Schwachstellenbewertungen und Penetrationstests der IT-Security sind wichtiger denn je

Ein Kommentar von John Shier, Field CTO Commercial bei Sophos

„Wir haben gut vorgesorgt und ich glaube, dass wir gut abgesichert sind“. Dieser oft ausgesprochene Satz täuscht eine trügerische Sicherheit vor. Denn viele Unternehmen haben zwar in die Cybersicherheit investiert, erfahren allerdings erst im Ernstfall, ob die Sicherheitsresilienz tatsächlich an allen Stellen hält, was sie verspricht. Studien wie der aktuelle Sophos Threat Report zeigen, dass trotz aller Anstrengungen noch zu viele Schlupflöcher für die Cyberkriminellen vorhanden sind. Fast 50 Prozent aller analysierten Schadsoftwarefälle hatten es auf kleine und mittlere Unternehmen abgesehen und 90 Prozent aller Cyberangriffe beinhalten Daten- oder Identitätsdiebstahl. Cyberkriminelle nutzen diese entwendeten Informationen später für weitere Aktionen wie unautorisierten Fernzugriff, Erpressung oder das Installieren von Ransomware. Darüber hinaus sind nicht selten unsichere IoT-Geräte ein Einfallstor für die Cyberkriminellen.

Das Problem sind selten die Sicherheitslösungen, sondern unerkannte Schwachstellen in der IT-Infrastruktur, die ohne eine eindeutige Identifizierung nicht abgesichert werden können. Daher sind regelmäßige Schwachstellenbewertungen als auch Penetrationstests wichtig. Erst sie liefern verlässliche Rückmeldungen über den tatsächlichen Stand der Sicherheit und Cyberresilienz im Unternehmen.

Schwachstellenbewertungen und Penetrationstests haben unterschiedliche Ziele. Laut NIST bieten Schwachstellenbewertungen eine „formale Beschreibung und Bewertung der Schwachstellen eines Informationssystems“, während Penetrationstests eine Methodik verwenden, „bei der Prüfer, die in der Regel unter bestimmten Einschränkungen arbeiten, versuchen, die Sicherheitsmerkmale eines Systems zu umgehen oder zu überwinden“. Erst die Ergebnisse beider Maßnahmen geben Unternehmen Aufschluss über die existierenden Risiken und lassen Rückschlüsse zu, welche Prioritäten bei der Beseitigung dieser Risiken gesetzt werden sollten.
Die Frequenz beider Maßnahmen hängt vom IT-Verhalten des Unternehmens und von gesetzlichen Regeln (z. B. Payment Card Industry) ab. Unternehmen mit geringer technologischer Fluktuation (z. B. Code-Änderungen, Hardware-Upgrades, Personalwechsel, Topologieänderungen usw.) kommen zwar keinesfalls ohne Tests, allerdings mit einer niedrigeren Frequenz aus. Organisationen mit hohem technologischem Wandel steigern ihre Cyberresilienz mit häufigeren Tests.

Stufen der Schwachstellenbewertungen und Penetrationstests
Die Durchführung von Schwachstellenbewertungen und Penetrationstests umfasst zwölf wichtige Schritte – von der Suche über die Bewertung bis hin zur Abhilfe und einer abschließenden Berichterstattung:

1. **Definition des Umfangs:** Klare Definition des Umfangs, einschließlich der zu prüfenden Systeme, Netze und Anwendungen sowie aller spezifischen Ziele oder Vorgaben.
2. **Erkundung:** Sammeln von Informationen über die Zielsysteme, -netzwerke und -anwendungen mit passiven Mitteln, wie öffentlich zugänglichen Informationen und Social-Engineering-Techniken.

3. **Scannen auf Schwachstellen:** Einsatz automatisierter Tools, um die Zielsysteme auf bekannte Schwachstellen, Fehlkonfigurationen und Schwachstellen zu überprüfen. Dies kann sowohl interne als auch externe Scans umfassen.
4. **Bewertung der Schwachstellen:** Analyse der Ergebnisse der Schwachstellen-Scans, um Schwachstellen zu identifizieren und nach Schweregrad, Auswirkung und Wahrscheinlichkeit der Ausnutzung zu priorisieren.
5. **Manuelle Tests:** Durchführung manueller Tests, um die Ergebnisse der automatisierten Scans zu validieren und zu verifizieren und um zusätzliche Schwachstellen zu identifizieren, die von den automatisierten Tools nicht erkannt wurden.
6. **Penetrationstests:** Aktives Ausnutzen von Schwachstellen, um die Sicherheitslage der Zielsysteme, -netze und -anwendungen zu bewerten. Dabei können verschiedene Techniken zum Einsatz kommen, z. B. die Ausnutzung von Netzwerken, Angriffe auf Webanwendungen und Social Engineering.
7. **Post-Exploitation:** Sobald in der Zielumgebung Fuß gefasst wurde, wird die Umgebung weiter erkundet und die Berechtigungen erweitert, um das Ausmaß des potenziellen Schadens zu ermitteln, den ein echter Angreifer verursachen könnte.
8. **Dokumentation:** Erfassen und Zusammenstellen alle Ergebnisse, einschließlich der entdeckten Schwachstellen, der angewandten Ausnutzungstechniken und aller Empfehlungen für Abhilfemaßnahmen oder Schadensbegrenzung.
9. **Berichterstattung:** Erstellen eines umfassenden Berichts sowohl für Sicherheitsverantwortliche als auch das Management mit den Ergebnissen der Bewertung, einschließlich einer Zusammenfassung, technischen Details der Schwachstellen, Risikobewertungen und Empfehlungen für Abhilfemaßnahmen oder Schadensbegrenzung.
10. **Planung von Abhilfemaßnahmen:** Festlegung von Prioritäten und der Planung von Abhilfemaßnahmen auf der Grundlage der Ergebnisse der Bewertung sowie der Risikotoleranz und der geschäftlichen Prioritäten des Unternehmens.
11. **Erneute Bewertung:** Durchführung von Folgebewertungen, um zu überprüfen, ob die Schwachstellen wirksam behoben wurden und um sicherzustellen, dass sich die Sicherheitslage der Systeme, Netzwerke und Anwendungen des Unternehmens verbessert hat.
12. **Kontinuierliche Überwachung:** Implementieren von regelmäßigen Überwachungs- und Testprozessen, um neue Sicherheitslücken zu erkennen und zu beheben, sobald sie auftreten.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de