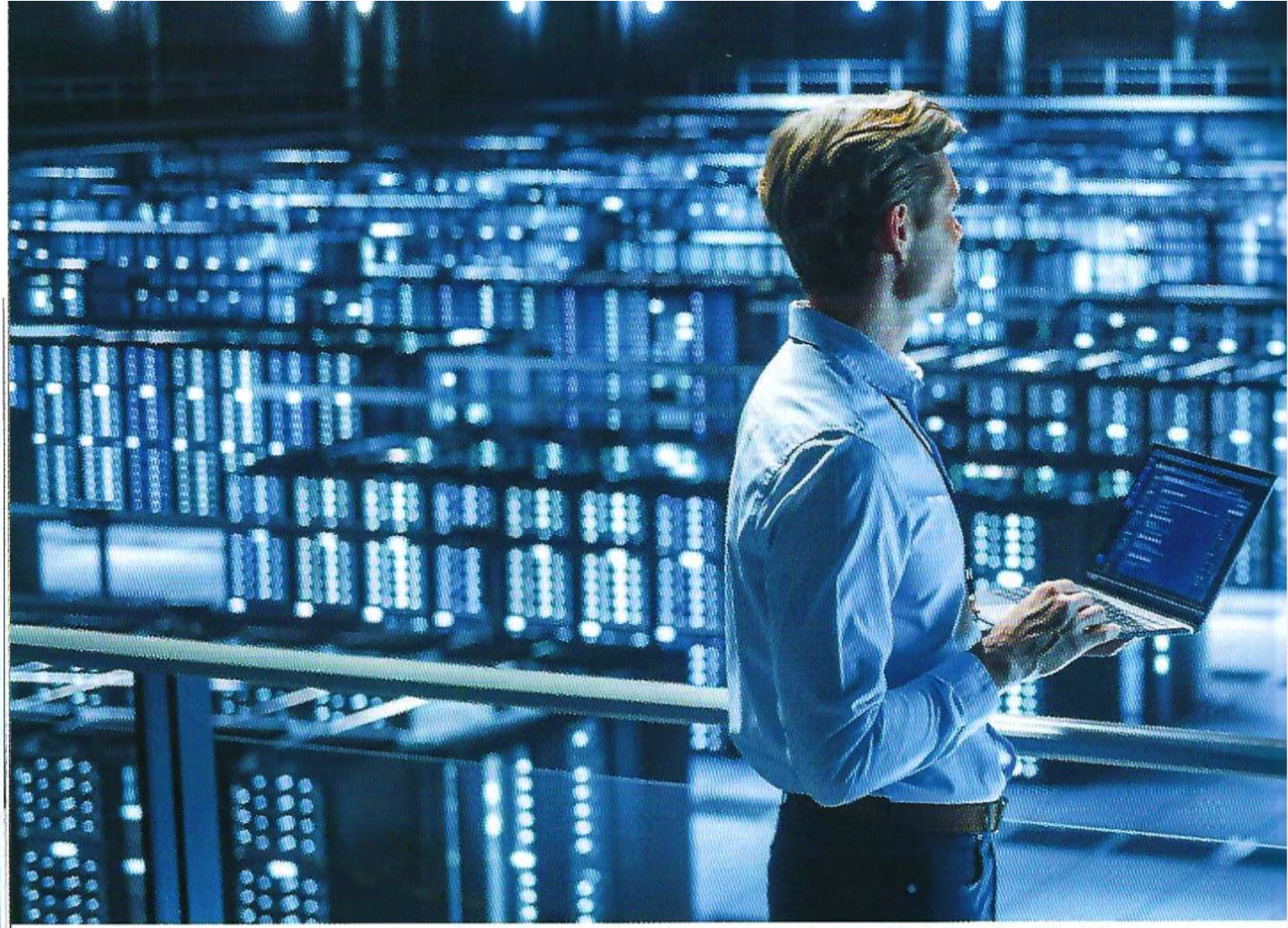


Der Schutz von Rechenzentren und Firmendaten muss zur Chefaufgabe werden, sagen Experten. Häufig ist es das noch nicht.

Unsichtbar, aber real – die **Angreifer** aus dem Netz

Cyberkriminalität Die meisten Betriebe kennen Attacken aus dem Internet. Gut gerüstet sind jedoch die wenigsten. Dabei kann es schnell um das Überleben der Firma gehen.

