Ein Akt der Zerstörung

Hackerangriffe gelten Unternehmen aller Größen und Branchen. Von langer Hand wurde der Angriff auf die Autohausgruppe von Anja Bauer aus Flensburg geplant.

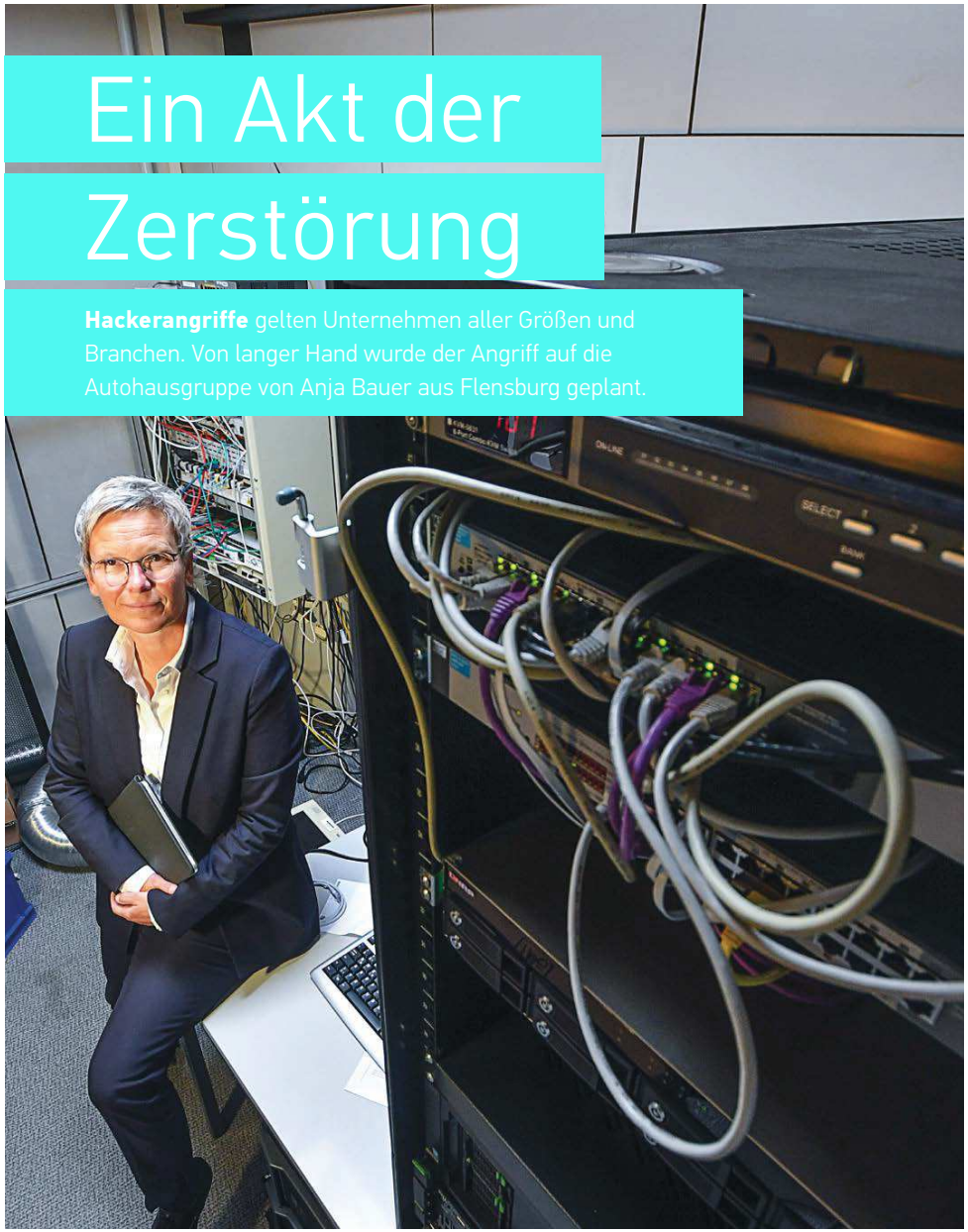


FOTO: SEEMANN

Nach 16 Monaten ist das Gefühl der Normalität zurück. So lange verfolgt Anja Bauer ein Ziel: die Rettung ihres Betriebes. Ein Kraftakt. Eine Teamleistung. Ein stetiges Auf und Ab zwischen Hoffen und Bangen. Noch immer läuft nicht alles rund. Doch Anja Bauer sieht sich für die Zukunft gut gerüstet: „Wir sind erstmals wieder an einem Punkt angekommen, der es uns ermöglicht, die Prozesse verlässlich zu überblicken und wirtschaftlich planen zu können." Die Bauer Gruppe beschäftigt in Flensburg, Schleswig, Heide und Husum 250 Mitarbeiter. In Autohäusern und Werkstätten.

Rückblick: 9. Juni 2022. Freitag. Ein unbeschwerter Abend. Das Sommerfest der Bauer Gruppe. Hinter allen liegen zwei Jahre ohne soziales Miteinander. Corona. Geschlossene Autohäuser. Masken. Abstand. Sonderregelungen. Daran will heute keiner mehr denken. Es ist Zeit zum Feiern. Essen. Trinken. Tanzen. Niemand ahnt, dass in wenigen Stunden ein böses Erwachen droht. Das Unternehmen wird Opfer eines Hackerangriffs. Eine Attacke, die Experten des Landeskriminalamtes später als einen Großangriff beschreiben. Totale Zerstörung. Lange vorbereitet. In nur 90 Minuten vollendet.

