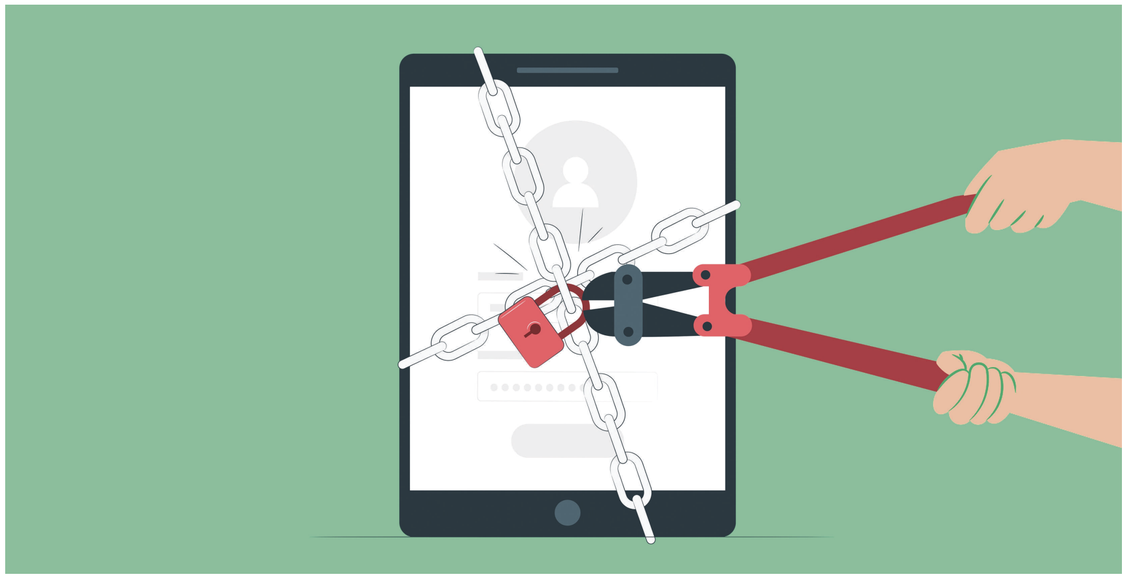
Serie



Mittelstand als Sorgenkind

Kleine und mittlere Unternehmen stehen immer wieder im Fokus von Cyberkriminellen. Was sind die größten IT-Schwachstellen der Firmen – und was können sie dagegen tun?

Von Ulrich Hottelet

Die Gefährdungslage im Cyberraum ist vor allem wegen des russischen Angriffskriegs so hoch wie nie. Diese Einschätzung traf das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Lagebericht 2022. Sorge bereitet den Fachleuten besonders der Mittelstand, denn er ist oft schlechter gerüstet gegen Angriffe als Großunternehmen.

Als größte aktuelle Bedrohung gelten Ransomware-Angriffe. Das sind Attacken auf Unternehmen und andere Organisationen mit dem Ziel, Lösegeld zu erpressen. Einen solchen Fall gab es zuletzt bei dem Hamburger Abfallentsorgungsunternehmen Otto Dörner.

Im Januar 2022 stellte die Firma bei einer Wartung der Systeme fest, dass immer mehr Dateien eine kryptische Endung als Dateityp hatten. Datenbanken und Anwendungsdateien liefen nicht mehr. Die meisten Windows-Systeme waren verschlüsselt.

„Wir fanden eine Textdatei der Täter mit dem Titel ‚How to decrypt' und eine typische Ransomware-Nachricht", berichtet IT-Leiter Stefan Stelling. Mittels Forensik fand man heraus, dass der Angriff über ein kompromittiertes Nutzerkonto eines Dienstleisters erfolgt war, der über keine Zwei-Faktor-Authentifizierung verfügte.

Lösegeld sollte nicht gezahlt werden

„Die Täter wollten eine siebenstellige Summe per Bitcoin erpressen", sagt Stelling. Er schaltete die Cyberkriminalitätsabteilung des Landeskriminalamts Hamburg ein. Schnell war man sich einig, dass kein Lösegeld gezahlt werden sollte. Da die Entschlüsselung zu lange gedauert hätte, kam es darauf an, Zeit zu gewinnen, um eine neue IT-Landschaft mit einem höheren Sicherheitsniveau aufzubauen. „Ich habe mich in der Kommunikation mit

Tim Berghoff ist führender Sicherheitsberater von G Data, einem Anbieter von IT-Sicherheitslösungen. Das Bochumer Softwarehaus brachte 1987 das weltweit erste kommerzielle Antivirenprogramm auf den Markt.

© freepik.com/Montage: tsp: G Data

den Tätern dumm gestellt, um sie hinzuhalten. Zum Beispiel tat ich so, als wüsste ich nicht, wie man Bitcoin überweist", sagt Stelling.