Es sind besorgniserregende Zahlen, die der Digitalverband Bitkom erhoben und im Sommer veröffentlicht hat: Durch Cyber-Diebstahl, -Spionage und -Sabotage ist der deutschen Wirtschaft innerhalb der letzten zwölf Monate ein Gesamtschaden von 223 Milliarden Euro entstanden. Das bedeutet eine Verdoppelung innerhalb der letzten zwei Jahre.

Fast alle Unternehmen waren laut der Bitkom-Auswertung bereits von Angriffen aus dem Internet betroffen – so wie kürzlich das Bauunternehmen Leonhard Weiss mit Stammsitz in Göppingen. Oder in Freiburg – dort konnte der Versandunternehmer Waschbär drei Monate nicht richtig arbeiten, weil Daten verschlüsselt wurden und deren Freigabe erpresst wurde. Lieferungen waren nur noch teilweise möglich. Auch Fertigungshersteller von Dieselinjektoren waren betroffen und ebenfalls über Monate nicht in der Lage, die Produktion ordnungsgemäß aufrecht zu erhalten.

Den Verbrechern geht es fast immer um hohe Lösegeldforderungen, die in Kryptowährung beglichen werden müssen. Und die Opfer zahlen, denn sie haben meist keine andere Wahl. Wenn Produktions- oder Geschäftsbetrieb lahmgelegt sind, wird für die betroffenen Betriebe daraus schnell eine Überlebensfrage. Zehn Prozent aller deutschen Firmen fürchten laut Verbandsumfrage wegen der Online-Attacken inzwischen um ihre Existenz.

Zur Person

Sebastian Artz vom Verband Bitkom vertrat dieses Jahr als Sachverständiger die Perspektive der Wirtschaft in der öffentlichen Anhörung zum IT-Sicherheitsgesetz 2.0 im Ausschuss des Deutschen Bundestags.

Angriffsflächen vergrößern sich

„Mit voranschreitender Digitalisierung als solcher vergrößern sich auch die Angriffsflächen", resümiert Sebastian Artz, Bereichsleiter Cyber- & Informationssicherheit beim Verband Bitkom. Die Corona-Pandemie, bei der viele Belegschaften ins Home-Office migrierten, verursachte noch einmal einen besonderen Schub, da sich damit ein weiteres Öffnungstor für Kriminelle erschloss. „Die organisierte Kriminalität hat parallel stark zugenommen, weil heutzutage Cyberangriffe ohne

