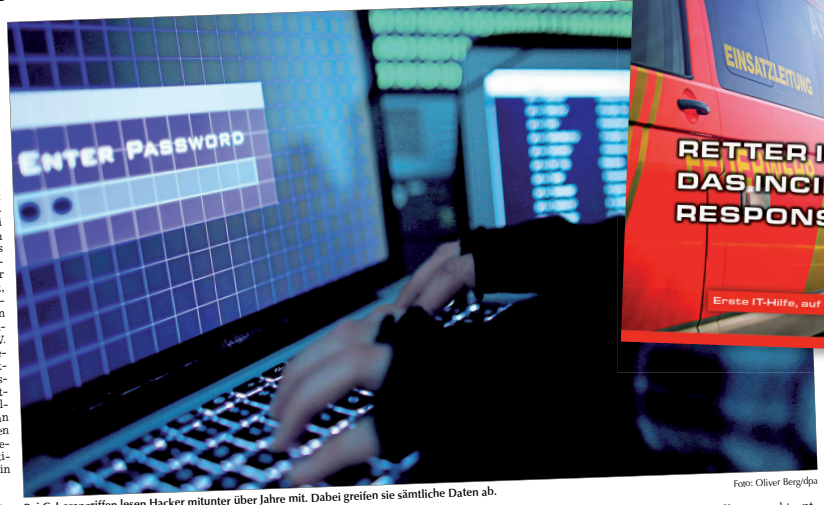
PRESSECLIPPING

Straubinger Tagblatt/Landshuter Zeitung, 29.01.2024

Wenn Hacker den Betrieb lahmlegen

Cyberangriffe sind stark verbreitet. Auch in Ostbayern sind immer wieder Unternehmen betroffen. Im Interview erklärt ein IT-Experte, worauf die Angreifer aus sind und was ihnen hilft



Bei Cyberangriffen lesen Hacker mitunter über Jahre mit. Dabei greifen sie sämtliche Daten ab. Foto: Oliver Berg/dpa

Sie schleichen sich ein, lesen unbemerkt mit: E-Mails, Aufträge, Abbuchungen von Konten – über Wochen, Monate oder Jahre. Dann schlagen die Hacker plötzlich zu. Computerbildschirme bleiben dunkel. Der Betrieb steht still.

Bei Cyberangriffen verschaffen sich Kriminelle Zugriff auf Computersysteme anderer, um ihre Daten zu stehlen und Systeme lahmzulegen oder zu zerstören. Diese Angriffe im Internet haben zugenommen: Vor einer Woche wurde ein Hackerangriff auf Microsoft öffentlich, bei dem Daten von Managern gestohlen wurden. Auch in Ostbayern gibt es immer wieder Vorfälle, wie der Systemausfall der Online-Dienste der Handwerkskammern (hwk) zeigt, der auch die hwk Niederbayern-Oberpfalz betrifft. Der Grund: ein Malware-Angriff im Rechenzentrum des IT-Dienstleisters ODAV. Die Firma mit Sitz in Straubing bestätigte dies auf Nachfrage. Bei Attacken wie dieser wurde das IT-System mittels einer schädlichen Software außer Gefecht gesetzt. Wie solche Angriffe ablaufen und wie man sich davor schützen kann, haben wir den IT-Spezialisten Patrick Hieber, Bereichsleiter für Informationssicherheit in der IS4IT GmbH in Oberhaching, gefragt.

Wie groß ist die Gefahr durch Cyberangriffe wirklich, Herr Hieber?

Patrick Hieber: Cyberangriffe sind eine sehr konkrete Gefahr, die die Geschäftsführung beschäftigen sollten, weil sie das Alltagsgeschäft enorm stören können. Die Angriffe können einerseits Produktivitätsausfälle zur Folge haben, weil man im Betrieb womöglich über Wochen nicht richtig arbeiten kann. Andererseits können sie zum Verlust der Reputation führen, wenn Daten extern verfügbar sind. Das ist besonders kritisch, wenn Mitbewerber Einblicke in wichtige Unterlagen erhalten.

Patrick Hieber ist IT-Experte. Foto: Hieber

Sind große Unternehmen für Angreifer attraktiver als mittelständische Betriebe?

Hieber: Die Größe eines Unternehmens ist nicht entscheidend. Es trifft sehr große Konzerne und genauso den Mittelstand. Allerdings sind größere Firmen meist technisch besser aufgestellt als mittelständische. Bei Letzteren fehlt oft noch einiges an Infrastruktur. Hier sind die Einfallstore offener und die Angreifer haben weniger Widerstände, sich im Netzwerk zu bewegen. Typischerweise fallen die Angriffe im Mittelstand erst auf, wenn etwas nicht mehr funktioniert.

