SCHADEN.NEWS


23.08.2023

# ACHTUNG, CYBERANGRIFF: SO SCHÜTZEN SIE IHREN BETRIEB

Vor wenigen Wochen wurden mehrere Kfz-Versicherer Opfer von Cyber-Attacken. Das rückt das Thema Cyber-Sicherheit immer stärker in den Fokus von K&L-Betrieben. Doch zahlreiche kleine und mittelständische Betriebe sind nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) nicht ausreichend vor Attacken aus dem Netz geschützt. Um den Unternehmen ihre offenen Flanken aufzuzeigen, hat das BSI daher einen Ratgeber für KMU herausgebracht. Dieser klärt leicht verständlich über die Gefahren für IT-Systeme auf und gibt Tipps, mit denen sich die Unternehmen besser schützen können. Im Vorfeld ist es demnach für Betriebe wichtig, zu erkennen, dass man sich mit der IT-Sicherheit seines Unternehmens beschäftigen muss. Verantwortlich dafür ist die Unternehmensleitung. Das heißt natürlich nicht, dass dieser das dann selbst komplett durchführen muss – dafür gibt es Dienstleister. Grundlegend sollte sich der Betrieb die Frage stellen, „was passieren würde, wenn bei Ihnen Daten verloren gingen, verändert oder unbrauchbar würden. Bei welchen Daten würden Sie Gefahr laufen, dass Ihr Geschäftsbetrieb beeinträchtigt oder sogar unterbrochen würde?“, heißt es dazu in der Broschüre. Das Bundesamt gibt darin eine Reihe von nützlichen Hinweisen, mit denen kleine und mittelständische Betriebe überhaupt verhindern, Ziel eines Cyberangriffs zu werden. Dazu gehören unter anderem folgende:

## SOFTWARE-UPDATES DURCHFÜHREN

Cyber-Attacken können häufig deshalb entstehen, weil die Angreifer öffentliche Schwachstellen nutzen, um in das IT-System einzudringen. „Es ist wichtig, Betriebssysteme und Anwendungssoftware zu aktualisieren, sobald Sicherheitsupdates von den jeweiligen Herstellern zur Verfügung gestellt werden“, rät das Bundesamt. Viele Anbieter stellen automatische Update-Funktionen bereit, diese

sollten auch aktiviert sein. Alternativ können Betriebe ihren IT-Dienstleister mit der regelmäßigen Aktualisierung der Programme beauftragen. Nicht mehr aktualisierbare Hard- oder Software sollte entsorgt oder deinstalliert werden.

### MAKROS DEAKTIVIEREN

Laut BIS ist ein Haupteinfallstor für Ransomware ein sogenanntes Makro, das sich in Dateianhängen von versendeten E-Mails verbergen können. Öffnet der Nutzer die Datei, fragt ihn das öffnende Programm automatisch um Erlaubnis. Das sollte in den Windows-Gruppenrichtlinien durch den Administrator von vornherein deaktiviert und die Entscheidung keinesfalls den Anwendern überlassen werden. Denn: Die Schadsoftware kann sich auch über Mails von bekannten Absendern verbreiten, ohne das diese davon Kenntnis haben – schlimmstenfalls sind sie selbst schon Opfer der Schadsoftware geworden.

### VIRENSCHUTZPROGRAMME UND FIREWALLS VERWENDEN

Weiterhin kann der Einsatz von Virenschutzprogrammen die IT-Ressourcen schützen und eine Schadsoftware abwehren. Wichtig: Auch diese Programme sollten immer auf dem neuesten Stand gehalten werden, damit sie auch neue Schadsoftware identifizieren können. Einige Virenschutzprogramme werden gleich mit einer Firewall ausgeliefert. Diese sollte auf jeden Fall jedes Unternehmen installieren.

### SICHERE PASSWÖRTER NUTZEN

Dieselben Passwörter für verschiedene Dienste zu nutzen ist ein weit verbreiteter Fehler, der es Angreifern aus dem Netz einfach macht. Deshalb: Für jeden Zweck ein anderes Passwort ausdenken. Dieses sollte mindestens acht Zeichen lang sein und aus Buchstaben, Zahlen und Sonderzeichen bestehen, nicht aus Tastenfolgen wie asdfgh oder 12345 und nicht im Wörterbuch stehen. Zudem sollte, wo möglich, eine Zwei-Faktor-Authentifizierung eingerichtet werden.

### MAILACCOUNTS ABSICHERN

Der häufigste Weg, den Angreifer im Internet nutzen, ist der Mailverkehr. Deshalb sollte laut BSI der Mailbox eines jeden Benutzers im Unternehmen ein Virenscanner vorgeschaltet werden. Zudem ist es wichtig, die Mitarbeiter zu sensibilisieren: „Ein paar einfache Fragen schützen zumindest teilweise vor Angriffen per E-Mail: Ist der Absender bekannt? Erwarten Sie irgendwelche Informationen von ihm? Steht der vorgeschlagene Link im Zusammenhang mit dem erwähnten Thema? Im Zweifelsfall ist es erforderlich, die Echtheit der Nachricht über einen anderen Kanal (Telefon, SMS usw.) beim Absender zu überprüfen“, heißt es dazu in der Broschüre.

### REGELMÄSSIGE DATENSICHERUNG

Vorbeugen ist wichtig: Falls es trotz Sicherheitsmaßnahmen zu einem sogenannten Ransomware-Angriff kommt, bei dem Daten verschlüsselt werden, können betriebliche Aktivitäten schneller wider aufgenommen werden, wenn regelmäßig Datensicherungen durchgeführt werden. Das BSI empfiehlt kleineren Unternehmen im Handwerksbereich, mindestens einmal wöchentlich die Daten zu sichern. Als Speichermedium eignet sich beispielsweise eine externe Fesplatte oder ein Cloud-Dienst. Bei Datenspeicherung in der Cloud oder auf einem mobilen Gerät ist zudem eine Verschlüsselung der Daten angebracht. Weitere Hinweise, wie sich Betriebe nach einem Cyberangriff verhalten sollten, erhalten Sie in der Infobox auf dieser Seite.

Die gesamte Broschüre mit allen hilfreichen Tipps können sich Betriebe auf der Website des Bundesamtes kostenlos herunterladen.

Ina Otto