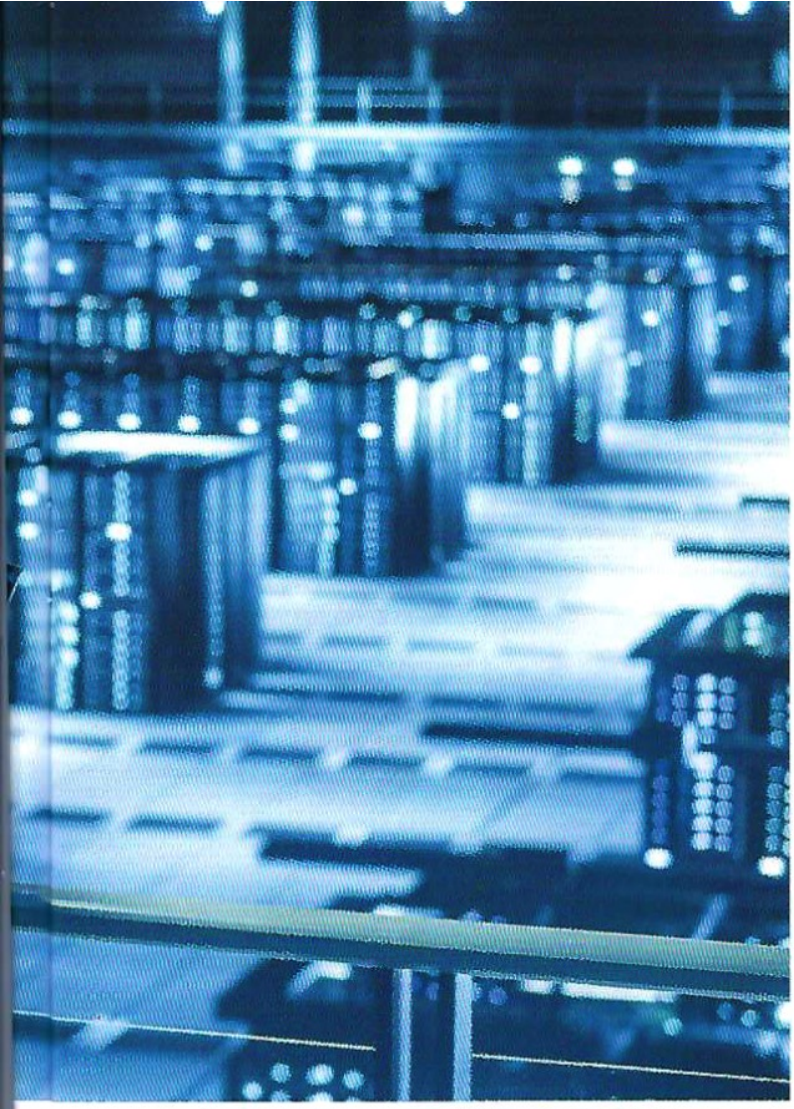
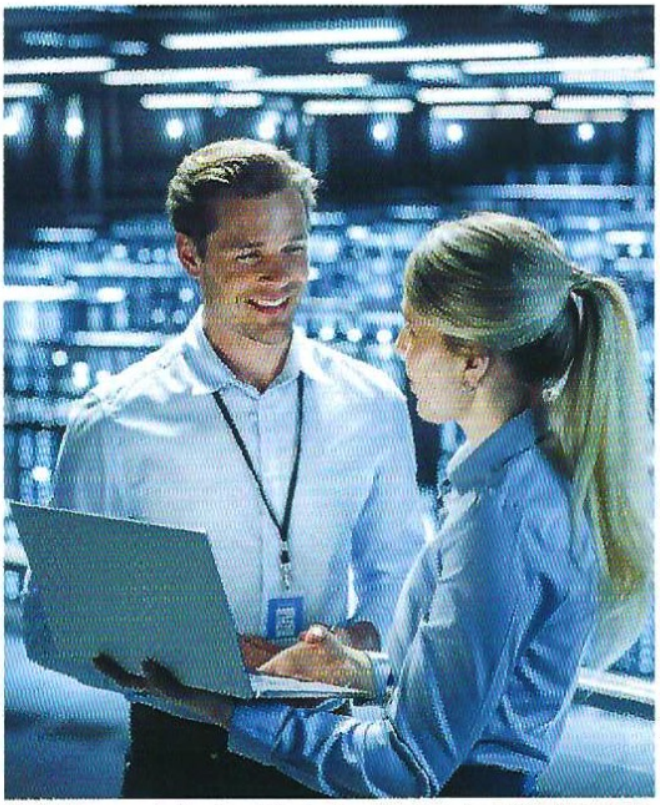


Foto: © Gorodenkoff/shutterstock.com



Vieler Firmen schulen ihre Mitarbeiter: Sie sind die größte Schwachstelle – vor allem bei echt anmutenden Phishing-Mails.

FOTO: © GORODENKOFF/SHUTTERSTOCK.COM

große IT-Kenntnisse von Kriminellen gefahren werden können und man Unternehmen damit so gut erpressen kann", sagt Artz. „Und das zwar nicht nur mit der Verschlüsselung von Daten, sondern auch mit dem Diebstahl sensibler Daten und der Drohung der Veröffentlichung."

Laut Bitkom-Experten ist das meistgenutzte Instrument der Cyber-Gangster die Phishing-Mail, entweder als Massenversendung oder individuell zugeschnitten auf eine bestimmte Person. Die Schadsoftware wird meist beim Öffnen von Anhängen solcher Mails auf das Endgerät gespielt und kann sich dann auf das gesamte Unternehmensnetzwerk verbreiten, wenn keine oder nicht ausreichende interne Schutzwälle eingezogen wurden. Softwareschwachstellen, etwa wenn Updates nicht aktualisiert werden, bieten weitere Möglichkeiten für virtuelle Eindringlinge.

