AUS SCHADEN LERNEN

Cyber-Kriminalität – wenn ein Link Geld erpresst

Ausgabe 1/2022

Das Bewusstsein für die Risiken eines Cyberangriffs ist bei kleinen und mittelständischen Unternehmen durchaus vorhanden. Allerdings überwiegt die Hoffnung, dass sie es nicht selbst trifft. Dabei nimmt die Zahl der Angriffe weiter zu. Oft verschaffen sich Hacker über die einfachste Schnittstelle Zugang zum Unternehmen – das E-Mail-Postfach. 100-Prozent-Schutz gegen einen Angriff gibt es leider nicht. Der Verlust von sensiblen Daten oder auch nur ein einziger Klick auf eine infizierte E-Mail – aus einem Cyber-Angriff können Ansprüche im hohen sechsstelligen Bereich entstehen. Weitere Gefahr: Ist das Computersystem mittels sogenannter Ransomware (englisch: ransom = Lösegeld) lahmgelegt, kann nicht mehr gearbeitet werden, bis eine bestimmte Geldsumme gezahlt wird oder IT-Spezialisten die Schadsoftware entfernen können.

Beispiel 1 – Angriff durch Ransomware

Ein Mitarbeiter eines Sportartikel-Unternehmens klickt versehentlich auf einen E-Mail-Anhang. Das Computersystem wird von einer Schadsoftware befallen und am nächsten Tag sind alle Programme und Dateien auf dem Server und auf dem Daten-NAS-System mit der Endung „.pysa“ verschlüsselt. Auf dem Bildschirm des PC erscheint der Hinweis, dass die Entschlüsselung der Dateien nur gegen die Zahlung von zwei Bitcoins – zum Zeitpunkt der Forderung ca. 80.000 Euro – erfolgt.

Zwei Tage lang kann weder im Ladengeschäft noch im dazugehörigen Onlinehandel gearbeitet werden.

Der Inhaber des Unternehmens wendet sich sofort an die Experten der Mannheimer Firmen-Cyberversicherung. Und weil es den Profis der Hotline gelingt, die Schadsoftware zu entfernen, kann die Lösegeldzahlung vermieden werden.

Schadenhöhe: 15.500 Euro – wurden vollständig von der Firmen-Cyberversicherung übernommen

- Soforthilfe wie telefonische Krisenunterstützung, Empfehlungen zur Schadenbegrenzung und technische Sofortmaßnahmen — 2.500 Euro
- Entfernen der Schadsoftware und Entschlüsselung der Programme und Daten, zwei Tage IT-Dienstleister — 5.000 Euro
- Ersatz der Kosten für Betriebsausfall und Ersatz des Ertragsausfalls — 8.000 Euro

AUS SCHADEN LERNEN

Cyber-Kriminalität – wenn ein Link Geld erpresst

Beispiel 2 – Laptop im Zug vergessen

Auf einer Geschäftsreise lässt der Mitarbeiter eines Schmuckhändlers das Firmen-Laptop mit vertraulichen Kundendaten versehentlich im Zug liegen. Das Laptop findet „neue Besitzer", die die 1.000 auf dem Gerät gespeicherten Kundendaten auslesen. Diese werden für fingierte Rechnungen mit falscher Kontonummer genutzt und die Kunden erhalten Rechnungen für Waren, die sie nie bestellt hatten.

Die DSGVO sieht in so einem Fall vor, dass alle betroffenen Kunden vom Schmuckhändler informiert werden müssen.

Schadenhöhe: 6.500 Euro – abgedeckt durch die Mannheimer Firmen-Cyberversicherung

- Soforthilfe – Empfehlungen zur Schadenbegrenzung und technische Sofortmaßnahmen — 2.500 Euro
- Schriftliche Information an die 1.000 Kunden gem. DSGVO, Kosten pro Brief 4 Euro — 4.000 Euro

Was ist Ransomware?

ransom = engl. und bedeutet „Lösegeld". Das zu erpressen ist das Ziel der Täter. Mithilfe einer Schadsoftware wird der Computer gesperrt oder sämtliche Dateien auf dem Rechner verschlüsselt.
Der Nutzer bemerkt die Schadsoftware oftmals durch einen blockierten Bildschirm oder durch einen „Erpresserbrief", der sich nicht mehr schließen lässt. Es gibt auch Schadsoftware-Varianten, die eine gewisse „Inkubationszeit" haben. Die Wirkung tritt erst später auf, so dass nicht mehr nachvollzogen werden kann, wann und wie die Schadsoftware auf das System gelangt ist.

