Sicherheitslücken automatisch finden und schließen

Toolgestütztes Schwachstellenmanagement war das Thema der mbuf Arbeitsgruppe IT Security Management am 11. November. Zwei Vorträge von Microsoft und der Bericht eines Toolherstellers beschrieben die Vorgehensweise und die Werkzeuge.

Beim Schwachstellenmanagement prüfen Unternehmen ihre Systeme regelmäßig auf Sicherheitslücken und legen Maßnahmen fest, wie und in welcher Reihenfolge sie diese schließen. Anders als beim Virenscan, der maliziösen Code vom System entfernt, läuft das Schwachstellenmanagement proaktiv, wie Arbeitsgruppenleiter Norbert Breidohr berichtet: „Ich weiß, dass ich verwundbar bin gegen etwas, das kommen könnte. Und ich versuche, die entdeckten Lücken durch Patches oder eine geänderte Konfiguration zu schließen."

Exposure Management Plattform bewertet Risiken

Um Schwachstellen zu finden, nutzen die Unternehmen Tools, die ihre Systeme anhand von Erkennungskriterien prüfen. Einige dieser Lösungen laufen On Premise, andere scannen die Server aus der Cloud. Nach dem Auffinden einer Sicherheitslücke erfolgt die Bewertung, wie groß die konkrete Gefahr für das Unternehmen ist, und mit welchen Maßnahmen sich die Angriffsfläche reduzieren lässt.

Eines dieser Werkzeuge hat der Anbieter Tenable vorgestellt. „Tenable One ist eine Exposure Management Plattform, die IT-Systeme nach Schwachstellen untersucht", berichtet Breidohr. „Neben diesem Scan bildet die Applikation auch das Bewerten einer Schwachstelle ab." Völlig alleine kann diese Lösung laut Breidohr Schwachstellen allerdings nicht einschätzen: „Die Risikobewertung sollte ein Unternehmen immer selbst vornehmen, denn niemand kennt die IT-Landschaft besser."

Die Maßnahmen zur Behebung von Schwachstellen können durchaus unterschiedlich ausfallen, erläutert Andreas Sternberg, ein weiterer Leiter der Arbeitsgruppe IT Security Management: „Den größten Nutzen erzielen Unternehmen nicht immer damit, dass sie die am höchsten bewerteten Lücken schnell schließen. Sinnvoller ist es manchmal, im ersten Schritt eine weniger hoch bewertete aber viel weiter verbreitete Lücke zu schließen." Unternehmen mit einer sehr strikten Netzwerktrennung können es sich laut Sternberg möglicherweise leisten, in einem abgeschotteten Bereich verwundbare Systeme zu betreiben. Unternehmen ohne eine solche Trennung müssten die Schwachstellen sofort schließen.

Sensorik-Daten von Windows zeigen maliziöse Vorgänge

Microsoft hat zwei hauseigene Lösungen vorgestellt, die IT-Systeme auf Schwachstellen untersuchen: Defender Threat Intelligence Service und Defender External Attack Surface Management. Im Threat Intelligence Feed führt Microsoft Informationen aus den Sensorik-Daten der Windows-Server und Clients zusammen und leitet daraus Informationen über die Gefahrenlage und über Sicherheitslücken ab. Den Blick von außen liefert Microsoft Defender External Attack Surface Management. Hiermit verschaffen sich Unternehmen einen Überblick darüber, wie sich ihre IT-Systeme nach außen hin darstellen. „Ein Angreifer, der irgendwo in der Welt sitzt, sieht die Web-Server und die Mail-Server des Unternehmens und erkennt, wie die Telefonie abgebildet wird", berichtet Breidohr. „Dann scannt er die Systeme und sucht nach einer Schwachstelle."

Genau diesen Weg verfolgt auch Defender External Attack Surface Management. Die Applikation bewertet dann nicht nur die einzelnen Systeme, sondern auch das Gesamtrisiko. Ein solcher Scan entdeckt beispielsweise Systeme, die eine Fachabteilung ohne Rücksprache mit der IT-Abteilung aufgebaut hat. Ebenfalls ans Tageslicht kommen solche Systeme, die vor Jahren mit den damals aktuellen Sicherheitsmaßnahmen eingerichtet wurden, die aber inzwischen niemand mehr nutzt und pflegt. „Eventuell haben die Verantwortlichen im Unternehmen gewechselt, und dabei geriet völlig in Vergessenheit, dass hier noch ein System arbeitet, dessen Schutz in keiner Weise den aktuellen Erfordernissen entspricht“, berichtet Sternberg.

Windows Update für Business braucht Azure Active Directory

Mit Windows Update für Business und Windows Auto Patch beschäftigte sich der zweite Vortrag von Microsoft. Windows Update for Business ist ein Nachfolger der früheren Windows Server Update Services, die Unternehmen im eigenen Netz installiert haben. Das kostenlose aktuelle Update-System arbeitet Cloud-basiert und nutzt mehrere Update-Ringe. „Im Fast Ring werden die Patches sofort nach der Verfügbarkeit eingespielt“, berichtet Sternberg. „Dann fragt Microsoft die Sensorik dieser Clients bei allen Kunden ab, ob es Abstürze oder ein ungewöhnliches Verhalten gibt. Auf Basis dieser Informationen schlägt das System vor, ob der Patch weiter ausgerollt wird, oder ob das Unternehmen warten sollte, bis ein Fix vorliegt. Darüber hinaus zeigt das System, welche Clients in der frühen Phase Schwierigkeiten hatten.“

Die technische Grundvoraussetzung für Windows Update for Business und Windows Auto Patch ist es, dass die Clients in einem Azure Active Directory laufen und Cloud-fähig sind. „Mit Windows Update für Business macht Microsoft denjenigen Unternehmen das Leben leichter, die heute kein systematisches Patch Management in Einsatz haben“, berichtet Breidohr. „Man gibt dabei die Entscheidung darüber, ob ein Patch eingespielt wird oder nicht, an Microsoft ab.“ Immerhin könnten Unternehmen davon ausgehen, dass Microsoft durch die Masse seiner Sensordaten einen sehr guten Überblick hat und bei Bedarf einen Patch auch schnell berichtigen kann.

Künftig finden wieder Präsenztreffen statt

Die Sitzung am 10. November war das 50. Treffen der mbuf Arbeitsgruppe IT Security Management. Die Präsenzveranstaltung mit einem Vorabendtreff kam bei den Teilnehmern sehr gut an. „Um künftig ein Stück Normalität wiederherzustellen, setzen wir weiterhin auf Präsenztreffen“, berichtet Breidohr. Der Nutzen dieser Veranstaltungsform war in der Vergangenheit sehr hoch und wird es auch künftig wieder sein. Wir freuen uns auf eine rege Beteiligung!“

Das nächste Treffen der mbuf Arbeitsgruppe IT Security Management findet im März statt. Die Themen erarbeiten die Arbeitsgruppenleiter anhand der Vorschläge der Teilnehmer. *Jürgen Frisch*