IMMER MEHR CYBER-ANGRIFFE

Wenn ein falscher Klick den Betrieb lahmlegt

Ein einziger Klick kann heute ein gesamtes Unternehmen lahmlegen. Schon das Öffnen einer E-Mail kann Kosten in Millionenhöhe verursachen. Was können Unternehmer tun, wenn Hacker Daten abfangen oder Lösegeld fordern?

Cyberangriffe sind derzeit die größte Sorge für Unternehmen weltweit. Die Bedrohung durch Ransomware, Datenverletzungen oder IT-Ausfälle beunruhigt die Unternehmen sogar noch mehr als Geschäfts- und Lieferkettenunterbrechungen, Naturkatastrophen oder die Folgen der Corona-Pandemie. Das ist das Ergebnis des Allianz-Risikobarometers, für das 2 650 Experten in 89 Ländern befragt wurden.

Das hat seinen Grund: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt die Cyber-Bedrohungslage in Deutschland als „angespannt bis kritisch“ ein. Die Angriffsmethoden entwickelten sich schnell weiter, und auch die Anzahl der Schadprogramm-Varianten nimmt laut BSI-Lagebericht deutlich zu. Im vergangenen Jahr wurden 144 Millionen neue Varianten identifiziert – ein Zuwachs von 22 Prozent im Vergleich zum Vorjahr.

Mehr Kompetenzen für den Bund

Das zuständige Bundesinnenministerium war in der vergangenen Legislaturperiode nicht untätig. Mit einer neuen Cybersicherheitsstrategie und einem IT-Sicherheitsgesetz wurden zwei Meilensteine für mehr Sicherheit im Netz gesetzt. Das Personal im BSI wurde mit mehr als 700 neuen Stellen fast verdoppelt. Die Behörde wurde mit mehr Kompetenzen bei der Detektion von Sicherheitslücken und bei der Abwehr von Cyberangriffen ausgestattet. Durch klare Meldewege sollen rechtliche Unsicherheiten bei der Aufdeckung von IT-Schwachstellen bei Unternehmen ausgeräumt werden.

Zudem wurde ein einheitliches IT-Sicherheitskennzeichen eingeführt, das die Sicherheitsfunktionen von IT-Produkten auf einen Blick sichtbar macht. Die neuen Befugnisse stießen damals insbesondere bei der FDP auf Kritik.

Ukraine-Krieg verschärft Lage

Doch wie wichtig die Kompetenzausstattung staatlicher Behörden ist, zeigt sich spätestens seit der „Zeitenwende“ in diesem Jahr. Nach dem Angriff Russlands auf die Ukraine habe sich die Bedrohung durch Cyberangriffe weiter ver-

Foto: appledesign/adobe.Stock.com

schärft, sagte BSI-Präsident Arne Schönbohm im Juni auf einer Sicherheitskonferenz in Potsdam.

Er berichtete von einer Attacke auf die deutsche Tochtergesellschaft des russischen Ölkonzerns Rosneft, die beinahe zu einer massiven Störung der Mineralöl-Distribution vor allem im Großraum Berlin und Brandenburg geführt hätte. „Das konnte gerade noch abgewendet werden, weil es gelungen ist, die IT-Systeme von Rosneft Deutschland wieder kurzfristig in Gang zu bringen“, so Schönbohm.

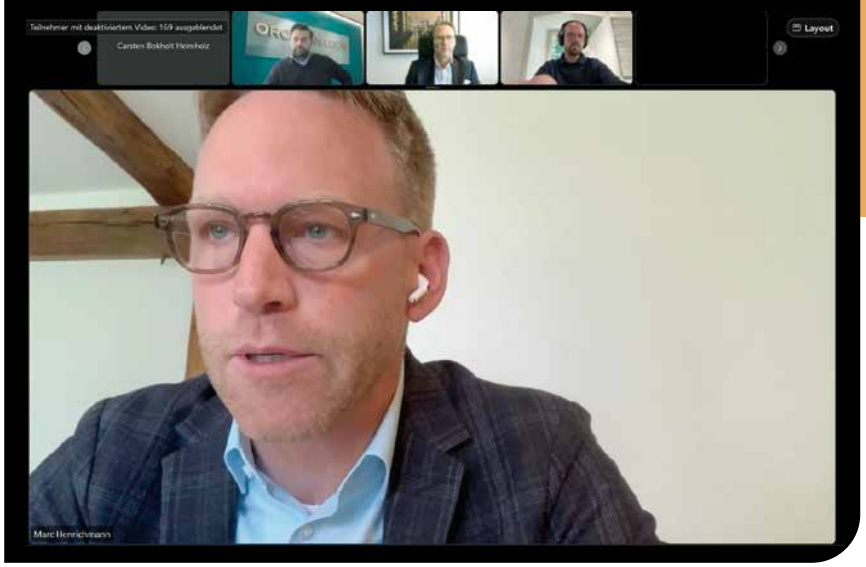
220 Milliarden Euro Schaden

Doch es sind nicht nur einige wenige Konzerne betroffen. Dem Digitalverband Bitkom zufolge haben Cyberangriffe im vergangenen Jahr bei 86 Prozent der Unternehmen in Deutschland Schaden verursacht. Umfang: mehr als 220 Milliarden Euro. „Die Wucht, mit der insbesondere Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend und trifft Betriebe aller Branchen und Größen“, sagt Bitkom-Präsident Achim Berg.

