geht nicht mehr allein oder primär darum, ob ein Unternehmen oder KRITIS-Betreiber angegriffen wird. Im Fokus steht vielmehr: Wann passiert es, wird der Angriff rechtzeitig erkannt und wie lange kann das Unternehmen bei einem erfolgreichen Angriff handlungsfähig bleiben?

Olschok: Professionelle Sicherheit ist heute also viel mehr als originäre Gefahrenabwehr. Es geht darum, sich widerstandsfähig aufzustellen, dafür die notwendigen Ressourcen vorzuhalten und so auch in turbulenten Zeiten die überlebenswichtigen Geschäftsprozesse weiterführen zu können. Hier besteht in Deutschland noch erheblicher Nachholbedarf. Eine Studie zeigt, dass zwar 98 % der Unternehmen Resilienz als Priorität ansehen, allerdings nur 52 % sie aktiv umsetzen. Die Diskrepanz zwischen Anspruch und Wirklichkeit ist also erheblich. Resilienz braucht aber Verantwortung und muss strategisch als Chefsache verankert sein.

„KI ändert die Optionen – auf der Angriffsseite ebenso wie bei der Verteidigung."
Dirk H. Bürhaus

Das heißt in voller Konsequenz: Resilienz und damit die Sicherung der eigenen Handlungsfähigkeit müssen zum eigentlichen Maßstab werden?
Bürhaus: Exakt. Wir brauchen Handlungsfähigkeit statt Sicherheitsillusionen und Versicherungsmentalität. Hundertprozentigen Schutz gibt es nicht – erst recht nicht angesichts einer durch KI beschleunigten regelrechten Cybercrime-Industrie. Allein entscheidend ist deshalb nicht, jeden Angriff verhindern zu können. Noch viel wichtiger ist inzwischen, vorbereitet zu sein und den Betrieb auch unter Krisenbedingungen aufrechterhalten zu können. Resilienz und Business Continuity Management sind damit längst Kernfaktoren für jedes Unternehmen und jeden KRITIS-Betreiber.

Dirk H. Bürhaus, Geschäftsführender Direktor in der KÖTTER Security Gruppe und unter anderem Geschäftsführer von KÖTTER Cyber Security.

Was ist Ihre größte Zukunftssorge: dass Cyberangriffe immer ausgefeilter werden oder dass unsere digitale Abhängigkeit schneller wächst als die Fähigkeit, Folgen von Ausfällen zu managen?
Olschok: Beides. Die zunehmende technische und durch KI forcierte Raffinesse der Angriffe ist problematisch. Gleichzeitig wächst unsere Abhängigkeit von digitalen und KI-basierten Systemen rasant. Wenn diese Abhängigkeit schneller zunimmt als unsere Fähigkeit, Ausfälle und Angriffe zu bewältigen, entsteht eine gefährliche Lücke. Hinzu kommt die teilweise noch immer fehlende Sicherheitssensibilität vieler Akteure. Deshalb ist neben massiven Investitionen in die IT-Sicherheit der beschriebene BCM-Ausbau eben von so großer Relevanz – nicht nur in Unternehmen, sondern gerade auch beim Staat. Am Ende geht es um eine einfache Frage: Können wir auch dann noch handeln, wenn unsere digitalen Systeme einmal nicht funktionieren? Darauf müssen wir vorbereitet sein.

Das Interview führte Carsten Gronwald, Pressesprecher der KÖTTER GmbH & Co. KG Verwaltungsdienstleistungen.

Ergänzende Infos zum integrierten KRITIS-Schutz finden Sie hier:

Hybride Bedrohungen frühzeitig erkennen und integrativ managen

KI-forcierte Internetkriminalität

- Massenhafte Phishing- oder Ransomware-Attacken mittels gefälschter E-Mails etc. oder per Schadsoftware. Ziel: Preisgabe von u. a. Passwörtern bzw. Verschlüsselung von Systemen und anschließende Erpressung.
- Daten- bzw. Identitätsdiebstahl: Datenklau z. B. für Produktpiraterie oder zur kriminellen Verwendung fremder personenbezogener Daten.
- Deepfakes: täuschend echte Audio-/Videoaufnahmen von Personen, um sich z. B. als vermeintlicher Kunde auszugeben.
- Die kriminelle Nutzung von Künstlicher Intelligenz (KI) forciert diese Delikte massiv.

Kombination mit hybriden Gefahren

- Gestohlene Zugangsdaten oder kompromittierte Kameras etc. ermöglichen umgekehrt z. B. Zutritt zu Geländen und unterstützen Sabotage u. Ä.
- Einbrüche als Basis für spätere digitale Angriffe, etwa durch physische Manipulation von Rechenzentren oder Platzieren manipulierter Sticks zur unachtsamen Mitarbeiternutzung.

Integrierte Resilienzkonzepte

- Strategische Maßnahmen: u. a. Risikoanalysen und Business Continuity Management zur Implementierung von Sicherheitsrichtlinien sowie Maßnahmen bei Sicherheitsvorfällen.
- Cyber Security: z. B. SOC-Monitoring (kontinuierliche Überwachung der IT-Infrastruktur durch Security Operations Center) plus 24/7-Ad-hoc-Reaktionsfähigkeit (Cyber Defense as a Service, CDaaS).
- Personelle/technische Sicherheit: u. a. Werkschutz, Zutrittskontrollsysteme, Videotechnik.

Ergänzende Infos zu 360-Grad-Resilienz:

KÖTTER Services

IMPRESSUM

© KÖTTER Sicherheitsbrief wird herausgegeben von der Presse- und Öffentlichkeitsarbeit der KÖTTER GmbH & Co. KG Verwaltungsdienstleistungen, Essen.
Redaktion: Carsten Gronwald, Tel.: +49 201 2788-126, E-Mail: presse@koetter.de.

Die Zeitschrift und alle ihre für die externe Veröffentlichung bestimmten Beiträge sind urheberrechtlich geschützt. Das Copyright kann jedoch jederzeit bei der Redaktion eingeholt werden und wird in der Regel erteilt, wenn die Quelle ausdrücklich genannt und ein Belegexemplar zugestellt wird.

Fotos: S. 1, Titelmotiv Cybercrime: © Veayo – stock.adobe.com; S. 1, Titelmotiv Piktogramme: © magnific.com; S. 2, Herr Prof. Dr. Olschok: © KÖTTER Services/Sven Lorenz; S. 3, Herr Dirk H. Bürhaus: © KÖTTER Services/Sven Lorenz; S. 4, Hybride Bedrohung: © Pixim Stock – stock.adobe.com, S. 4, Monitorabbildungen: © magnific.com.

Sie lesen lieber digital?
Nutzen Sie unser E-Paper

koetter.de/newsletter

Ihr Kontakt zur KÖTTER Unternehmensgruppe:

Wilhelm-Beckmann-Straße 7
45307 Essen

Hotline: +49 201 2788-388
Telefax: +49 201 2788-488

E-Mail: info@koetter.de
Internet: koetter.de