Anja Bauer erlebt den Samstagmorgen am Frühstückstisch. Zeitgleich will sich in der Firma der erste Mitarbeiter am Computer anmelden. Ohne Erfolg. Der Bildschirm bleibt schwarz. Störungen in der IT sind normal und meist schnell behoben. Ein Anruf beim IT-Spezialisten sollte reichen. Aber der kann nichts machen. Kein Zugriff aus der Ferne. Die Server stehen still. Schnell macht er sich auf den Weg in die Firma. Vor Ort findet er auf dem Server eine Textnachricht. Wenige Zeilen mit gewaltiger Bedeutung. Die Gruppe Black Basta erklärt, das Firmennetzwerk gehackt und alle Daten verschlüsselt zu haben. Weitere Informationen können im Darknet abgerufen werden.

> »Corona und geschlossene Autohäuser waren zum Üben. Dieser Angriff verursachte das größte denkbare Chaos.«
>
> **Anja Bauer**
>
> Geschäftsführerin der Bauer Gruppe in Flensburg

136.865

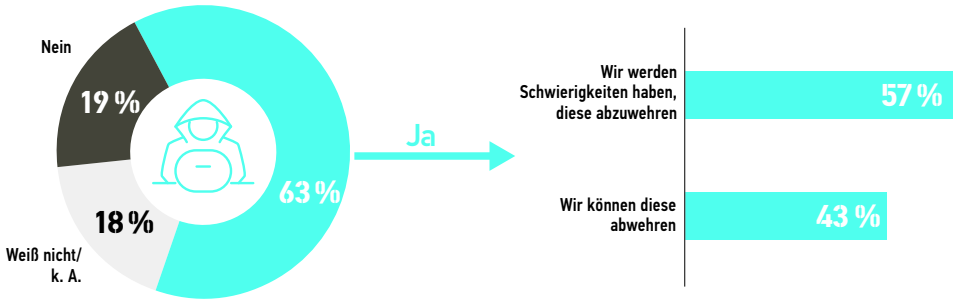
Cyberangriffe registrierte das Bundeskriminalamt (BKA) 2022. Die Zahl ist leicht gesunken. Dennoch rechnet die Behörde mit einer Dunkelziffer von 90 Prozent.