Bei einem Ransomware-Angriff verschafft sich ein Schadprogramm Zugriff auf das Gerät. Das erreichen Hacker auf immer clevere Weise, bspw. über Phishing-Angriffe, bei denen sich die Schadsoftware in einem infizierten, aber legitim getarnten E-Mail-Anhang verbirgt. Öffnet ein Mitarbeiter diesen Anhang, kann sich die Software automatisch auf dem Gerät ausbreiten – im schlimmsten Fall sogar auf das gesamte Unternehmensnetzwerk und verbundene Server. Neben dem Ziel, Daten abzugreifen oder an wertvolle interne Informationen zu gelangen, sind nicht selten Erpressungen das Ziel der Angreifer.

„Die Wucht, mit der Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend.“

Achim Berg, Präsident Bitkom



„Achtung, Cyber-Attacke“: 180 zugeschaltete Mittelständler haben bei einer MIT-Videokonferenz miterleben können, wie ein Cyberangriff abläuft. CDU-Digitalexperte Marc Henrichmann gab Tipps.

„Achtung, Cyber-Attacke“

Dabei tun Unternehmen nach Einschätzung vieler Experten noch nicht genug, um sich abzusichern. Laut einer BSI-Umfrage investiert jedes zweite Unternehmen gerade einmal ein bis zehn Prozent des IT-Budgets in Cybersicherheit. Notwendig wären aber 20 Prozent, heißt es von Seiten der Behörde.

Wie sollte ein Unternehmen im Fall eines Hackerangriffs reagieren? Um diese Frage zu beantworten, hat die MIT gemeinsam mit Fachexperten die Online-Veranstaltung „Achtung, Cyber-Attacke: Was Sie für den Ernstfall wissen sollten“ durchgeführt. Dabei wurde vor rund 180 zugeschalteten MIT-Mitgliedern eine realistische Cyber-Attacke simuliert.

„Alle Gesetze sollten zukünftig auf den Faktor Cybersicherheit geprüft werden.“

Catarina dos Santos Firnhaber,
CDU-Bundestagsabgeordnete

So reagieren Unternehmen richtig

Die Experten empfehlen, im Falle eines Cyberangriffs umgehend folgende Schritte einzuleiten – egal ob Kleinstbetrieb oder Großkonzern: Server offline stellen, WLAN abstellen, Stecker ziehen, die „Ransom note“, also das Erpresserschreiben, sichern. Server und Systeme sollten dabei nicht heruntergefahren werden, sondern nur vom Netzwerk getrennt werden. Sonst würden eventuell Spuren für die Forensik, die Spurensicherung, vernichtet.

Unverzüglich sollte ein zuvor festgelegter Krisenstab informiert werden. Dieser Krisenstab sollte zum Zeitpunkt des Angriffs bereits geschult und sofort einsatzbereit sein. Im Idealfall steuert ein Experte für Krisenkommunikation die interne Kommunikation gegenüber den Mitarbeitern, aber auch die Kommunikation gegenüber Kunden, Lieferanten und der Presse. Hier ist es insbesondere bei Mittelständlern oft ratsam, sich externe Hilfe zu suchen.

Datenverletzungen sind meldepflichtig

Ebenso sollten Rechtsberater und Versicherungsmakler hinzugezogen werden. Denn es besteht eine gesetzliche Meldepflicht gegenüber Datenschutzbehörden innerhalb von 72 Stunden, sofern personenbezogene Daten betroffen sind. Deshalb sollten auch der Datenschutzbeauftragte und der Personalrat hinzugezogen werden – falls vorhanden. Sollte die Datenschutzgrundverordnung verletzt werden, können Unternehmen mit vier Prozent des Jahresumsatzes haftbar gemacht werden.

Außerdem empfehlen die Experten, Anzeige bei der Kriminalpolizei zu erstatten. Insbesondere dann, wenn man erpresst wird. Denn, was viele nicht wissen: Wer Lösegeld zahlt, kann sich strafbar machen. Nämlich dann, wenn das Geld einer kriminellen Vereinigung zufließt – auch dann, wenn der Zahlungsempfänger unbekannt ist.

Oft kommen die Angreifer aus dem Ausland oder die Konten befinden sich dort. Deshalb sollte das Unternehmen ebenso eine Selbstanzeige beim Zoll stellen, da Zahlungen als Geldwäsche gewertet werden könnten. „Haftbar ist man in der Regel aber nur, wenn man sich nachweislich etwas zu Schulden kommen lassen hat“, erläutert Rechtsanwalt Philipp Heinrichs. Er rät: Lösegeld sollte nur gezahlt werden, wenn die Existenz des Unternehmens gefährdet ist. Überprüfen sollte das Unternehmen zudem, ob in einer Cyber-Versicherung, die jedoch die wenigsten Unternehmen abgeschlossen haben, eine Lösegeldzahlung mitversichert ist – und bis zu welcher Höhe.