Wie wird Ransomware verbreitet?

Häufig werden über manipulierte Websites Links per E-Mail versendet oder sind in sozialen Netzwerken zugänglich. Getarnt in der E-Mail als vermeintliche Rechnung, Lieferschein oder Gewinnbenachrichtigung soll beim Opfer Aufmerksamkeit geweckt werden. Wird der Link geklickt, installiert sich die Schadsoftware.

So schützt man sich vor Ransomware

- **Backups**

Regelmäßige Backups (Datensicherungen) erstellen, die auf einem vom System getrennten Speichermedium aufbewahrt werden. Dieses sollte nach Sicherung der Daten offline geschaltet werden.
Dabei muss geprüft werden, ob das erstellte Backup auch zur Wiederherstellung der Systeme/Daten genutzt werden kann.

- **Aktuelles Betriebssystem**

Das Betriebssystem wie auch der Browser sowie jede genutzte Software sollten regelmäßig aktualisiert werden, um Sicherheitslücken zu schließen.

- **Browser-Schutz**

Schützt vor gefährlichen sogenannten Skripten (= Liste von Befehlen, die von einem bestimmten Programm ausgeführt werden) und dem versehentlichen Download von Schaddateien.

- **E-Mail-Schutz**

Eine Sicherheitssoftware stellt potenziell trügerische E-Mails bereits im Posteingang fest.

- **Ransomware-Cleaner**

Wird durch eine Schadsoftware der Bildschirm blockiert, gibt es die Möglichkeit, die Blockierung aufzuheben und die Schadsoftware zu entfernen.

- **Nutzerkonten**

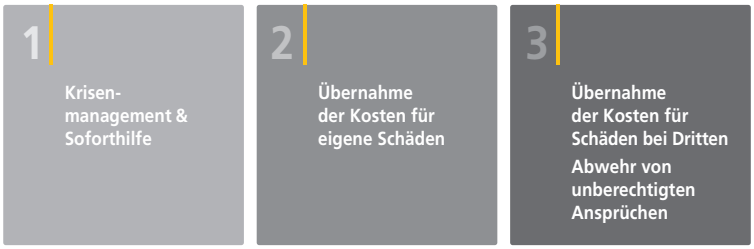
System-Admins sollten sich nicht mit ihrem umfänglichen Admin-Account, sondern besser als „normaler Benutzer" anmelden. Ein normaler Benutzer hat weniger Rechte – Ransomware kann dadurch nicht so tief ins System eindringen bzw. richtet weniger Schaden an.

AUS SCHADEN LERNEN

Cyber-Kriminalität – wenn ein Link Geld erpresst

Argumente für den Vertrieb

- Machen Sie das Cyber-Thema zu Ihrem Thema und erläutern Sie Ihren Kunden zum Beispiel die Risiken durch Ransomware.
- Stellen Sie Ihren Kunden die drei Bausteine der Mannheimer Firmen-Cyberversicherung vor:



Weitere Informationen

- Produktinformation Firmen-Cyberversicherung für Vertriebspartner
- Im Fadenkreuz von Hackern – Aus Schaden lernen-Artikel 01/2021
- Bleiben Sie dauerhaft auf dem Laufenden und abonnieren Sie den 14-tägigen Newsletter „Sicher informiert" auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit aktuellen Sicherheitslücken und wichtigen Ereignissen in der IT-Sicherheit.
- Broschüre des Bundesamts für Sicherung in der Informationstechnik (BSI) „Schadprogramme – So schützen Sie sich"
- Broschüre des Bundesamts für Sicherung in der Informationstechnik (BSI) „Hinweise zur Sicherheitsrichtlinie nach § 75b SGB V" für Ärztinnen und Ärzte, Psychologinnen und Psychologen, Zahnärztinnen und Zahnärzten

Mannheimer Versicherung AG

Augustaanlage 66
68165 Mannheim
Telefon 06 21. 4 57 80 00
Telefax 06 21. 4 57 80 08
service@mannheimer.de
mannheimer.de

ASL 0322