6 Schritte, mit denen Führungskräfte ihr Unternehmen vor Ransomware schützen können

Ransomware-Attacken kosteten US-Unternehmen in 2019 laut Berichten über 7,5 Milliarden Dollar. Anlass zu Sorge und Prävention gibt ebenso der aktuelle BSI-Report zur IT-Sicherheitslage in Deutschland. Auch hier wird Ransomware als eine der maßgeblichen Bedrohungen angesehen. Laut einer von StorageCraft in Auftrag gegebenen Umfrage (Dimensional Research, November 2020) gaben 52 Prozent der Befragten in Deutschland auf die Frage nach ihrer größten Besorgnis hinsichtlich Ransomware-Angriffe an, dass das finanzielle Risiko für ihre Organisation sehr groß ist, sollten sie kompromittiert werden. Der Gesamtschaden innerhalb der letzten zwei Jahre für deutsche Unternehmen in den Bereichen Spionage, Sabotage und Datendiebstahl beträgt laut Bitkom über 205 Milliarden Euro, also über 100 Milliarden Euro pro Jahr. Im Jahr 2017 waren es noch 2017 noch 55 Milliarden Euro.

Die Trends deuten darauf hin, dass Cyberangriffe, Schadsoftware und Ransomware weiter auf dem Vormarsch sind. Die Anzahl der Schadprogramme übersteigt laut BSI inzwischen die Milliardengrenze. Allein zwischen Juni 2019 und Mai 2020 sind 117,4 Millionen neue Varianten bekannter Malware hinzugekommen.

Folglich plagen sich nicht nur IT-Spezialisten, sondern auch verantwortungsvolle Führungskräfte mit Fragen dazu, wie man Ransomware-Angriffe generell vereiteln kann und wie bei einem erfolgreichen Angriff die Zahlung von Lösegeld abgewendet werden kann. Auf diese Sorgen gibt es keine universelle und einfache Antwort. Allerdings können Führungskräfte mit

nur sechs Schritten den Schutz vor Ransomware und vor weiteren Cyber-Gefahren härten und damit einen wesentlichen Beitrag zur Unversehrtheit des Unternehmens leisten:

1. Ransomware- und Sicherheitsaudits durchführen

Auf Security spezialisierte Dienstleister sollten ein Sicherheitsaudit im Unternehmen durchführen, um den tatsächlichen Zustand der Security zu ermitteln. Die Leistungen der Anbieter können dabei von Penetrationstests bis hin zu Schwachstellen-Risikobewertungen und mehr reichen. Es empfiehlt sich, mit Experten, die dem Team nicht bekannt sind, zusammenzuarbeiten. Diese überprüfen das Unternehmen unvoreingenommen und können so Schwachstellen leichter identifizieren.

2. Strategie zur Datensicherung entwickeln

Wer sein Unternehmen von einem externen Spezialisten auf Sicherheitsrisiken prüfen lässt, sollte danach eine detaillierte Liste der Probleme vorliegen haben. Für diese gilt es Lösungen zu finden. Neben einer modernen Firewall und einer leistungsfähigen Endpoint Security, die einer wirkungsvollen und effizienten Data-Safety-Strategie folgt, steht immer die geeignete Backup-Lösung im Zentrum. Denn nur mit einem guten und vor Ransomware geschützten Backup kann den Cyberkriminellen im Ernstfall ein Riegel vorgeschoben werden. Sollte die Expertise im Unternehmen dafür nicht ausreichen, bieten sich Managed Service Provider an, die bei der Planung, Umsetzung und dem Betrieb der Datensicherungsinfrastruktur helfen.

3. Backup- und Disaster Recovery-Plan einrichten

Die meisten Unternehmen legen Backups ihrer Daten an, aber nur wenige haben sich auch überlegt, wie sie diese Daten im Ernstfall wiederherstellen können. Umso wichtiger ist es, konkrete Ziele für die Wiederherstellung von Daten zu definieren, insbesondere RPO (Recovery Point Objective) und RTO (Recovery Time Objective). Beide Wiederherstellungsziele definieren dabei wie schnell das Kerngeschäft eines Unternehmens und dessen IT Systeme nach einem Vorfall wieder online sein müssen, um keinen schwerwiegenden Schaden zu erleiden.