> **Pro Tag entstehen 300 000 neue Varianten von Schadcodes.**
>
> **Sebastian Artz**
> Bitkom-Experte

Schadsoftware per Mail

Auch wenn die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) in Frankfurt in Zusammenarbeit mit den Strafverfolgungsbehörden der Niederlande, der Ukraine, Litauens, Frankreichs, Großbritanniens, Kanadas und den USA die Infrastruktur der weltweit als am ge-

Erste Hilfe im Notfall

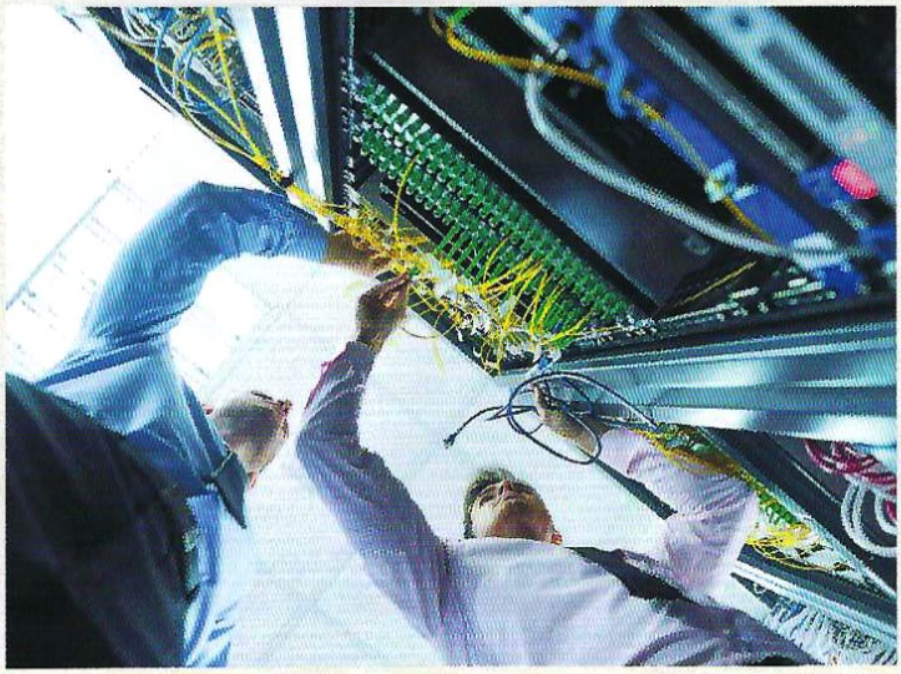


FOTO: © DOTSHOCK/SHUTTERSTOCK.COM

Ist ein Unternehmen Opfer eines Cyber-Angriffs geworden, ist meist Hilfe von Experten nötig.

Von Cyberangriffen betroffene kleine und mittlere Unternehmen können sich in einem ersten Schritt an die Cyberwehr Baden-Württemberg, ein Projekt der Digitalisierungsstrategie des Landes, wenden. Die Experten dort leisten bislang ausschließlich am Telefon kostenlos und vertraulich erste Hilfe und schalten zur Vorfalldiagnose weitere IT-Fachleute dazu, die Sofortmaßnahmen empfehlen können. Stellt sich heraus, dass weitere Maßnahmen oder ein Einsatz vor Ort erforderlich sind, werden Experten zu vorab festgelegten Preisen vermittelt. Sobald der Schaden eingetreten beziehungsweise erkannt ist, raten die Experten der Cyberwehr dazu, sofort auffällige Bildschirminhalten zu fotografieren und Snapshots von virtuellen Infrastrukturen zu erstellen. Notfall-Rufnummer: 0800-CYBERWEHR oder 0800/29 23 79 347.

fährlichsten geltenden Schadsoftware „Emotet" übernehmen und zerschlagen konnte, sind solche Erfolge eher die Ausnahme. Oberstaatsanwalt Benjamin Krause, Pressesprecher der ZIT, bestätigt, dass immer mal wieder Täter gefasst werden, vor allem wenn sie aus Deutschland heraus agieren.

International vernetzt

Durch die internationale Vernetzung der Kriminellen gelinge ihre Identifizierung aber nur selten. „Pro Tag", ergänzt Artz, „entstehen 300 000 neue Schadcode-Varianten, die im Internet dazu kommen, pausenlos werden Angriffe auf Infrastrukturen gefahren."