Zwei Monate lang zog sich der Nachrichtenaustausch mit den Angreifern hin, deren IP-Adressen aus dem Baltikum stammten. Schließlich starteten die Kriminellen eine massive DDoS-Attacke auf die Website mit einem Datenverkehr von 4 Gigabit.

Die 350 LKWs der Firma konnten zum Glück weiter täglich fahren, auch wenn die Planung teilweise händisch statt digital gemacht werden musste und die Telekommunikation einige Tage lang nicht funktionierte. Großteils konnte der Geschäftsbetrieb also weiterlaufen. Den finanziellen Schaden kann der IT-Leiter daher nicht beziffern.

Täter setzen oft mehrere Druckmittel ein

Ransomware-Angriffe wie bei der Firma Otto Dörner sind auch nach Einschätzung von Tim Berghoff weiter ein großes Problem für die deutsche Wirtschaft. Er arbeitet als führender Sicherheitsberater von G Data, einem Anbieter von IT-Sicherheitslösungen. Das Bochumer Softwarehaus brachte 1987 das weltweit erste kommerzielle Antivirenprogramm auf den Markt. Die meisten Kunden heute sind kleine und mittelständische Unternehmen.

„Inzwischen sind Unternehmen weniger bereit, Lösegeld zu bezahlen", sagt Berghoff. Das hat zum Trend der Double Extortion geführt. Dabei setzen die Täter mehrere Druckmittel für die Erpressung ein. Neben der Unbrauchbarmachung der Firmendaten durch Verschlüsselung ist die Veröffentlichung von Geschäftsgeheimnissen und sensiblen Daten besonders geschäftsschädlich.

Bei der Double Extortion kopieren die Angreifer daher meist geschäftskritische Daten vor der Verschlüsselung. Im Verlauf der Erpressung wird dann mit der Veröffentlichung oder Versteigerung dieser Informationen gedroht.

Die Täter gehen oft ähnlich vor: „Erst sehen sie sich als legale Nutzer im System um und forschen es aus. Zum Beispiel wollen sie herausfinden, wer die Kunden des Unternehmens sind", sagt Berghoff. Interessant seien dabei vor allem Dienstleister von Großunternehmen, da sie den Zugriff auf deren Netze ermöglichen können. Zu diesem Zweck werden seit Jahren Phishing-Mails verschickt, die Mitarbeiter täuschen sollen.

Viele Mittelständler vernachlässigen das Thema

Fachleute in der IT-Sicherheit warnen bereits seit vielen Jahren insbesondere den Mittelstand vor Versäumnissen und empfehlen Schutzmaßnahmen. Dennoch wird das Thema von vielen Mittelständlern immer noch vernachlässigt oder nur halbherzig angegangen. „Die Unternehmen fragen zuerst: Was kostet das?", sagt Berghoff.

Selbst wenn sie Sicherheitsprodukte kaufen und einsetzen wollen, werden diese oft schlecht konfiguriert oder nicht genutzt. „Doch dann nutzt die teuerste Firewall nichts", sagt Berghoff. Oft liegt es in kleinen Firmen auch an der unzureichenden personellen Kapazität, der Fachkräftemangel ist auch hier spürbar.

„Meist ist es kein technisches Problem, sondern ein organisatorisches", sagt Berghoff. Zum Beispiel werde oft Warnungen des IT-Systems vor Auffälligkeiten nicht nachgegangen. Dann können Angriffe nicht rechtzeitig erkannt werden, um größere Schäden zu vermeiden.

Fachmann Berghoff hat einige wichtige Tipps für Mittelständler. „Am Anfang sollte die Bestandsaufnahme stehen: Welche Daten sind die Kronjuwelen, zum Beispiel Geschäftsgeheimnisse, Kundendatenbanken oder Mitarbeiterdaten? Wo liegen diese Daten? Welche Mitarbeiter dürfen darauf zugreifen?". Zu beachten ist auch das Rechtemanagement: Wer sind die Administratoren? Sind es möglicherweise zu viele? Oft werde auch die Abschaltung der Nutzer-Accounts von früheren Mitarbeitern vergessen, berichtet Berghoff. Das kann Angreifern Einfallstore öffnen.

Regelmäßige Back-ups sind Pflicht

Besonders wichtig sei es auch, regelmäßig Sicherungskopien der Firmendaten anzulegen. „Back-ups sind Pflicht", sagt Berghoff, „wer keines hat, darf im Schadensfall nicht auf Mitleid hoffen." Ein Klassiker unter den Tipps für Unternehmen und Privatnutzer sind gute Passwörter mit einer Mischung aus Buchstaben, Zahlen und Sonderzeichen. Zudem sollte man sie regelmäßig wechseln.