Schock am Frühstückstisch

Am Frühstückstisch von Anja Bauer klingelt das Telefon. Sie ahnt, dass etwas Schlimmes passiert sein muss. Ihr Dienstleister hat bislang noch jede Störung ohne viel Aufhebens behoben. Selbst Schäden kleinerer Hackerangriffe waren schnell identifiziert und beseitigt. Doch heute ist alles anders. Anja Bauer hört ihm zu: Alle 25 Server sind verschlüsselt. Alle Sicherungen sind zerstört. Anja Bauer legt auf, versucht die Ruhe zu bewahren, geht eine Runde mit dem Hund, packt eine Flasche Rum ein und fährt zum Betrieb. Dort angekommen, verschafft sie →

Zwei Drittel der Unternehmen erwarten Cyberangriffe

Glauben Sie, dass Ihr Unternehmen in den kommenden zwölf Monaten Ziel von Cyberangriffen wird?



Quelle: Bitkom Research 2023

Basis links: Alle Unternehmen (n=603); Basis rechts: Unternehmen, die Cyberangriffe erwarten (n=380)

→ sich einen ersten Überblick und informiert die Polizei.

Puzzleteile eines Großangriffs

Vor Ort verschaffen sich Beamte des Landeskriminalamtes einen Überblick. Viel Hoffnung können sie Anja Bauer nicht machen. Die Hackergruppe zählt zu den weltweit besten. Festnahmen sind nahezu ausgeschlossen. Von wo aus sie agieren, ist kaum nachzuvollziehen. Den Fahndern bleibt die Analyse des Angriffs. Aus Puzzleteilen entsteht ein Bild der vergangenen Stunden, Tage und Monate. Ein Bild eines Großangriffs. Gestartet vor etwa sechs Monaten, als Kriminelle sich vermutlich über einen Chip in einer Überwachungskamera unbemerkt Zugriff auf das IT-System verschafften. Warum die Bauer Gruppe? Um sie als Autohändler geht es wohl nur zweitrangig. Die Polizei vermutet einen Zusammenhang mit dem Krieg in der Ukraine. In Dithmarschen schweißt das Unternehmen doppelwandige Auflieger für Tankwagen und prüft deren Dichtigkeit. Eine Dienstleistung, die nur ganz wenige anbieten. Kunde ist die Bundeswehr. In den Tanks transportieren die Fahrzeuge Benzin und Kerosin. Die Vermutung: die Hacker wollten den Betrieb zerstören. Dafür beobachteten sie die Vorgänge im IT-System genau und investierten Hackerstunden im geschätzten Wert von rund einer Million Euro. Auch der Zeitpunkt scheint gezielt gewählt: die Nacht des Sommerfestes.

203 MILLIARDEN

Euro Schaden richteten Hackerangriffe im Jahr 2022 in Deutschland laut dem Digitalverband Bitkom an. Für 2023 wird mit einem Anstieg auf 206 Milliarden gerechnet.

NACHGEFRAGT BEI

Kevin Gailus

Beauftragter für Innovation und Technologie in der Handwerkskammer Schwerin

Herr Gailus, Sie beraten Handwerker in Fragen der Digitalisierung. Wie ernst nehmen Firmen den Schutz vor Cyberangriffen?

Kevin Gailus: Ich treffe viele Unternehmer, die das Thema sehr ernst nehmen und viele Vorkehrungen treffen. Aber es gibt auch jene, vor allem kleine Unternehmen, die das Thema für sich nicht als relevant erachten. Für sie ist es ein unliebsames Thema. Es kostet einfach Zeit und Geld. Das ist gefährlich. Unsere Sicherheitsbotschafter raten zur Prävention. Sie ist das beste Mittel und verhindert, dass man erst nach einem Angriff den hohen Wert der verlorenen Daten erkennt. Im schlimmsten Fall wird man handlungsunfähig.

Was empfehlen Sie konkret?