Wie merkt man, dass man gehackt wurde?

Hieber: Wenn es großflächige Ausfälle von Systemen gibt und diese nicht durch einen technischen Defekt erklärbar sind, ist ein Cyberangriff wahrscheinlich. Dieser kann auch unbemerkt stattfinden, ohne große Störungen. Über eine sehr lange Zeit werden Daten nach außen transportiert. Das zu erkennen ist sehr schwer, denn dafür benötigt man eine gute Sichtbarkeit in der IT-Umgebung.

Worauf sind die Angreifer aus?

Hieber: Bei der Wahl ihres Ziels schauen die Angreifer, welche Art von Daten das Unternehmen besitzt. Je sensibler die Daten, umso mehr sind sie wert. Deshalb sind Krankenhäuser ein gerngesehenes Ziel. Wenn Patientenakten, also hochkritische Daten, in die falschen Hände kommen, hat man einen starken Hebel. Wenn die Daten weg sind, sind sie weg.

Bietet Künstliche Intelligenz ganz neue Möglichkeiten für Cyberangriffe?

Hieber: Cyberkriminalität ist global gesehen ein sehr lukrativer Markt. Die Angreifer sind inzwischen sehr gut organisiert. Auf der einen Seite gibt es bei Angriffen durch Ransomware (Anm. d. Red.: eine Art von Malware, die auf Erpressung abzielt und Daten verschlüsselt oder den PC sperrt) jene, die die reine Technologie als Plattform anbieten. Denn: Ransomware kann man – wie einen Cloudservice – für eine Zeit mieten. Andererseits gibt es jene, die diese Software ausnutzen, um Firmen zu erpressen. Und natürlich werden die Möglichkeiten der Künstlichen Intelligenz (KI) genutzt, denn mit ihr werden die Programme für den Angriff umgeschrieben. Man kann sich das wie ein Virus vorstellen, das sich weiterentwickelt: Die Standardimpfung passt nicht immer, deshalb muss sich der Impfstoff anpassen. Auch unsere Reaktion muss sich jedes Mal anpassen.

Wie läuft ein Cyberangriff ab?

Hieber: Zunächst erfolgen Phishing-Attacken. Dafür werden beispielsweise Zugangsdaten über fehlgeleitete Links in Mails abgegriffen. Der Angreifer schaut die Daten im gehackten System durch und formuliert bei Ransomware-Angriffen seine Lösegeldforderung – denn hierbei geht es nur um Erpressung. Aber es gibt auch Angriffe, die auf Zerstörung abzielen: Der Angreifer möchte das Unternehmen komplett außer Betrieb setzen, sodass es für Wochen nicht mehr produzieren und liefern kann oder insolvent wird. In dem Fall setzt sich der Angreifer überall an die wichtigen Stellen des Netzwerks, löscht die kritischen Daten auf allen Systemen und macht die Backups funktionsunfähig. Dann steht man mit nichts da.

Gibt es ein Zeitfenster, um den Schaden zu begrenzen?

Hieber: Bei einem klassischen Ransomware-Angriff hat man ein Zeitfenster. Der Angreifer möchte ja, dass das Lösegeld gezahlt wird. Natürlich muss man das erst einmal beschaffen, das dauert. Zudem muss der Geschädigte das volle Ausmaß realisieren. Dabei ist die Lösegeldforderung nie beliebig gestaltet, sondern am Jahresumsatz der Firma orientiert. Das Unternehmen soll schließlich zahlen können. Die Erpresser nutzen für das Lösegeld keine Überweisungen. Typischerweise läuft das über Kryptowährungen wie Bitcoins ab, die später in Dollar und Co. umgewandelt werden.

Sollte Lösegeld gezahlt werden?

Hieber: Lösegeld sollte man keinesfalls zahlen. Das ist auch die Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI). Aber die Lösegeldforderung kann man nutzen, um sich Zeit für die Wiederherstellung der gehackten Systeme zu verschaffen. Grundsätzlich ist nicht gewährleistet, dass man den Zugriff auf die Daten zurückbekommt, wenn man zahlt. Dabei sind die Ransomware-Angriffe so gestaltet, dass die Wiederherstellung technisch funktioniert, da deren Geschäftsmodell hinfällig wäre, wenn sich das herumspricht. Doch es gibt eine große Dunkelziffer an Unternehmen, die stillschweigend die Lösegeldforderung bezahlen. Nicht jeder meldet solch einen Angriff den Strafverfolgungsbehörden oder dem BSI.

Wie gehen Sie vor, wenn Sie gerufen werden?