4. Mitarbeiter schulen

Es hilft die beste Soft- und Hardware wenig, wenn ein hohes Sicherheitsrisiko im Unternehmen durch die eigenen Mitarbeiter besteht. Ein Teil der Security-Strategie sollte daher die Schulung der Mitarbeiter sein, um diese für die Gefahren einer Schadsoftware zu sensibilisieren. Viele Unternehmen halten verpflichtende Seminare zum Thema Sicherheit ab, in denen die Mitarbeiter die unterschiedlichen Arten von Cyberattacken, Ransomware-Angriffen, Phishing oder auch Social-Engineering-Methoden kennenlernen.

5. Mitarbeiter und Systeme regelmäßig überprüfen

Regelmäßige Sicherheitsaudits der IT-Struktur sind ebenso wichtig wie die wiederkehrende Prüfung des Sicherheitsbewusstseins bei Mitarbeitern. In der IT ändern sich Konfigurationen ständig und das Risiko, versehentlich ein Einfallstor für Cyberkriminelle zu öffnen ist hoch. Ähnlich verhält es sich bei Mitarbeitern. Neue Mitarbeiter oder die Versetzung an andere Positionen mit anderen Aufgaben können das Security-Bewusstsein im Unternehmen schnell aufweichen. Tests sollten ein regelmäßiger Bestandteil der Sicherheitsstrategie sein.

6. Versicherung für Cybersicherheit abschließen

Die großen Versicherungsgesellschaften bieten inzwischen erschwingliche Cybersicherheits-Policen an. Eine solche Cybersicherheitsversicherung kann auch die Risiken einer Datenschutzverletzung oder eines Datenverlusts aufgrund von Ransomware-Attacken abdecken. In einigen Fällen zahlen Versicherungsgesellschaften sogar Lösegelder, für den Fall, dass kein Datenzugriff mehr möglich ist. Aber Achtung: Das Bezahlen von Kriminellen sollte das absolute „Worst-Case-Szenario“ sein und ist gegebenenfalls sogar strafbar.

Fazit

Die Investition in eine Strategie gegen Cyberattacken wie beispielsweise Ransomware ist nicht nur Kür, sondern Pflicht in jedem Unternehmen. Da es aufgrund von immer häufigeren und raffinierteren Attacken zunehmend um das Überleben von Unternehmen geht – völlig unabhängig von der Unternehmensgröße – steht automatisch auch die Führungsriege in der Pflicht, die Strategie und die nötigen Maßnahmen zu tragen und einzuleiten. Denn selbst wenn im Ernstfall eine Versicherung dabei helfen kann, den finanziellen Schaden in Grenzen zu halten, ist es letztlich auch der Ruf eines Unternehmens, der maßgeblich zum Erfolg beiträgt. Anstatt das Risiko einzugehen Opfer zu werden, ist es daher notwendig, aktiv die nötigen Maßnahmen zu ergreifen, damit Kriminelle ein Unternehmen niemals in die Zange nehmen können.

###

Folgen Sie StorageCraft auf Twitter, LinkedIn und Facebook.
Lesen Sie die neuesten Artikel zum Thema Datensicherung und Datenwiederherstellung im StorageCraft Blog.

Über StorageCraft
Seit fast zwei Jahrzehnten entwickelt StorageCraft fortschrittliche Lösungen für Datenmanagement, -schutz und -wiederherstellung. Zusammen mit Vertriebspartnern stellt StorageCraft sicher, dass mittlere und kleine Unternehmen ihre geschäftskritischen Informationen immer sicher, zugänglich und optimiert halten können. Kunden profitieren von branchenführenden, intelligenten Lösungen für die Datensicherung und -verwaltung, einer konvergierten primären und sekundären Scale-out-Speicherplattform und erstklassigen Cloud-Backup- und DRaaS-Diensten. Unabhängig davon, ob sich ein Unternehmen auf firmeninterne, cloudbasierte oder hybride IT-Umgebungen verlässt, löst StorageCraft die Herausforderungen eines explosionsartigen Datenwachstums und gewährleistet gleichzeitig die Geschäftskontinuität durch erstklassige Schutz- und Wiederherstellungslösungen.
Weitere Informationen finden Sie unter www.StorageCraft.com/de.

Unternehmenskontakt
Jock Breitwieser
StorageCraft Technology Corp.
+1 408.800.5625
jock.breitwieser@storagecraft.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
storagecraft@tc-communications.de
www.tc-communications.de