KG: Mit kleinem Aufwand lässt sich großer Schaden verhindern. Grundsätzlich sollten die IT-Systeme auf dem neuesten Stand sein. Jedes Update schließt Sicherheitslücken. Auch die Anschaffung von Firewalls kann helfen. Die wichtigste Maßnahme sind regelmäßige Backups. Es kann hilfreich sein, wenn Firmen gedanklich den Brandfall simulieren. Der Schaden ähnelt einem Cyberangriff. Wie groß wäre dann der Verlust der Daten? Wer merkt, wie sehr es schmerzen würde, muss handeln. Das gilt erfahrungsgemäß insbesondere für sensible Daten von Kunden und Aufträgen. Werden Daten häufig verändert oder müssen sie schnell verfügbar sein, sollten sie auch möglichst häufig gesichert werden. Am besten täglich.

Viele verbinden den Cyberangriff mit der Spam-E-Mail. Sind Mitarbeiter, die Anhänge öffnen und Links anklicken, die größte Sicherheitslücke?

KG: Der E-Mail-Server ist ein großes Einfallstor für Hacker. Deshalb ist die Aufklärung aller Beteiligten der zweite wichtige Baustein der Prävention. Niemand klickt beabsichtigt auf fragwürdige Links oder Anhänge. Das sollte man seinen Mitarbeitern unbedingt vermittelt. Es geht nicht um Misstrauen oder Kontrolle. Mitarbeiter und auch die Chefs sollten geschult sein. Denn Spam-Mails lassen sich meist gut erkennen, wenn man sich im turbulenten Arbeitsalltag die Zeit dafür nimmt. Wer sensibilisiert ist, prüft E-Mail-Adressen auf Plausibilität oder ignoriert unbekannte Anhänge. Im Zweifel sollten Betroffene immer die IT-Spezialisten, Dienstleister oder den Chef kontaktieren und mit ihnen beraten, ob unbekannte Inhalte gefährlich sind.

Können Firmen sich auch auf den Fall eines Angriffs vorbereiten?

KG: Auch das sollte vorab gut durchdacht und geregelt werden. Wir empfehlen einen IT-Notfallplan. Firmen müssen diesen digital und ausgedruckt verfügbar haben. Die wichtigste Info ist die Notfallnummer des IT-Dienstleisters oder zuständigen Mitarbeiters. Es sollte deutlich erkennbar sein, dass die Arbeit beendet und die betroffenen Geräte vom Netzwerk getrennt werden müssen. Ebenso wird festgehalten, wer den Schaden meldet und dann darüber informiert, welche IT-Systeme betroffen sind, wo diese sich befinden und was beobachtet wurde. |

Die Fragen stellte Jens Seemann

Infos und Download zur IT-Notfallkarte :
bit.ly/48jw35d

FOTOS: HFR/ADOBE STOCK

Wie sicher ist mein Betrieb?

Sicherheitscheck vom Deutschland sicher im Netz e.V. (DsiN)

Unternehmen können per Online-Test ihr IT-Sicherheitsniveau ermitteln und erhalten Tipps. In wenigen Minuten erhalten Sie eine Auswertung mit passenden Handlungsempfehlungen.

Zum Test:
www.sicher-im-netz.de/dsin-sicherheitscheck

Hohe Dunkelziffer

Das Bundeskriminalamt (BKA) registrierte im Jahr 2022 insgesamt 136.865 Cyberangriffe auf Unternehmen. Die Spitze des Eisbergs. Das BKA schätzt die Dunkelziffer auf 90 Prozent. Die einen stehlen Daten. Andere legen Computer-Systeme lahm und verschlüsseln sie. Schon längst sitzen Cyberkriminelle nicht mehr nur alleine in einem Keller. Das BKA spricht von einem internationalen, weit verzweigten Wirtschaftszweig mit gezielter Aufgabenteilung.

„Im Jahr 2022 fühlten sich 52 Prozent der Betriebe durch Cyberangriffe in ihrer Existenz bedroht. So viele wie nie zuvor", sagt Ralf Wintergerst, Präsident des Digitalverbandes Bitkom. Zwei Jahre zuvor waren es lediglich 29. Eine Umfrage seines Verbandes ergab, dass 63 Prozent in den kommenden zwölf Monaten mit einem Angriff rechnen. Wintergerst unterstreicht die hohe Attraktivität der deutschen Wirtschaft als Ziel der Kriminellen. Hinzu kämen staatlich gelenkte Angriffe. Bitkom beziffert den Schaden durch Diebstahl und Sabotage für das Jahr 2022 auf 203 Milliarden Euro. Rund doppelt so viel wie 2019. Die Prognose für 2023: rund 206 Milliarden Euro.

„Es ist höchste Zeit, aufzuwachen. Wer Verantwortung für ein Unternehmen trägt, muss dafür sorgen, dass IT-Sicherheit nicht allein Thema der IT-Spezialisten ist", sagt Bitkom-Präsident Wintergerst. Er empfiehlt drei Dinge: IT-Sicherheit muss mit den notwendigen Ressourcen ausgestattet werden. Sein Rat: 20 Prozent aller IT-Ausgaben sollten bereitgestellt werden. Ergänzend dazu sollten alle Mitarbeiter geschult werden. Weil der Mensch das häufigste Einfallstor für Angriffe ist. Deshalb sollte das eigene Team regelmäßig auf den neuesten Stand der Gefahren gebracht werden. Für den Fall eines Angriffs empfiehlt Bitkom einen Notfallplan. Dieser muss klar regeln, was zu tun ist. „Wenn ein Unternehmen Opfer eines Angriffs wird, ist keine Zeit, sich diese Fragen erstmals zu stellen. Je schneller reagiert wird, desto besser stehen die Chancen, größeren Schaden abzuwenden", so Wintergerst.

Fehlender Überblick

Zurück nach Flensburg: ein Erwachen im totalen Chaos. Die mitgebrachte Flasche Rum beruhigt das Team nur kurz. Jetzt müssen Entscheidungen getroffen werden. Soll man sich auf die Erpressung einlassen? Anja Bauer ist sich mit ihren Geschäftspartnern einig: keine Lösegeldzahlung. Sie vermeiden jeglichen Kontakt zu den Hackern. Kein Aufsuchen der genannten Seite im Darknet. Kein Abrufen der Forderungen. Gemeinsam wollen sie ab sofort alles tun, um den Betrieb zu retten. Anja Bauer hat zwar Mitarbeiter, Gebäude und auch Autos. Aber es fehlen Daten und der Überblick. Welche Autos gehören der Firma. Wer hat bezahlt? Wer ist für welchen Bereich verantwortlich? Ob →

Prävention und Bewältigung

... Tipps zum Thema gibt es in der Rubrik Lohnenswert auf Seite 40

Beratung zur IT-Sicherheit

Ansprechpartner der Handwerkskammern

Flensburg
Marius Vespermann
0461 866 -132
m.vespermann@hwk-flensburg.de

Hamburg
Célia Rodrigues
040 35905 -533
Celia.Rodrigues@hwk-hamburg.de

Lübeck
Wolfram Kroker
0451 1506 -727
wkroker@hwk-luebeck.de

Schwerin
Kevin Gailus
0385 7417-146
k.gailus@hwk-schwerin.de

ES IST DIE FRAGE NACH DEM WANN

Für die Sicherheit der Firmen kooperieren die Kammern mit den Landeskriminalämtern.

Jannika Grade Zentrale Ansprechstelle Cybercrime (ZAC) im LKA Schleswig-Holstein.

Frau Grade, wie schätzen Sie die IT-Sicherheitslage in Unternehmen ein?

Jannika Grade: Das Risiko, Opfer eines Cyberangriffs zu werden, ist unvermindert hoch. Durch die Digitalisierung und Vernetzung und vermehrtes Homeoffice entstehen mehr Angriffsmöglichkeiten. Oft sind Unternehmen nicht ausreichend geschützt. Besonders häufig und existenzbedrohend sind Ransomware-Angriffe, die die gesamte IT verschlüsseln. Die Täter versenden Erpresserschreiben und drohen oftmals mit der Veröffentlichung von sensiblen Daten. Zudem werden Daten von Sicherheitslücken in Firmen im Darknet verkauft. Deshalb sollte man sich nicht nur fragen, ob man angegriffen wird. Es ist eher die Frage, wann man angegriffen wird.

Was tun Sie, um das Bewusstsein zu schärfen?

JG: In Zusammenarbeit mit Kammern und Verbänden laden wir zu Präventionsveranstaltungen ein. IT-Fachleute und auch Chefs informieren sich. Besonders wichtig ist der Bereich Social Engineering. Wer das Bewusstsein der Mitarbeiter schärft, verringert das Risiko, dass unbedarft sensible Daten weitergegeben werden oder unachtsam Schadsoftware installiert wird.

Können Firmen in der Prävention finanziell entlastet werden?

JG: Viele Unternehmen sind bereit, Geld für ihre IT-Sicherheit auszugeben. Besonders technische Maßnahmen wie regelmäßige Updates, Segmentierung der Netzwerke, ein guter Virenschutz und ein Datensicherungskonzept inklusive eines funktionierenden Backups sind wichtige Maßnahmen, die viel Geld kosten. Wir empfehlen staatliche Förderprogramme, wie den ERP-Digitalisierungs- und Innovationskredit der Kreditanstalt für Wiederaufbau (KFW) oder das Go-Digital-Förderprogramm des Bundeswirtschaftsministeriums.

Was sollten Firmen nach einem Angriff tun?

JG: Erstmal müssen sie die Ruhe bewahren und möglichst das betroffene System vom Netz trennen. Anschließend ist es wichtig, die IT-Abteilung oder Dienstleister sowie die Zentrale Ansprechstelle Cybercrime (ZAC) im zuständigen Landeskriminalamt zu informieren. Im besten Falle liegt ein Notfallplan in Papierform vor. Er enthält Rufnummern und beschreibt weitere Schritte. Die ZAC nimmt Anzeigen auf und steht der IT beratend zur Seite. Sie wird sich für die forensischen Datensicherung eng mit der IT abstimmen. |

Die Fragen stellte Jens Seemann

→ Verträge, Rechnungen, Personaldaten, Lagerbestände oder Bilanzen – alle Daten der sieben betroffenen Unternehmen sind verschwunden.

Vor Anja Bauer und ihrem Team liegt ein riesiger Knoten, den es aufzulösen gilt. Immer wenn sie an einem Ende zieht, um eine Aufgabe zu erledigen, kommen fünf neue Aufgaben hinzu. Für die Umsetzung der dringendsten Entscheidungen und Maßnahmen vergehen zehn Tage. Ein Mix aus vielem Nachdenken und wenig Schlaf. Immer wieder Anrufe und E-Mails, um nur keine Idee zu vergessen.

Ein Team überprüft über 1.000 IT-Geräte auf ihre Speicherfähigkeit. Sie werden zurückgesetzt oder vernichtet. Mit flachen Hierarchien gelingt die Bildung einer weiteren Gruppe aus Mitarbeitern unterschiedlichster Bereiche. Gemeinsam entwickeln sie einen Plan für die neue Softwareinfrastruktur. Denn eines ist in der komplizierten Lage positiv. Sie bietet die Möglichkeit der Modernisierung und Optimierung.

Auch von Seiten der Behörden wird die Notlage erkannt. Mit pragmatischen und unbürokratischen Lösungen beschleunigen sie den Neustart. Im laufenden Geschäft werden alle sieben Firmen der Gruppe abgemeldet. Zwei neue entstehen. Mit Gesellschafterverträgen, Konten und Gewerbeanmeldungen. Mitarbeiter werden übernommen. Bestände werden herausgekauft. Anja Bauer atmet auf, als die Firmen am 1. Juli erstmals wieder digitale Daten erfassen.

