Cybersicherheit für Handwerksbetriebe

Auch kleinere Handwerksbetriebe können von Cyberattacken betroffen sein

Cyberattacken – die betreffen doch nur große Unternehmen und keine mittelständischen Handwerksbetriebe, denken die meisten. Ein Irrtum: Es kann jeden treffen, auch den eigenen Elektrobetrieb, und der Schaden kann ganz schön groß sein. Da ist es gut, wenn man vorher Vorsorge trifft. Experte Florian Schottenheim von der Firma Partnersoft GmbH gibt Tipps, worauf Handwerksbetriebe achten sollten, um keine Opfer zu werden, und zeigt die Gefahren auf.

Wie angreifbar ein Unternehmen ist, das hängt für Florian Schottenheim vom Grad der Technisierung des Betriebs, seiner Größe und davon ab, wie intensiv EDV genutzt wird.

Ein großes Thema derzeit ist Ransomware. Dabei handelt es sich laut dem IT-Experten um eine Schadsoftware, die Daten abzieht und diese verschlüsselt, sodass das Unternehmen nicht mehr Herr darüber ist und sie nicht mehr nutzen kann. „Derjenige, der die Daten verschlüsselt hat, möchte Lösegeld dafür, dass er sie wieder freigibt“, erklärt der IT-Experte. Dieses Lösegeld kann leicht und locker bis zu 50.000 Euro betragen.

Ob der Betrieb zahlt, hängt davon ab, wie wichtig es ihm ist, dass er seine Daten zurückbekommt. Wer nicht zahlt, bei dem bleibt alles verschlüsselt. Der Betrieb muss laut Schottenheim dann in eine neue Infrastruktur investieren, die Daten sind weg und können im schlimmsten Fall sogar im Darknet zum Verkauf stehen, sodass dies auch den Kunden schadet. Apropos Darknet: „Hier bieten immer mehr Hackergruppen auch Tools zum Verkauf an. Das bedeutet, dass der Kreis jener, die Schaden anrichten können, immer größer wird und somit auch Handwerksbetriebe von den Angriffen betroffen sein können, weil sie einfach zunehmen“, erklärt der Fachmann.

Was tun?

„Die IT-Infrastruktur muss professionell abgeschirmt werden“, nennt Schottenheim als wichtige Maßnahme. Das bedeutet, dass es eine richtig professionelle Firewall braucht, nicht nur die, die in der Fritz!-Box enthalten ist.

„Außerdem muss ein Backup der Daten gemacht werden, am besten unter Verwendung eines Tape-Drives oder Tape-Libraries, auf Datenbänder gesichert, die vom Netzwerk abgekoppelt werden.“ Technisch gebe es viele Möglichkeiten, allerdings ist der größte Schwachpunkt der Mensch selbst: Schottenheim zitiert eine Studie, laut der rund 80 bis 85 Prozent der Cyberangriffe auf Fehlverhalten der Mitarbeiter oder des Chefs zurückzuführen sind.

Ein Beispiel: Eine Phishing-Mail trifft ein und besagt, man soll seine Daten eingeben, damit der E-Mail-Dienst weiterlaufen kann. Oder eine SMS, dass ein Paket in der DHL-Station liegt und man soll ebenfalls Daten eintippen. Und schon hat der Betrüger leichtes Spiel. Es gebe auch Anrufe eines vermeintlichen Microsoft-Mitarbeiters, der einem mitteilt, der Computer sei virenverseucht und es müsse Geld überwiesen werden. Oder in der Buchhaltung wird angerufen, der Vorgesetzte lasse ausrichten, dass sofort an eine bestimmte Firma ein Geldbetrag überwiesen werden muss. Denn oft geht es nicht nur um Daten, sondern auch ums Geld.

Nicht nur Chefsache

Für Florian Schottenheim ist es wichtig, dass alle im Betrieb aufpassen und auch regelmäßig dafür sensibilisiert werden, vorsichtig zu sein. Das Stichwort hier ist „User-Awareness“.

IT-Spezialisten wie auch die Firma Partnersoft bieten derartige User-Awareness-Schulungen an, um den Mitarbeitern und auch dem Chef aufzuzeigen, welche Gefahren es gibt und was man dagegen tun kann. Kommt eine E-Mail, eine SMS oder ein Anruf, der einem komisch vorkommt, dann hat der Experte einen Tipp parat: „Keine Daten eingeben, lieber zweimal zu viel beim angeblichen Unternehmen anrufen, ob die Nachricht wirklich von dort kam.“ Das gilt auch bei USB-Sticks, die mit der Post kommen oder vor der Tür liegen: „Nie einfach in den PC schieben, sondern vorher fragen, ob der Stick wirklich vom angegebenen Absender kommt.“

Passwort ist nicht gleich Passwort

Vorsicht gilt auch bei Passwörtern. Ein gängiges Passwort ist immer noch „12345“. „Und mit diesem Passwort wird auch häufig von Betrügern versucht, sich einzuloggen“, weiß Schottenheim. Er rät: „Komplexe Passwörter verwenden, die nichts mit einem selbst zu tun haben, und Groß- und Kleinbuchstaben und Sonderzeichen miteinander kombinieren.“

Er rät außerdem, einen Passwordmanager zu benutzen und eine Zwei-Faktor-Authentifizierung, bei der man nach einer Anmeldung auch noch per SMS einen Code bekommt, der dann eingetippt werden muss.

Und auch ein Mitarbeiter, der das Unternehmen verlässt – vielleicht sogar im Schlechten -, kann ein Risiko sein. Deshalb ist es wichtig, zum Eintritt eines neuen Mitarbeiters im Unternehmen aufzuzeichnen, welche Zugänge er hat, und diese nach seinem Austritt dann auch wieder zu sperren.

Insgesamt rät Florian Schottenheim darauf, stets die Augen offen zu halten und sich regelmäßig schlau zu machen, welche neuen Formen von Cyberangriffen es gibt. Denn er weiß eines ganz genau: „Prävention ist billiger als ein Schadensfall.“