Gerne geraten wird auch zur Verschlüsselung von geschäftskritischen Daten und Mails. „Verschlüsselung ist sehr sinnvoll, aber vielen zu aufwendig. Sicherheit ist immer ein Trade-off zwischen hohem Schutzniveau und Bedienfreundlichkeit. Da muss man einen Kompromiss finden", so Berghoff. Schließlich nützen die besten Sicherheitsregeln der IT-Abteilung wenig, wenn die Mitarbeiter sie nicht umsetzen, weil sie ihnen zu umständlich sind.

Trainings für Mitarbeitende
Aufmerksam gegen Gefahren

Es soll Unternehmen geben, die beim Thema Cybersicherheit auf drakonische Methoden setzen: Beim ersten falschen Klick gibt es ein Gespräch mit dem Chef, beim zweiten mit der Personalabteilung, beim dritten droht die Kündigung. Dabei werden die Mitarbeitenden mittels simulierter Phishing-Mails in die Falle gelockt. Das Simulieren von Cyberangriffen ist eine Trainigsmethode, um Mitarbeitende aufmerksamer für kriminelle Einflussnahme zu machen.

Laut dem Sicherheitsindex 2022 der Initiative Deutschland sicher im Netz e.V. (DsiN), der sich mit der IT-Gefährdungslage von Onlinenutzern befasst hat, waren Verbraucher zuletzt schlechter vor Cyberangriffen geschützt als in den acht Jahren zuvor. Die Angriffe im Netz hätten einen neuen Höchstwert erreicht, so die Initiative. Im Durchschnitt benötigten zwei Drittel aller Verbraucher zusätzliche Hilfestellungen im Netz.

Und das zeigt sich auch am Arbeitsplatz – eine ganzheitliche Aufklärung über den sicheren Umgang mit digitalen Tools ist unabdingbar. Dabei können entsprechende Awareness-Trainings helfen, in denen die gängigen Betrugstricks aufgezeigt werden und bei denen dann mit unechten Angriffen getestet wird, wie das Gelernte Anwendung findet. Schulungen und Trainings sind allerdings keine einmalige Sache, sondern müssen regelmäßig durchgeführt werden. Experten empfehlen zudem eine Kultur der Offenheit, also einen aufgeschlossenen Umgang mit Cybercrime-Risiken – und eben nicht die Androhung von Strafen.

IT-Sicherheitstipps für Unternehmen auf einen Blick

1 Machen Sie Cyber-Sicherheit zur Chefsache.

2 Erhöhen Sie die Cyber-Resilienz durch Übungen.

3 Managen Sie Cyber-Risiken: Prüfen Sie ständig die Bedrohungslage.

4 Sichern Sie Ihre Daten: Legen Sie Back-ups an und testen diese.

5 Nehmen Sie die Mitarbeiter mit: Regelmäßige Schulungen sind wichtig.

6 Patchen Sie schnell mit Sicherheitsupdates.

7 Nutzen Sie die Infos des BSI.

(Ulrich Hottelet)

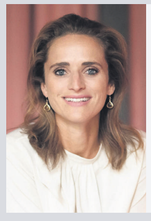
Netzwerke regelmäßig prüfen

Doch nicht immer reicht das: Methoden wie das „Pig Butchering", bei dem Angreifer über soziale Netzwerke Kontakt zu ihren späteren Opfern aufnehmen und ein Vertrauensverhältnis aufbauen, seien auch deshalb so gefährlich, weil der Ansatzpunkt von üblichen Angriffsmethoden abweiche, erklärt Rüdiger Kirsch von Allianz Trade.

Sicherheitsmechanismen wie Inhaltskontrollen von Internetseiten oder Mailüberwachung als erste Linien der Verteidigung würden damit komplett ausgehebelt. „Daher sollten Unternehmen ihre Firmennetzwerke regelmäßig auf eine mögliche Infiltration überprüfen und Sicherheitslücken schließen", sagt Kirsch. „Wirksam sind auch Einschränkungen auf den Endgeräten, die verhindern, weitere Software von Drittanbietern zu installieren." *Johannes Steger*

ANZEIGE

Das Briefing für Digitalisierung & KI



„Ein richtiger Deep Dive in Digital- und Datenpolitik. Wenn du den mal ein halbes Jahr gelesen hast, dann bist du drin."

Verena Pausder, Gründerin, Digitalexpertin und Host des Podcasts FAST & CURIOUS

Jetzt kostenlos testen

Jeden Morgen ab 6 Uhr – per E-Mail und im Webportal.
Die vierwöchige Leseprobe endet automatisch.

background.tagesspiegel.de

TAGESSPIEGEL BACKGROUND

Tagesspiegel Background
Das Fachbriefing für entscheidende Köpfe. Morgens ab 6 Uhr

Jetzt kostenlos testen:
background.tagesspiegel.de

TAGESSPIEGEL BACKGROUND