Automated Vulnerability Management

SCHWACHSTELLEN SYSTEMATISCH SCHLIESSEN

DIGITAL Trust.

Schwachstellen existieren – nicht selten sind es in Unternehmen mehrere hunderttausend. Die kritischen Schwachstellen mit einem handelsüblichen Scanner zu identifizieren, ist einfach – der Prozess, diese anschließend zu schließen, ist aufwendig. Die Zeit dafür drängt jedoch, denn mittlerweile dauert es nur noch 2,5 Tage, bis ein Exploit publik wird. 2013 lag dieser Zeitraum noch bei 60 Tagen – das Patchen muss also deutlich schneller sein, um Angriffe zu vermeiden.

Um die Geschwindigkeit beim Patchen zu erhöhen, haben wir mit Automated Vulnerability Management (AVM) einen intelligenten Lösungsansatz entwickelt, der den gesamten Prozess der Identifikation und Beseitigung von Schwachstellen weitgehend automatisiert. Mit unserem integrierten Patch-Management in hybriden Multi-Cloud-Umgebungen sichern wir Ihr Unternehmen gegen Exploits agil ab. Schwachstellen schließen wir gemeinsam mit Ihren Sicherheitsverantwortlichen im laufenden IT-Betrieb. So erhalten Sie einen automatisierten Remediation Operation Service, der Ihr IT-Budget schont.

VIRTUAL PATCHING – SCHNELLER ALS EIN EXPLOIT

Virtual Patching bessert die Schwachstelle nicht aus, sondern schützt sie gegen bösartige Angriffe. Basis sind Intrusion-Prevention-Systeme, die zur Endpoint Protection oder im Netzwerk eingesetzt werden. Beim Virtual Patching werden auf die Schwachstelle abgestimmte Regeln implementiert, die einen Exploit dran hindern, Netzwerkpfade von und zu einer Schwachstelle zu verwenden. Die Lösung inspiziert und blockiert die bösartigen Angriffe und verhindert so, dass Cyber-Kriminelle erfolgreich eindringen können. Damit ist Virtual Patching eine Ergänzung zu Patch-Management-Lösungen.

ALTERNATIVES PATCHING – BEDROHUNGEN SCHNELL PRIORISIEREN

Ein risikobasierter Ansatz ist das Alternative Patching. Hierbei wird die Angriffsfläche über Firewall-Regeln und Access Control Lists reduziert. Dafür werden zunächst Informationen von Schwachstellen-Scannern gesammelt. Im Anschluss identifizieren geeignete Tools auf Firewalls und Routern die Kommunikationsregeln im Netzwerk. Angriffswege können auf Basis dieser Erkenntnisse simuliert und Schwachpunkte mithilfe eines systematischen, fokussierten Ansatzes beseitigt werden. Wo der simulierte Angriff erfolgreich ist, können direkt Maßnahmen erfolgen – beispielweise das Ändern von Kommunikationsregeln auf den Netzwerkkoppelelementen.

SICHERHEITSLÜCKEN AUTOMATISIERT ERKENNEN UND BEHEBEN

Im Rahmen des Automated Vulnerability Managements sind Virtual Patching und Alternatives Patching intelligente Lösungsansätze, die den gesamten Prozess der Erkennung und Behebung von Sicherheitslücken automatisieren. Dank der automatisierten Bearbeitung lassen sich Schwachstellen vom IT-Betrieb in der Geschwindigkeit schließen, die die Angreifer brauchen, um einen Exploit zu entwickeln. Hierdurch erhöht sich das Sicherheitslevel entsprechend. Ein weiteres Plus: Sowohl das virtuelle Patching als auch das Alternative Patching lassen sich von Security-Spezialist:innen abwickeln – Entwicklung und IT-Betrieb müssen sich nicht darum kümmern – jeder kann sich also weiterhin auf seine Kompetenzbereiche konzentrieren.

Sie möchten mehr erfahren?
Sprechen Sie gern Ihr Account Management an oder kontaktieren Sie uns über
www.computacenter.com/de

> Exploits legen rasant an Tempo zu, Schwachstellen müssen deutlich schneller behoben werden. Kluge Patching-Strategien sind nicht nur schnell, sondern beeinträchtigen auch nicht den IT-Betrieb.

Ralf Nemeyer
Solution Manager Information Security bei Computacenter

Computacenter

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen