Foto: James Thew/Adobe Stock ©
Nichts geht mehr – immer öfter werden Firmen Opfer von Hackerangriffen

---

Die Produktion lahmgelegt, die Firmendaten verschlüsselt – Cybercrime-Attacken bedeuten ein gewaltiges Bedrohungspotenzial für Betriebe. Wie können sich Unternehmen gegen solche Gefahren wappnen?

Josef Stelzer, Ausgabe 11/2021

Die Angriffe mit Ransomware und anderen Schadcodes, von Onlineviren bis hin zu Spionagesoftware, häufen sich. Allein 2020 erfasste das Bundeskriminalamt (BKA) rund 108 000 Delikte – 7,9 Prozent mehr als 2019. Oft sind Unternehmen das Ziel. Dem BKA zufolge gehörte einer der größten deutschen Computerspielanbieter zu den Opfern, ebenso ein Automobilzulieferer sowie ein börsennotierter Lebensmittelproduzent. Dabei dürfte die Zahl der nicht angezeigten Attacken aus dem Netz weitaus höher liegen als die von den Behörden registrierten Fälle. Die Schäden für die Wirtschaft sind jedenfalls gigantisch. Nach Schätzungen des IT-Branchenverbands Bitkom dürften es etwa 223 Milliarden Euro pro Jahr sein – Tendenz steigend. Doch die Risiken, die durch Cybercrime drohen, lassen sich eindämmen. Zum einen durch moderne Sicherheitstechnik, zum anderen durch ein gesteigertes Gefahrenbewusstsein in den Unternehmen.

In den Betrieben gewinnt das Thema Cybercrime denn auch immer mehr an Bedeutung. »Die Zahl von Anfragen für Beratung und Schulungen steigt bei uns jedenfalls massiv an«, sagt **Caroline Eder** (45), Geschäftsführerin des Bayerischen Verbands für Sicherheit in der Wirtschaft (BVSW).

Schock: auch alle Sicherungskopien verschlüsselt

Anna Klinke, Geschäftsführerin der Hardy's Freizeit Sport & Event GmbH in Greifenberg, kennt die Gefahren, die im Internet lauern. Im Dezember 2019 wurde ihr Unternehmen, das westlich von München fünf Fitnesscenter betreibt, Ziel eines Ransomware-Angriffs: »Sämtliche Firmendaten mit allen Kundeninformationen wurden auf einen Schlag verschlüsselt, sodass wir keinerlei Zugriff mehr hatten«, erinnert sich die 30-jährige Firmenchefin. »Das war ein Schock, zumal auch alle Sicherungskopien verschlüsselt und damit gesperrt waren.« Die Erpresser versprachen nach Zahlung von knapp 50.000 Euro per Bitcoins einen Entschlüsselungscode.

Nach Rücksprache mit den Behörden und Verhandlungen mit den Erpressern im Darknet, dem für gängige Browser unsichtbaren Teil des Internets, entschloss sich die Unternehmerin schließlich zur Zahlung von 20.000 Euro. »Freunde haben uns mit Bitcoins ausgeholfen, da wir kein Konto mit Digitalwährung eingerichtet hatten«, sagt Klinke, die nach der Bitcoin-Überweisung eine Datei mit dem Entschlüsselungscode erhielt.

Hohe Investition nötig

Die Unternehmerin zog Konsequenzen aus der Attacke: Sie ließ die IT-Sicherheitstechnik komplett modernisieren und zum Beispiel eine Firewall als Brandmauer gegen Onlineangriffe installieren. Die Kosten summierten sich auf insgesamt rund 100.000 Euro. »Der Aufwand lohnt sich, denn damit ist unser System mit wichtigen Daten und Anwendungen nun gut abgeschirmt«, so Klinke.

Vorsichtsmaßnahmen sind angesichts der wachsenden Risiken notwendig, meint **Boris Bärmichl** (55), Vorstandsmitglied des BVSW. Ein unbedachter Klick auf einen scheinbar harmlosen Link dient oft schon als Türöffner für Schadsoftware, die Daten für Erpressungsversuche verschlüsselt oder Firmengeheimnisse ausspäht. Mancher Schadcode hinterlässt keine Spuren und ist nur schwer aufzuspüren. Zudem sind digitale Schädlinge häufig so programmiert, dass sie eine Zeit lang im infizierten Netzwerk bleiben, ohne weiter aufzufallen. Währenddessen spioniert der Schadcode das ganze Netzwerk aus und lädt Schritt für Schritt weitere Schadsoftware nach. »Ich erlebe immer wieder, wie verwundbar gerade die kleinen und mittelständischen Unternehmen gegenüber Cybercrime-Attacken und deren Folgen sind«, sagt der Sicherheitsexperte.

Er rät zu einem Notfallplan, wie nach Computerausfällen und Ransomware-Angriffen vorzugehen ist (siehe IHK-Service "Bausteine" unten) und welche rechtlichen Risiken drohen, etwa wegen Vertragsstrafen infolge von Lieferverzögerungen. »Man sollte zur Sicherheit auch mindestens zwei verschiedene E-Mail-Accounts nutzen«, ergänzt Bärmichl. Wenn nämlich beide Accounts gleichzeitig dieselbe Mail erhalten, könne dies auf einen Onlineangriff hinweisen.

»Ein ganz wichtiger Baustein für den wirksamen Schutz gegen Cybercrime«, so der Sicherheitsexperte, »sind gut geschulte Mitarbeiter, die wissen, welche Gefahren in E-Mail-Anhängen und Links lauern können, vor allem wenn es sich um unbekannte Absender handelt.«

Mehr Informationen zur Vorbereitung auf IT-Notfälle gibt es auf der IHK-Website.

IHK-Service: Bausteine für einen IT-Notfallplan

Wie können Unternehmen für den Ernstfall eines IT-Ausfalls vorsorgen? Der Bayerische Verband für Sicherheit in der Wirtschaft (BVSW) rät zu folgenden Maßnahmen:

- Kernprozesse im Unternehmen mit möglichen Ausfallszenarien erfassen
- Schäden von IT-Ausfällen und mögliche Folgeschäden definieren
- Gesetzliche Vorgaben für Notsituationen beachten

- Interne und externe Mitarbeiter bestimmen, die für die Wiederherstellung der IT-Systeme sowie für die Leitung im Notfall verantwortlich sind
- Ausgewählte Beschäftigte den Krisenstäben und Notfallteams zuordnen
- Handbücher für Computer und Software, Lizenzverträge, Lage- und Raumpläne sowie andere relevante Dokumente sammeln und sichern
- Sämtliche Systeme und Geräte erfassen, die für den IT-Wiederanlauf wichtig sind – zum Beispiel Anwendungen, Schnittstellen und Computer –, sowie organisatorische Maßnahmen festlegen
- Die IT-Infrastruktur mit den unternehmenskritischen Prozessen verknüpfen und Wiederanlaufprozeduren erstellen: Insbesondere Backups so verwalten, dass diese auch nach einem Angriff nutzbar sind

---