> **„Unternehmen verheimlichen Cyberattacken, weil sie um ihr Ansehen fürchten."**
>
> **Jens Fröhner**
> IHK Digital

Daher gilt Prävention als der einzig wirksame Schutz. Aber die Aufmerksamkeit für diese Problematik ist noch nicht so verbreitet wie es ihrer Bedeutung entspricht. Das betont Jens Fröhner, der federführend bei den baden-württembergischen IHK für das Thema Digitalisierung zuständig ist: „Die Geschäftsführungen müssen dafür noch mehr sensibilisiert werden. Brandschutzübungen beispielsweise sind an der Tagesordnung, aber Simulationen, um mit Cyberangriffen umzugehen, finden kaum statt." Zudem verheimlichten viele Betriebe, dass sie Opfer einer Cyberattacke geworden sind, weil sie befürchten ihr Ansehen zu verlieren.

Neben den grundsätzlichen klassischen Vorsichtsmaßnahmen wie stets aktualisierte Firewalls und Softwareupdates sollten sich die Verantwortlichen in den Unternehmen grundsätzlich darüber Klarheit verschaffen, welche Bereiche, Daten und Informationen überhaupt geschützt werden sollten

Zur Person

Michael Lück Der Kölner ist seit über 20 Jahren als Berater für Strategie- und Personalentwicklung tätig. Ungewöhnlich ist sein Konzept „Lichtlos", mit dem er Workshops in völliger Dunkelheit durchführt.

und wo entsprechend die Schwachstellen liegen können rät Steven Arzt, Leiter der Abteilung Secure Software Engineering, Fraunhofer Institut für Sichere Informationstechnologie SIT in Darmstadt.

Schwachstellen identifizieren

Und Markus Grau von Purestorage ergänzt, dass das frühe Erkennen einer möglichen Attacke wichtig sei. „Da auch im Mittelstand die IT-Umgebungen und Datenvolumen immens gewachsen sind, können IT-Teams und deren Experten alleine dies nicht leisten. Der Einsatz künstlicher Intelligenz entlastet die IT-Teams und erweitert deren Möglichkeiten deutlich, Angriffe schnell zu erkennen und rasch zu handeln."

Die meisten Fachleute im Cyberbereich mahnen aber auch, den „menschlichen Faktor" nicht außer Acht zu lassen. So auch der Kölner Strategieberater im Bereich IT-Security Michael Lück. Als Kooperationspartner der Cyber Alliance des Bundesamtes für Sicherheit in der Informationstechnik führt der Trainer und Coach regelmä-

FOTO: © FIRMENFOTO

Um Unregelmäßigkeiten an besonderen Tagen wie Hausmessen oder an Wochenenden zu erkennen, braucht es nicht nur Technik, sondern auch Fachkräfte.

ßig Workshops und Schulungen durch, um Mitarbeiter in den Unternehmen zu sensibilisieren. „Bei der Unmenge an Daten, die täglich über den Bildschirm flimmern, ist das Gespür, das Bauchgefühl oder die Intuition entscheidend", sagt er und ergänzt: „Das Empfinden ‚Achtung, hier könnte etwas nicht stimmen' ist von besonderer Bedeutung." Denn Menschen, die schon seit Jahren im Unternehmen arbeiten und ganz genau wissen, wie die Datennetze an besonderen Tagen wie etwa Messen, Betriebsurlaub, Feiertage, Wochenende oder bei bestimmten Prozessen wie Wartungsarbeiten oder dem Anfahren neuer Produktionsstraßen reagieren. „Sie haben oft ein gutes Gespür für Anomalien."

Unbekannte Anomalien gelten als Gefahren-Indikatoren. Es sei eine wichtige Führungsaufgabe, dieses Gespür ernst zu nehmen, die Kollegen und Kolleginnen dafür zu sensibilisieren und das Bewusstsein zu schärfen.

Ganz wichtig, so Lück: Der Bereich Cybersicherheit muss direkt bei der Geschäftsführung angesiedelt sein, am besten mit einer eigenen Abteilung oder einem speziellen Team. [!]

Wilfried Urbe