AUS SCHADEN LERNEN

Im Fadenkreuz von Hackern – kleine und mittelständische Unternehmen

Ausgabe 1/2021

Jeder zehnte Betrieb war bereits von einem Cyber-Angriff betroffen. Und die meisten der Cyber-Angriffe erfolgten bei kleinen und mittelständischen Unternehmen über Anhänge oder Links in E-Mails. Trotz dieser hohen Zahl sind viele dieser Unternehmen immer noch schlecht vorbereitet. Im Ernstfall fehlen Verantwortliche für IT-Sicherheit, Notfallpläne oder entsprechende vertragliche Vereinbarungen mit IT-Dienstleistern. Dabei können tagelange Betriebsausfälle und Schadenersatzforderungen durch Lieferverzug oder Datenmissbrauch schnell Kosten in Höhe von mehreren zehntausend Euro erreichen.

Hackerangriff legt Hotelbetrieb lahm

Der Bildschirm des Computers am Hotelempfang wurde schwarz. Nichts ging mehr. Es erschien die Nachricht, dass alle Daten verschlüsselt wurden und ein Lösegeld von 1.500 Euro gefordert wird. Die Hacker hatten Tage zuvor durch mit einem infizierten Link in einer E-Mail das Hauptsystem des Hotels angegriffen. Die Mitarbeiter hatten keinen Zugriff mehr auf Gästedaten, das Hotelzimmer-Schließsystem, die Rechnungserstellung oder den Warenbestand. Die letzte Datensicherung wurde ebenfalls verschlüsselt. Es bestand keine Cyberversicherung. Der Hotelier konnte sich nicht mehr anders helfen und hat das Lösegeld bezahlt. Der Schaden für ihn betrug ca. 15.000 Euro. Das Lösegeld mit 1.500 Euro ist dabei einer geringsten Kostenblöcke gewesen.

Mit einer Cyberversicherung der Mannheimer wären diese Kosten übernommen worden:

■ Soforthilfe wie telefonische Krisenunterstützung, Empfehlungen zur Schadenbegrenzung und technische Sofortmaßnahmen	3.000 Euro
■ Wiederherstellen von Daten	5.000 Euro
■ Daten von 800 Gästen fielen den Hackern in die Hände. Darüber mussten die Betroffenen gemäß DSGVO informiert werden. Kosten pro Info-Brief: 5 Euro.	4.000 Euro
	12.000 Euro

Durch die schnelle Hilfe wäre die Zahlung des **Lösegelds vermieden worden**.

Neben der Kostenübernahmen für den Hotelier mindestens genauso wichtig: Die Mannheimer hätte die gesamte Schadenabwicklung begleitet und dem Hotelier eben auch z. B. die Computersysteme zeitnah wieder entschlüsselt.

AUS SCHADEN LERNEN

Im Fadenkreuz von Hackern – kleine und mittelständische Unternehmen

Nichts geht mehr, die Produktion steht still

Hacker griffen mithilfe einer per E-Mail versandten, manipulierten Konstruktionsdatei auf das Produktionssystem eines mittelständischen Metallteileherstellers zu. Die Produktion stand trotz der sofortigen Hilfe der Cyber-Experten für drei Tage still. Wichtige Aufträge konnten nicht termingerecht erfüllt werden. Eine Firmen-Cyberversicherung bestand.

Schadenhöhe: 46.500 Euro

Die Leistungen der Firmen-Cyberversicherung:

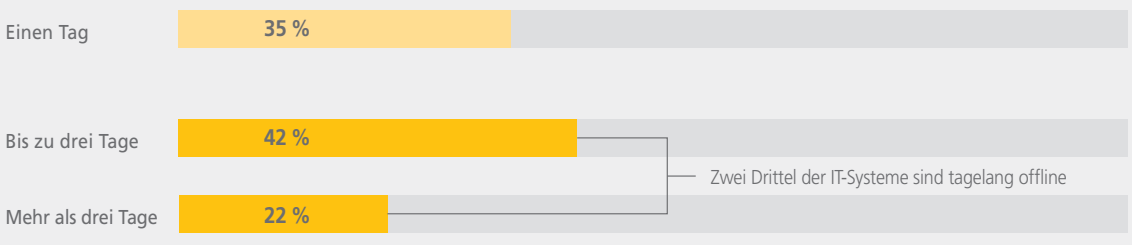
Soforthilfe wie telefonische Krisenunterstützung, Empfehlungen zur Schadenbegrenzung und technische Sofortmaßnahmen	6.500 Euro
Entfernen der Schadsoftware und Wiederherstellen der Produktionssoftware	15.000 Euro
Ersatz der Kosten für den Betriebsausfall und Ersatz des Ertragsausfalls	25.000 Euro
	46.500 Euro

Das unterschätzte Risiko – viele kleine und mittelständische Unternehmen (KMU) sehen sich nicht gefährdet

- Viele Verantwortliche bei KMUs denken irrtümlich, Cyberangriffe seien über die Sach- und Haftpflichtversicherungen abgedeckt.
- Von niedrigen IT-Sicherheitsstandards bei KMUs versprechen sich Cyber-Kriminelle höhere Erfolgschancen.
- In KMUs fehlt oftmals das Bewusstsein über den Wert eigener Daten und die Zunahme der Digitalisierung im eigenen Unternehmen.
- Faktor Zeit: Nach einem Hackerangriff versuchen KMUs entstandene Probleme selbst zu lösen. Es vergehen Tage, bis IT-Spezialisten beauftragt werden. Die Eindämmung der Folgen und die Wiederherstellung der Daten werden dadurch deutlich erschwert.
- Der mögliche Reputationsverlust wird unterschätzt.

