Cyber Exposure: So können Unternehmen ihre Angriffsfläche erkennen und verringern

Die Digitalisierung im Arbeitsleben erlaubt effiziente Arbeitsmethoden und ein flexibles Geschäftsleben. Mit der Vielzahl an neuen, smarten Geräten im Unternehmensnetz und dem verstärkten Einsatz von Cloud sowie Web-Applikationen ergeben sich neben den enormen Vorteilen auch neue Angriffsflächen für Hacker.

Während sich Assets stetig weiterentwickelten, veränderten sich traditionelle Tools, wie Antivirenprogramme, kaum. Sie decken nach wie vor nur Server, Desktops und Netzwerkinfrastrukturen ab. Doch um die gesamte Angriffsfläche zu erkennen, ist ein neuer, umfassender Ansatz nötig. Um diesen zu beschreiben, hat sich sich der Begriff Cyber Exposure etabliert. Cyber Exposure konzentriert sich darauf, wo Schwachstellen bestehen und wie diese reduziert werden können. Tenable erklärt, wie Unternehmen diesen Ansatz für sich nutzen können, damit moderne, flexible Arbeitsumgebungen sich nicht zum Sicherheitsrisiko entwickeln.

1. Cyber-Risiken erkennen

   IT-Verantwortliche können nur die Geräte und Assets im Netzwerk schützen, die sie auch kennen. Deshalb gilt als höchste Priorität: sämtliche Geräte umgehend identifizieren und durchgängig scannen, um alle Schwachstellen zu finden. Traditionelle Tools wie Firewalls und Antivirus-Software sind isoliert und decken jeweils nur einen kleinen Teil der Angriffsoberfläche ab. Moderne Umgebungen verlangen nach einem umfassenderen Ansatz, der alle Assets in IT, Cloud, IoT (Internet of Things) und OT (Operational Technology) abdeckt.

2. Schwachstellen priorisiert beheben

   Sobald die Schwachstellen bekannt sind, sind diese selbstverständlich zu beheben. Allerdings ist darauf zu achten, welche Schwachstellen den Geschäftsbetrieb besonders stark bedrohen. Erst mit diesem Bezug auf die tatsächlichen Gefahren haben Sicherheitsbeauftragte und Unternehmensleitung die nötigen Daten zur Hand, um relevante Entscheidungen zu treffen: Wo ist das Unternehmensnetzwerk anfällig, welche Schwachstellen sollten aufgrund des geschäftlichen Risikos priorisiert werden, welche sind zunächst weniger wichtig? Und mit welchen Maßnahmen können die Schwachstellen nach und nach reduziert werden? Erst der umfassende Einblick und die Priorisierung der Probleme kann diese Informationen liefern.

Die Digitale Transformation bietet Unternehmen enorme Vorteile, auf sie nicht mehr verzichten können. Die dadurch ausgelöste Beschleunigung mündet allerdings zwangsläufig in neuen Sicherheitsherausforderungen, die nach modernen Strategien verlangen. Nur wenn Verantwortliche die Schwachstellenproblematik systematisch angehen und sich ihrer Cyber Exposure bewusst sind, können sie ihre gesamte Angriffsfläche identifizieren und verringern.