Was geschieht, wenn Sie morgen nicht mehr an Ihre Unternehmensdaten kommen?

Wenn Ihr Rechner Ihnen mitteilt:

> „Ihr Zugang ist nicht mehr möglich. Um den Zugang frei zu schalten überweisen Sie € 15.000,00 auf das Konto:
> Beispielbank, IBAN: GI22 1234 5678 9012 3456 78.
> Nach Eingang der Zahlung erfolgt die Freischaltung Ihres Zugangs innerhalb von 5 Tagen."

Lassen Sie dieses Szenario ein paar Minuten auf sich wirken.
Was sind die Folgen für Ihr Unternehmen?

Die häufigste Form von Cyber-Angriffen sieht so, oder zumindest sehr ähnlich aus. Laut Studie von Ernst & Young sind die beiden Hauptziele die Erlangung von finanziellen und Wettbewerbsvorteilen.
Ob Sie zahlen oder nicht, spielt fast keine Rolle. Die wenigsten Unternehmen bekommen Ihre Daten zurück. Einmal infizierte Systeme sind grundsätzlich als vollständig kompromittiert zu betrachten und müssen neu aufgesetzt werden. In mehreren bekannten Fällen hatte dies Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke vollständig neu aufgebaut werden mussten.
In Deutschland ist die Gefahr Opfer einer Cyberattacke zu werden hoch und steigt stetig an. In den ersten beiden Quartalen 2017 betrug die Höhe der verursachten Schäden, allein in Deutschland rund 65-Milliarden EURO.
Gefährdet sind aber vor allem jene, die noch nicht wissen, dass sie gehackt wurden. In Deutschland gaben in einer Umfrage 56 Prozent der Firmenchefs an, in ihren Unternehmen gebe es keine konkreten Hinweise auf Cyberangriffe oder einen Datendiebstahl. Weil sie so sicher sind? Oder einfach unwissend?
IT-Experten beantworten die Frage, wie gut deutsche Unternehmen gegen einen Cyberangriff gesichert sind, gerne so: "Es gibt zwei Arten von Unternehmen: Die einen sind gehackt worden. Die anderen wissen es nur noch nicht."
Ungefähr jeder zweite Mittelständler in Deutschland wurde schon von Konkurrenten oder fremden Geheimdiensten bespitzelt - oder vermutet das zumindest. Das geht aus einer Befragung von 583 Unternehmen hervor. Sie ist Teil einer Untersuchung, die das Max-Planck-Institut für ausländisches und internationales Strafrecht gemeinsam mit dem Fraunhofer-Institut für System- und Innovationsforschung und der Polizei erstellt hat.
Die Angriffe ziehen sich quer durch Branchen und Unternehmensgrößen. „Die Ergebnisse dieser, wie auch anderer Befragungen zeigen, dass sich kein Unternehmen sicher fühlen kann", warnen die Autoren. Sie gehen von einer hohen Dunkelziffer aus: Viele Attacken würden auch gar nicht bemerkt und nur rund jedes fünfte betroffene Unternehmen erstatte Anzeige.ennoch hat fast jedes fünfte Unternehmen mit weniger als 50 Beschäftigen der Studie zufolge keine Strategie gegen Schnüffler vor Ort oder gegen Cyberspionage.

„Die Bedrohung durch Spionage besteht gleichermaßen von innen wie von außen", schreiben die Forscher. „In vielen Fällen stammt der Täter sogar aus dem unternehmerischen Umfeld: seien es eigene (auch ehemalige) Beschäftigte, Beschäftigte von Drittfirmen, Wettbewerber oder gar Kunden. Diese Täter sind besonders gefährlich, können sie doch die Lage des Unternehmens und den Wert der einzelnen zu erlangenden Informationen besonders gut einschätzen." Dabei ließe sich schon mit einfachen Maßnahmen gegensteuern, etwa mit Regeln für das Personal, regelmäßige Prüfung der Sicherheitsmaßnahmen oder Verschlüsselung von E-Mails.
Wer wissen will, in welcher Form Unternehmen schon angegriffen wurden, welche Schäden entstanden sind oder wie sie sich zu schützen versuchen, stößt auf Schwierigkeiten. Reden will darüber eigentlich niemand, schon gar nicht, wenn die eigene Firma betroffen ist, war oder sein könnte.

Effektiver Schutz vor den Folgen von Cyberangriffen ist vergleichsweise günstig realisierbar. Machen Sie jetzt den ersten Schritt zu mehr Sicherheit für Ihr Unternehmen: Fordern Sie jetzt die Bestandsaufnahme ihrer IT-Sicherheit an.

Andreas Lichtenfeld
Eichenstr. 88, 93164 Laaber
www.aggus.de
E-Mail: info@aggus.de

Aktuell: BSI und Allianz für Cybersicherheit warnen erneut vor Emotet.
Was Emotet ist und wie es funktioniert, aber auch wie Sie sich mit einfachen Mitteln einen Grundschutz aufbauen können, erfahren Sie bei uns.

Andreas Lichtenfeld
Eichenstr. 88, 93164 Laaber
www.aggus.de
E-Mail: info@aggus.de