Die IT-Systeme wieder zum Laufen zu bringen, kann dauern ...

Wie lange hat es gedauert, die IT-Systeme wiederherzustellen und die Schadsoftware zu beseitigen?



Quelle: GDV

Cybersecurity – diese 10 Sicherheitsstandards sollten alle Unternehmen haben

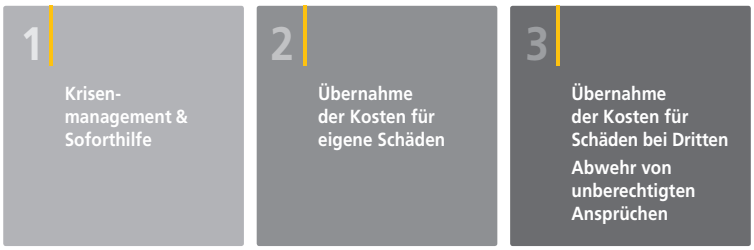
1. Antivirenprogramm auf aktuellstem Stand
   Ein absolutes Muss, wenn mehrere Mitarbeiter an einem Computer oder in einem Netzwerk arbeiten.
2. Wöchentliche Datensicherung
   Sogenannte Ransomware-Trojaner verschlüsseln Daten, die meist verloren sind. Mindestens wöchentliche Sicherungskopien erstellen. Diese Kopien extern verwalten/aufbewahren.
3. Manipulationen der Sicherungskopie verhindern
   Backups/Datensicherungen sind die Rückversicherung im Fall gelöschter oder manipulierter Daten. Daher sollten sie physisch getrennt aufbewahrt werden.
   Experten raten zur 3-2-1-Regel: Drei Kopien aller kritischen Daten sollten auf mindestens zwei unterschiedlichen Medien liegen – auf der Festplatte, der CD oder im Cloudspeicher. Und mindestens eine Kopie sollte außerhalb des Unternehmens gelagert werden – um zu verhindern, dass zum Beispiel ein Brand im Büro oder eine Überflutung alle Datenträger vernichtet.
4. Daten der Sicherungskopie testen
   In regelmäßigen Abständen prüfen, ob mithilfe der Sicherheitskopien die Daten auch tatsächlich wiederhergestellt werden können.
5. Updates und Sicherheitspatches schnell einspielen
   Automatisierte Update-Funktionen zum Einspielen von Updates für Betriebssysteme und Programme auf keinen Fall deaktivieren.
6. Firmen-Server mit Firewall sichern
   Software zur Sicherheitsüberwachung (Security Monitoring) oder zur Erkennung von Eindringlingen (Intrusion Detection) stärken die Sicherheit des eigenen Netzwerks.
7. IT-Administratorenzugänge einrichten und sparsam nutzen
   Administrator-Profil mit gesondertem Passwort nur zum Einrichten neuer Programme oder für Betriebssystemkonfigurationen nutzen.
   Für die alltägliche Arbeit Profile mit weniger Rechten nutzen. Im Falle eines eingeschleusten Virus kann dieser ohne Administratorenzugang weniger Schaden anrichten.
8. Individuelle Mitarbeiterzugänge einrichten
   Jeder Mitarbeiter verfügt über einen eigenen Benutzer-Account mit eigenem Passwort. Administratoren können genau definieren, wer welche Nutzungsrechte erhält. Im Falle eines Angriffs kann zurückverfolgt werden, wie der Eingriff ins Netzwerk erfolgte.
9. Komplexe Passwörter einsetzen
   Einfache Passwörter sind noch immer „Türöffner" für Hacker.
   Das Bundesamt für Sicherheit in der IT empfiehlt:
   – mindestens acht Zeichen
   – Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern
   – keine Namen von Familienmitgliedern, besten Freunden, Haustieren oder deren Geburtsdaten
   – keine gängigen Varianten und Wiederholungs- oder Tastaturmuster wie z. B. „qwertz" oder „1234abcd"
10. Mobilgeräte sichern
    Oft werden Firmendaten außerhalb des Betriebs genutzt, z. B. im Homeoffice. Mobile Datenträger sollten vollverschlüsselt und passwortgeschützt sein.

AUS SCHADEN LERNEN

Im Fadenkreuz von Hackern – kleine und mittelständische Unternehmen

Argumente für den Vertrieb

- Stellen Sie Ihren Kunden folgende Fragen:
  - „Wissen Sie und Ihre Mitarbeiter, wie Sie auf eine Cyberattacke reagieren?"
  - „Ist der Betreuer Ihrer IT-Systeme rund um die Uhr erreichbar?"
  - „Wen rufen Sie Sonntagnachmittag an, wenn Sie mitbekommen, dass in Ihrem Unternehmen ein Cybervorfall im Gange ist?"
- Beschäftigen Sie sich aktiv mit den notwendigen Cybersecurity-Standards für Unternehmen. Sprechen Sie Ihre Kunden auf deren Sicherungen an. Zeigen Sie auf, wie vernetzt und digital auch kleine und mittelständische Unternehmen heute sind.
- Faktor Zeit: Klären Sie Ihre Kunden über die Notwendigkeit der schnellen Schadenmeldung auf. Der Service-Dienstleister mit Cyber-Experten der Mannheimer ist rund um die Uhr erreichbar.
- Stellen Sie Ihren Kunden die drei Bausteine der Mannheimer Firmen-Cyberversicherung vor:



Weitere Informationen

- Firmen-Cyberversicherung: Produktinformation für Vertriebspartner
- Cyber-Sicherheitscheck der deutschen Versicherer – wie gut ist die IT-Sicherheit Ihres Unternehmens?
- Report des GDV, Cyberrisiken im Mittelstand

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 0121