Cyberkriminalität steigt stark – so schützen Sie sich richtig

Die Coronapandemie hat die Notwendigkeit für ein gutes Sicherheitskonzept drastisch verschärft: Nie gab es so viele Angriffe auf die Wirtschaft, nie waren Hacker so gut organisiert wie heute. Dennoch fehlen in vielen Unternehmen wichtige Bausteine für eine sichere IT-Infrastruktur.

DER AUTOR

André Schmid
Head Sales, Allgeier (Schweiz)

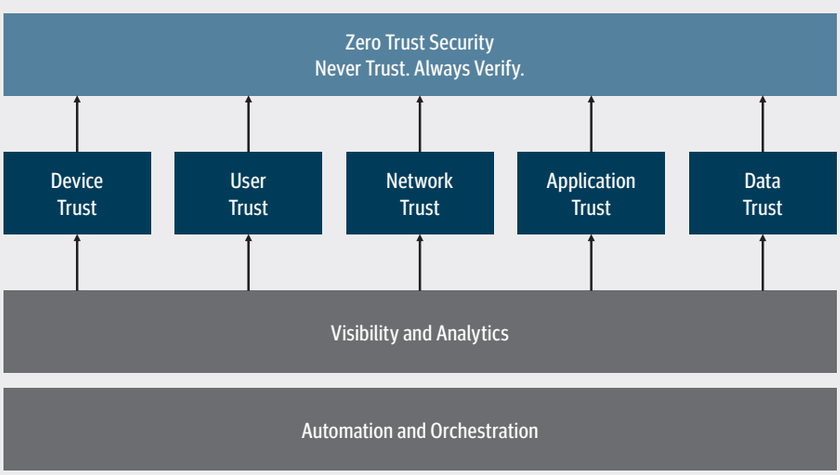
Den Beitrag finden Sie auch online
www.netzwoche.ch

Der Hack des Kassensoftware-Anbieters «Kaseya» im Juli 2021 hat über 1000 Firmen betroffen, Supermarktketten mussten schliessen. Die Nutzerdaten aller «Clubhouse»-User werden im Darknet angeboten, inklusiver aller Kontakte, also auch Millionen Menschen, welche die App nie benutzt haben.

Laut dem Nationalen Zentrum für Cybersicherheit (NCSC) hat sich die IT-Sicherheitslage in der Schweiz im Pandemiejahr 2020 rapide verschlechtert, die Anzahl der gemeldeten Vorfälle hat sich mehr als verdoppelt, wie aus dem Halbjahresbericht hervorgeht. Der Trend ist 2021 ungebrochen. Insbesondere die Angriffe mit Ransomware werden immer professioneller. Viele bekannte Schweizer Unternehmen wurden Opfer und erlitten nicht nur Reputationsschäden, sondern hatten mit Produktionsausfällen zu kämpfen.

Bei unseren Nachbarn sieht es ähnlich aus: Laut einer repräsentativen Umfrage des Deutschen Fachverbands Bitkom unter 1000 Firmen wurden während der Pandemie neun von zehn Firmen von Hackern angegriffen, wie es im Studienbericht vom August 2021 heisst. Der Schaden hat sich mit geschätzten 223 Milliarden Euro pro Jahr mehr als verdoppelt. Einen starken Zuwachs gab es bei Ransomware-Angriffen mit einer Vervierfachung innert 12 Monaten. Wie schützen wir unser Unternehmen am besten? Viele Firmen nutzen die Sicherheitsfunktionen ihrer Cloud-Provider. Das ist ein wichtiger erster Schritt. Ebenso haben viele Unternehmen zertifizierte IT-Prozesse, was eine gute Grundlage ist. Aber eine ISO-Zertifizierung ist kein Garant für gelebte IT-Sicherheit im Alltag.

Erhöhen Sie Ihre IT-Sicherheit durch die Umsetzung der folgenden drei Punkte.



Grafik: Allgeier (Schweiz)

1. Schutz vor Social Engineering mit Security-Awareness-Trainings
Die grösste Angriffsfläche für Hacker sind die Mitarbeitenden und ihr Verhalten. Kontinuierliches Online-Training mit Videos und Kontrollfragen, kombiniert mit simulierten Angriffen auf interne Zielgruppen ist nachhaltig und effektiv. Verschiedene Hersteller bieten Plattformen und Lösungen, die einfach einzuführen und zu verwalten sind. Die Resultate werden laufend ausgewertet und die Hersteller integrieren neue Angriffsformen.

2. Schutz vor Passwort-Diebstahl mit einer Enterprise-Passwort-Management-Plattform
Je nach Quelle lassen sich 70 bis 80 Prozent aller Datendiebstähle auf nachlässige Passwortsicherheit zurückführen. Solange Unternehmen Passwörter in Excel, Word, Onenote oder ähnlichen Plattformen ablegen und diese auch mehrfach verwendet werden, steht das Einfallstor weit offen. Eine Passwort-Management-Plattform verwaltet Passwörter, kontrolliert Zugänge, integriert in existierende Anmeldeverfahren und deckt den Mitarbeiterwechsel ab. Führende Hersteller zeichnen sich durch Zero Knowledge, Einhaltung von GDPR und weiteren Standards aus.

3. Zero-Trust-Architektur und Einsatz spezialisierter Lösungen
Eine Zero-Trust-Architektur ist der Grundpfeiler einer modernen IT-Infrastruktur. Dabei empfehlen wir, die Sicherheitsfunktionen der grossen Cloud-Anbieter (Amazon, Google, Microsoft) gezielt mit Lösungen von spezialisierten Herstellern zu kombinieren. Dies gewährt Unabhängigkeit, sichert den Einsatz von spezifischem Fachwissen und bietet eine optimale Abdeckung der Sicherheitsrisiken.