Hieber: Kein Einsatz ist gleich und man kann sich darauf nur bedingt vorbereiten. Zunächst gibt es kurzfristig einen Termin mit unseren Experten. Bei diesem wird geklärt, was über den Vorfall und die Systeme bekannt ist. Die Art des weiteren Vorgehens hängt dann von der Art und Schwere des Angriffs ab. Es kann sein, dass sich unser Notfallteam kurzfristig auf den Weg macht, um vor Ort so lange zu arbeiten, bis der Kunde wieder hergestellt ist oder wir die Restarbeiten von unserem Firmenstandort aus abschließen können. Dass wir zum Kunden fahren, ist aber nicht in jedem Fall erforderlich, wenn beispielsweise nur ein Teil der Firma betroffen ist. Die Spezialisten des Notfallteams beenden ihren Einsatz mit einem Plan, wie man in den Normalzustand übergehen kann. Die Wiederherstellung macht entweder der Kunde mit der eigenen IT oder wir unterstützen mit Kollegen aus anderen Abteilungen. Besser wäre es jedoch, entsprechende Schutzmaßnahmen im Vorfeld zu ergreifen.

Interview: Christine Henze

4 TIPPS GEGEN ANGRIFFE

Ständige Passwortwechsel unnötig: Anstelle des regelmäßigen Wechsels von Passwörtern empfehlen Experten ein komplexes Passwort, das mit Multi-Faktor-Authentifizierung abgesichert wird.

Externe Systeme mit Bedacht auswählen: Alle Systeme, die eine Firma von externen Anbietern nutzt, sind potenzielle Ziele für Angriffe. Dazu gehören auch Systeme, mit denen sich Mitarbeiter aus dem Homeoffice in die Firma verbinden.

Inventarisierungsliste deckt Sicherheitslücken auf: Unternehmen wissen oft gar nicht, welche Systeme und Komponenten bei ihnen im Einsatz sind. Dabei kann eine Inventarisierungsliste helfen, Sicherheitsrisikos rechtzeitig zu erkennen und zu minimieren.

Software-Updates einspielen: Veraltete Programme auf Computern und anderen Geräten sind ein Sicherheitsrisiko. Deshalb sind Updates wichtig, die viele Hersteller regelmäßig anbieten. Man kann sie auch automatisch einspielen lassen. (che)

Milliarden Euro Schaden durch Cyberangriffe

Die Zahl der Hackerangriffe ist hoch. Das Bundeskriminalamt registrierte für 2022 deutschlandweit knapp 137 000 Fälle von Cyberkriminalität. Die Schäden daraus beliefen sich dem Digitalverband Bitkom zufolge auf 203 Milliarden Euro – das ist beinahe doppelt so hoch wie 2019. „Generell kann sich niemand darauf verlassen, dass er ‚zu klein' oder ‚zu unbedeutend' für (...) einen Angreifer ist", sagt Dr. Kai Engelbrecht, Ministerialrat der Geschäftsstelle des Bayerischen Landesbeauftragten für den Datenschutz, auf Nachfrage.

Viele Angriffe werden jedoch gar nicht erst öffentlich. Dies bekräftigt die Aussage von Dr. Engelbrecht: „Die Meldungen von Pannen im öffentlichen Bereich nehmen kontinuierlich zu, allerdings stellen Cyberangriffe nur einen kleinen Teil unter den meldepflichtigen Ereignissen." Dennoch müssen Unternehmen folgendes beachten: Wenn personenbezogene Daten durch den Angriff in fremde Hände gekommen sind, muss das dem Bundesamt für Sicherheit in der Informationstechnik gemeldet werden. Ab Kenntnisstand haben die Betriebe dafür maximal 72 Stunden Zeit. Danach können Strafen verhängt werden, die prozentual an den Unternehmensumsatz gekoppelt sind. Cyberkriminellen drohen Gefängnis oder Geldstrafen. Die Paragrafen 202a, b, c im Strafgesetzbuch erschweren derzeit aber auch die Arbeit von Programmierern und Co., die Sicherheitslücken schließen wollen. Noch in der ersten Jahreshälfte soll es jedoch laut Koalitionsvertrag einen Gesetzentwurf geben, demnach das „Identifizieren, Melden und Schließen von Sicherheitslücken legal durchführbar sein" soll. (che)

Berichtigung

In dem Artikel mit dem Titel „Zwischen Vergangenheit und Zukunft", der am Freitag, 26. Januar, erschienen ist, hieß es, dass dem Holocaust allein in Deutschland 17 Millionen Menschenleben zum Opfer gefallen wären. Das ist falsch. Tatsächlich hat das Regime des Nationalsozialismus laut wissenschaftlichen Schätzungen etwa 17 Millionen Menschen getötet, allerdings nicht nur auf deutschem Gebiet. (red)