Je länger das Passwort, desto besser

Damit es erst überhaupt nicht zu diesem Szenario kommt, sollten Unternehmen vorsorgen. „Präventives Krisenmanagement muss geübt werden, um besser in der Krise aufgestellt

zu sein“, sagt der Versicherungsmakler Fredrik Köncke.

Er rät, regelmäßig zu prüfen, ob die Firewall ausreichend konfiguriert ist und diese auch ungewöhnliches Verhalten erkennen kann. Wichtig ist ferner die Schulung von Mitarbeitern, damit diese ungewöhnliches Verhalten erkennen können.

Die Nutzung von langen und komplexen Passwörtern erschwert den Hackern ebenfalls ihre Arbeit. Mittlerweile empfehlen Experten Passwörter mit mehr als 15 Stellen. Kürzere Passwörter könnten bereits in wenigen Stunden errechnet werden. Außerdem sollten Passwörter nicht ständig geändert werden. Denn dann neigen Nutzer dazu, simplere Passwörter zu verwenden. Passwörter sollten nicht auf Post-It-Zetteln, sondern in Safes aufbewahrt werden.

CDU-Bundestagsabgeordnete Catarina dos Santos Firnhaber wünscht sich mehr Einsatz der Bundesregierung im Kampf gegen Cyberkriminalität.

Software ständig aktualisieren

Software-Aktualisierungen können lästig sein, sollten aber nicht wochenlang aufgeschoben werden. Gefährlich sind insbesondere „End-of-Life-Systeme“: Also Software, die vom Hersteller nicht mehr produziert oder unterstützt wird. Somit ist diese besonders angreifbar, da keine Sicherheitsüberprüfungen mehr durchgeführt werden.

Neben einem Krisenstab sollte jedes Unternehmen den Experten zufolge eine IT-Taskforce einrichten, die ein Notfallsystem aufgebaut hat. Für einen geordneten Überblick und angemessene Reaktionen kann auch ein Handbuch hilfreich sein. Es sollte beispielsweise sichergestellt sein, dass es Zugang zu Geräten gibt, die nicht mit dem System verbunden sind und die notfalls laufen, wenn das gesamte System gehackt wurde.

Keine fremden USB-Sticks nutzen

Marc Henrichmann, Berichterstatter der CDU/CSU-Bundestagsfraktion für den Bereich Cybersicherheit im Ausschuss für Inneres und Heimat, warnt zudem vor „Smishing“. Dabei werden überzeugende SMS- oder Textnachrichten mit einem Link versendet, hinter dem sich Schadsoftware verbirgt. Henrichmann warnt zudem vor vermeintlich auf Parkbänken vergessenen USB-Sticks – diese könnten mit Schadsoftware beladen sein.

„Man muss immer wieder auf die kleinen Dinge hinweisen, damit die großen Dinge nicht geschehen“, sagt der Bundestagsabgeordnete. „Ein ständiges Monitoring kann helfen, dass diese kleinen außergewöhnlichen Geschehnisse schneller auffallen.“

Henrichmanns Fraktions- und MIT-Kollegin Catarina dos Santos Firnhaber weist darauf hin, dass nicht nur viele Bürger und Betriebe arglos seien. „In ähnlicher Weise fehlt ein grundlegendes Verständnis in der Politik für einen ganzheitlichen Ansatz bei der Digitalisierung, der auch das Feld Cybersicherheit ganz natürlich einbezieht. Denn Cybersicherheit ist eine Grundvoraussetzung für digitales Vertrauen“, sagt die CDU-Abgeordnete, die Mitglied im Digitalausschuss des Bundestages ist.

Ampel-Koalition schläft

Dos Santos Firnhaber wünscht sich vor allem nach dem Krieg in der Ukraine eine Reaktion der Politik. „Jedoch fehlt sogar im aktuellen Entwurf der Digitalstrategie der Bundesregierung bislang noch ein Hinweis auf die Problematik.“ Auch in aktuelle Gesetzgebungsverfahren wie bei der Einführung einer digitalen Hauptversammlung würden Cyber-Risiken nicht einmal erwähnt. „Es fehlt jeglicher Anspruch und auch eine Sensibilität, den digitalen Sicherheitsbedürfnissen der Unternehmen gerecht zu werden. Das reicht nicht. Alle Gesetze sollten zukünftig auf den Faktor Cybersicherheit geprüft werden“, fordert sie. Die Behörden benötigten eine bessere personelle und technische Ausstattung. „Auch sollten wir aktiver über Reformen in der Strafverfolgung in diesem Bereich nachdenken. Denn eine verbesserte IT-Sicherheit und die Absicherung gegen Schäden durch Cyber-Attacken sind zentral für den Wirtschaftsstandort Deutschland und können zum Standortvorteil für alle Beteiligten werden. Das muss auch ohne zusätzliche Kosten und Bürokratie möglich sein“, so die CDU-Digitalexpertin.

Alina Kemper
Redakteurin
kemper@mit-bund.de