Verborgene Schwächen entdecken

Sebastian Brabetz, Sicherheitsexperte bei mod, erklärt, wie Unternehmen in Zeiten zunehmender Cyber-Kriminalität ihre gesamte IT-Landschaft kontinuierlich schützen können.

Welche Windows-Version hat in den ersten drei Monaten nach ihrem Erscheinen die meisten Sicherheitslücken mit ‚hohem Schweregrad' gezeigt? Es ist die jüngste: 28 solcher Sicherheitslücken wurden allein innerhalb der ersten 100 Tage von Windows 10 identifiziert. Das Beispiel zeigt, wie gefährdet IT-Systeme heute sind – einerseits. Es zeigt andererseits aber auch die Wirksamkeit von Schwachstellenscans. Denn mit ihrer Hilfe kann man die von Microsoft geschlossenen Lücken effektiv in der eigenen Firma aufspüren und schließen.

Nicht nur das Betriebssystem Windows, jede Anwendung ist ein potenzielles Einfallstor für Hacker. Berühmt wurden die gravierenden Schwachstellen an der Multimedia-Anwendung FlashPlayer von Anfang 2015, weil sie lange offen blieben. Andere ‚Lecks' sind hausgemacht. Beispielsweise die veralteten Komponenten, die nach der letzten Anpassung der Unternehmens-IT nicht zurückgebaut wurden. Oder der ungeschützte Drucker für die streng vertraulichen Dokumente in der Chefetage.

Schwachstellen identifizieren und beseitigen

Am Anfang einer Schwachstellenscan-Lösung steht die Sichtung der gesamten IT-Landschaft, Cloud inklusive. Sperrt sich der Cloud-Dienstleister gegen Schwachstellenscans, ist ein Anbieterwechsel in Betracht zu ziehen. Im Unternehmen selbst müssen alle betroffenen Stellen informiert werden. Denn es kann nicht ausgeschlossen werden, dass ein Scan zu Störungen führt – was freilich selten vorkommt. Bei passiven Scans, die den Datenstrom in Echtzeit kontinuierlich prüfen, besteht diese Gefahr nicht.

Bei der Wahl der Scan-Technologie sollte nicht nur auf den Scanner selbst geachtet werden, sondern auch auf die Tools für Auswertung und Alarmierung. Eine komfortable Komplettlösung ist beispielsweise Tenables SecurityCenter. Expertise von außen kann an mehreren Stellen hilfreich sein: bei der Einrichtung der Scan-Lösung, bei der Auswertung der gewonnenen Informationen und bei der Beseitigung der identifizierten Schwachstellen.

Am meisten Sicherheit bietet ein Schwachstellen-Management mit kontinuierlichen passiven und täglichen aktiven Scans. Zwar bringt auch bereits ein jährlicher Scan einen gewissen Schutz. Doch man muss nicht Microsoft sein, um sich für erheblich kürzere Intervalle zu entscheiden. ◂

Nicht nur das Betriebssystem Windows, sondern jede Anwendung ist ein potenzielles Einfallstor für Hacker.

Sebastian Brabetz ist IT Security Engineer bei mod IT Services in Einbeck. Kontakt: *info@it-mod.de*

FOTO: STREICHHOLZ/PHOTOCASE.COM