Über 16 Monate ohne weitere Angriffe sind vergangen. Die Chefin zieht ein positives Fazit: „Das war alles schlimm und echt stressig. Aber wir haben es als Team gemeistert. Jeder war da, als er gebraucht wurde." | JENS SEEMANN

Links

Auf diesen Seiten finden Sie Infos zum Thema IT-Sicherheit

Allianz für Cybersicherheit
www.allianz-fuer-cybersicherheit.de

Mittelstand-Digital Zentrum Hamburg
www.kompetenzzentrum-hamburg.de

Bundeskriminalamt (Abteilung Cybercrime)
www.bka.de

Routenplaner Cybersicherheit für Handwerker (ZDH)
www.bit.ly/46griYE

FOTOS: HFR/ ADOBE STOCK

Maßnahmen nach einem Angriff

Die Bewältigung eines Cyber-Angriffs ist individuell. Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt diese Fragen.

- ☐ Bewerten Sie den Vorfall. Liegt ein technisches Problem oder ein Angriff vor?
- ☐ Haben Sie Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- ☐ Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- ☐ Haben Sie stets die zeitkritischen und vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- ☐ Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt?
- ☐ Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
- ☐ Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
- ☐ Wurden die beim Cyberangriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-)Prozessen durch relevante Maßnahmen adressiert und behoben?
- ☐ Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten etc.) benachrichtigt?
- ☐ Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene Accounts überprüft?
- ☐ Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
- ☐ Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

Quelle: www.allianz-fuer-cybersicherheit.de

Vorbereitet sein und zielgerichtet handeln

Kleine und mittlere Unternehmen geraten immer stärker ins Visier von Cyberkriminellen. Zwar gibt es keine absolute Sicherheit vor **Attacken aus dem World Wide Web.** Doch mit Prävention und durchdachtem Krisenmanagement lassen sich im Ernstfall Schäden begrenzen.

Ein erfolgreicher Cyberangriff kann für betroffene Betriebe massive, sogar existenzbedrohende Folgen haben. Es ist Ausdruck unternehmerischer Verantwortung, sich ernsthaft mit dem Thema auseinanderzusetzen und einen Notfallplan für den Fall der Fälle aufzustellen. Ein Maßnahmenkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) gibt einen Überblick, wie ein solcher Plan aussehen könnte.

VORBEREITUNG

Die nachfolgenden Aufgaben sollten Sie bearbeiten, um im Fall der Fälle geeignet auf einen IT-Notfall vorbereitet zu sein:

- Bestimmen Sie Beauftragte für die Belange der IT-Sicherheit und des Notfallmanagements in Ihrem Unternehmen.
- Stellen Sie sicher, dass Ihnen Ihre individuellen Erstmaßnahmen bei IT-Vorfällen vorliegen (u. a. Alarmierungs- und Meldewege im Unternehmen).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, bei welcher Art von IT-Vorfällen diese unterstützen können.
- Identifizieren und kontaktieren Sie ggf. weitere IT-Dienstleister, die Sie bei der Bewältigung unterstützen können.
- Fertigen Sie eine Liste mit Ansprechpartnern und deren Erreichbarkeiten und Verfügbarkeiten an.
- Legen Sie Regeln zur Kommunikation nach innen und außen fest, Stichwort: Presse- und Öffentlichkeitsarbeit.
- Implementieren Sie aktive Überwachungsmaßnahmen (Monitoring) für Ihre IT-Landschaft. Beachten Sie den Datenschutz.
- Üben Sie IT-Notfallszenarien jeglicher Art und lassen Sie ihre IT-Infrastruktur auf Angreifbarkeit prüfen .
- Lassen Sie Ihre IT-Infrastruktur auf Angreifbarkeit prüfen (Penetrationstests).
- Schulen und sensibilisieren Sie Ihr gesamtes Personal im Umgang mit den IT-Systemen und Cyberbedrohungen sowie zum Verhalten im Notfall.
- Denken Sie an grundlegende Schutzmaßnahmen:
  - Installieren Sie regelmäßig und unverzüglich Patches und Sicherheitsupdates.
  - Setzen Sie Programme zum Schutz vor Schadsoftware ein und aktualisieren Sie diese regelmäßig.
  - Nutzen Sie Firewalls, um Ihre Netze und Rechner vor Angriffen von außen zu schützen.
  - Ändern Sie in jedem Fall Standard-Passwörter und nutzen Sie sichere Passwörter und, wenn möglich, Zwei-Faktor-Authentisierung.
  - Erstellen Sie regelmäßig Sicherheitskopien (Backups) Ihrer Daten, und testen Sie regelmäßig deren Wiederherstellung.
- Inventarisieren Sie Ihre IT-Infrastruktur (unter anderem Netzplan).
- Vergeben Sie restriktive Benutzerrechte an Ihren Systemen.
- Vernetzen Sie Ihre Systeme restriktiv (Netzsegmentierung).
- Bereiten Sie Meldewege für externe Meldepflichten vor (Datenschutz, KRITIS etc.).

