Vier Dinge, die Sie noch nicht über IT-Schwachstellen wussten

Jens Freitag, Security Engineer DACH bei Tenable, stellt vier Erkenntnisse zu Schwachstellen vor.

16.500 – so hoch war die Zahl der 2018 entdeckten Schwachstellen. Ihre Zahl steigt seit Jahren. Zum Vergleich: 2016 lag die Zahl noch bei knapp 9.800, 2017 waren es bereits über 15.000. Dieser Anstieg hat verschiedene Ursachen. Der Hauptgrund ist eine immer komplexere IT-Infrastruktur: Sie vergrößert die Angriffsoberflächen in Unternehmen. Das Ponemon Institute veröffentlichte im Dezember 2018 eine Studie für Tenable, die sich auf Cyberrisiken im Geschäftsbetrieb konzentrierte. Sie förderte einige interessante Erkenntnisse zum Thema Schwachstellen zutage, die wir hier vorstellen.

1. **Personelle Engpässe gefährden die IT-Security**

Eines der Ergebnisse: Die meisten befragten Unternehmen (58 Prozent) haben zu wenig Personal, um zeitnah auf Schwachstellen zu reagieren. Zwar sind im Durchschnitt 19 Mitarbeiterinnen und Mitarbeiter am Schwachstellen-Management beteiligt. Doch reicht diese Zahl nicht aus, und die Fähigkeit auf bekannte Schwachstellen zu scannen leidet. Das zeigt die Frage nach Zeitplänen für Scans: 31 Prozent der Befragten haben keinen festgelegten Zeitplan. Noch schlimmer: 28 Prozent scannen gar nicht.

2. **Die Zahl der Schwachstellen-Scans hängt von der Fähigkeit zu priorisieren ab**

Vom Scan-Verhalten des Unternehmens lässt sich auf den Entwicklungsstand der Cybersecurity-Strategie schließen: Je ausgereifter die Strategie, desto eher planen Unternehmen die Häufigkeit der Scans danach, wie schwerwiegend die aktuellen Cyberrisiken für sie sind und in welchem Umfang ihre sensible Unternehmensdaten gefährdet sind. Für 46 Prozent der Antwortgeber ist die Priorisierung von Cyberrisiken ein Faktor für die Scan-Häufigkeit. 35 Prozent machen die Scan-Häufigkeit davon abhängig, wie sie das Risiko für sensible Daten bewerten. Und für 20 Prozent ist die Sorge um den Geschäftsbetrieb ein Argument für die Zahl der Scans.

3. **Manuelle Prozesse verhindern es, Schwachstellen zu reduzieren**

Die zu dünne Personaldecke wurde bereits angesprochen – hinzu kommt, dass viele Unternehmen Assets und Schwachstellen mit Excel-Tabellen nachverfolgen. Die unterbesetzten Teams müssen Probleme deswegen manuell erkennen und kommen nur langsam voran. 51 Prozent der von Ponemon Befragten gaben zu Protokoll, dass ihre Sicherheitsteams mehr Zeit für manuelle Prozesse aufwenden als darauf, die Schwachstellen zu beheben. Die Konsequenz ist ein wachsender Rückstau, der sich nicht mehr abarbeiten lässt. Ein Ergebnis, das sich positiv deuten lässt: Immerhin fast der Hälfte (48 Prozent) der Umfrageteilnehmer ist bewusst, dass ihr Unternehmen wegen der manuellen Prozesse beim Umgang mit Schwachstellen im Nachteil ist – das Problem ist erkannt.

4. **Unternehmen messen nicht, was Sicherheitsvorfälle kosten**

Ponemon nannte neun Faktoren, auf deren Basis Unternehmen das potenzielle Risiko eines Cyberangriffs quantifizieren können. Über alle Faktoren hinweg gaben nur 41 Prozent der Befragten an, dass sie den Schaden quantifizieren. Dabei bestehen allerdings große Unterschiede: 54 Prozent quantifizieren die Kosten des Diebstahls geistigen Eigentums, 43 Prozent berechnen den finanziellen Verlust, jedoch nur 31 Prozent die Ausfallzeiten von OT-Systemen und 28 Prozent den Verlust von Marktanteilen. Weitere Faktoren waren der Verlust von

Mitarbeiterproduktivität, Häufigkeit nicht gepatchter Schwachstellen, Mitarbeiterfluktuation und der Rückgang des Aktienkurses.

Fazit

Unternehmen sind mit einer wahren Schwachstellenflut konfrontiert und gehen unterschiedlich mit den Risiken um. Oft können Unternehmen mit der richtigen Security-Automatisierung und vorausschauender Priorisierung von Schwachstellen (Predictive Prioritization) ihre Schwachstellenmanagement effizienter gestalten. Das schützt das Unternehmen besser vor Angriffen und entlastet die Security-Mitarbeiterinnen und -Mitarbeiter, die häufig von der schieren Menge der Schwachstellen überfordert sind.