BEREIT SEIN

Um jederzeit einem IT-Notfall begegnen zu können, beachten Sie die nachfolgenden Punkte:

- Überprüfen Sie regelmäßig den Sicherheitsstatus Ihrer Systeme.
- Gewährleisten Sie, dass Ihr Personal den richtigen Ansprechpartner für IT-Notfälle kennt (Einsatz der IT-Notfallkarte). Bestimmen Sie einen angemessenen Erstkontakt für IT-Notfälle und gewährleisten Sie die Erreichbarkeit.

BEWÄLTIGUNG

Zur Bewältigung eines IT-Notfalls helfen Ihnen die folgenden Punkte:

- Kontaktieren Sie alle Ansprechpartner in der Organisation, die Sie zur Bewältigung brauchen.
- Befragen Sie betroffene Nutzer über Beobachtungen und Aktivitäten.
- Kontaktieren Sie IT-Dienstleister, die Ihnen bei der Bewältigung helfen können.
- Sammeln und sichern Sie Systemprotokolle, Logdateien etc. Die Daten sind für eine forensische Auswertung (auch Strafanzeige) essentiell.
- Dokumentieren Sie Sachverhalte, die mit dem Notfall in Zusammenhang stehen könnten.
- Prüfen Sie Kontaktaufnahmen mit den Zentralen Ansprechstellen Cybercrime (ZAC) der Polizeien sowie freiwillige Meldungen an die Allianz für Cyber-Sicherheit (ACS): www.allianz-fuer-cybersicherheit.de.
- Vermuten Sie als Urheber einen fremden Nachrichtendienst, wenden Sie sich an die Verfassungsschutzbehörden in Ihrem Bundesland oder an das Bundesamt für Verfassungsschutz.
- Beachten Sie Meldepflichten.

NACHBEREITUNG

Ein aufgetretener IT-Notfall muss auch nachbereitet werden. Hinweise geben die folgenden Punkte:

- Schließen Sie konsequent alle durch den IT-Notfall aufgedeckten Schwachstellen und Sicherheitslücken in Ihrer IT-Infrastruktur.
- Überwachen und Monitoren Sie Ihr Netzwerk und Ihre IT-Systeme im Nachgang besonders gründlich.
- Lessons Learned: Überprüfen Sie bestehende Regelungen, Prozesse und Maßnahmen, optimieren Sie diese gegebenenfalls.
- Halten Sie Ihre Dokumentationen zum Notfallmanagement auf dem aktuellen Stand.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur – Systeme, Netzwerke und Dokumente kontinuierlich weiter.

Hinweis: Bei dieser Übersicht handelt es sich um eine Kurzfassung des vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten „Maßnahmenkatalogs zum Notfallmanagement – Fokus IT-Notfälle". Der komplette Maßnahmenkatalog steht zum kostenlosen Download bereit unter dem Kurzlink: https://is.gd/Notfallmanagement.

ILL.: ADOBE STOCK

Auf alles vorbereitet sein. Hundertprozentige Sicherheit vor Cyberangriffen gibt es nicht. Entscheidend ist es, den Kriminellen vorbeugend ihr „Geschäft" so schwierig wie möglich zu machen und sich auf den Notfall vorzubereiten.