MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK

Analyse: Ein dreifacher Riegel für Hacker mit Microsofts neuem Defender

06.10.2020 10:43 Uhr
Hagen Molzer

(Bild: antb/Shutterstock.com)

Im Rahmen der Ignite hat Microsoft sein Security-Paket umstrukturiert. Aber neben dem neuen Namen bietet der Defender auch viele neue Funktionen für Firmen.

Auf seiner Ignite zeigte Microsoft im Bereich der IT-Security die Umbenennung und Neustrukturierung sowie die Wirkweisen der unterschiedlichen Defender-Schutzfunktionen. Künftig umfasst der Microsoft 365 Defender – vormals bekannt als Microsoft Threat Protection – folgende Dienste:

- Defender for Endpoint (vormals Defender Advanced Threat Protection)
- Defender for Office 365 (vormals Office 365 Advanced Threat Protection)
- Defender for Identity (vormals Azure Advanced Threat Protection)

Diese bilden zukünftig zusammen mit den Funktionen des Azure Defender – vormals Azure Security Center – den Umfang der XDR-Suite (Extended Detection and Response). Das Ganze ergänzt Azure Sentinel, das als SIEM-Tool auch Alarme und Logmeldungen anderer Sicherheitssoftware in das Gesamtbild integrieren und so das Analysieren von Angriffen erleichtern soll.

Unterschiedliche Angriffe, unterschiedliche Defender

Setzt ein Unternehmen alle XDR-Komponenten ein, lässt sich ein klassischer Angriff auf die IT – Phishing-E-Mail, Kompromittierung eines Geräts und anschließendes Lateral Movement mithilfe des Tools Mimikatz – auf mehrere Art und Weisen mit dem sogenannten Defense of Depth erkennen und verhindern. Eine eingehende Phishing-E-Mail erkennt und blockiert der Defender for Office 356. Defender for Endpoint erkennt die Ausführung von Mimikatz oder anderen schadhaften Dateien und löscht die Schadsoftware. Zuletzt erkennt der Defender for Identity einen Overpass-the-Hash-Angriff und alarmiert das Security Operations Center (SOC).

Bislang wäre zum Untersuchen der beschriebenen Angriffskette der Zugriff auf die einzelnen Microsoft-Portale nötig gewesen und ein SOC-Analyst hätte die Alarme der einzelnen Tools selbst miteinander in Verbindung bringen müssen. Microsoft 365 Defender aggregiert die Alarme aus den verschiedenen Quellen nun in einem Portal. Falls an dem skizzierten Angriff auch auffälliger Netzwerkverkehr mit externen Webseiten beteiligt ist und das Unternehmen einen Proxy eines Drittherstellers einsetzt, können die dort generierten und an Azure Sentinel weitergeleiteten Alarme das Gesamtbild vervollständigen.

Immer mehr Angriffe, MFA soll helfen

Mehrere Sessions der Ignite gingen auf die stark zunehmende Anzahl an Angriffen auf Benutzerkonten im Azure Active Directory (AAD) und auf mögliche Gegenmaßnahmen ein. So stellte beispielsweise Microsoft in diesem Jahr bei Password-Spray-Angriffen **einen Anstieg von 230 Prozent [1]** fest, außerdem beinhaltet fast jeder dritte Angriff eine Phishing-Komponente. Um derartigen Angriffen entgegenzuwirken, rät der Konzern davon ab, die Benutzerkonten ausschließlich mit Passwörtern abzusichern. Stattdessen sollen Unternehmen **verschiedene Arten der Multi-Faktor-Authentifizierung (MFA) [2]** einsetzen, wobei deren Schutzwirkung in drei Kategorien aufgeteilt ist.

Eine gute Schutzwirkung versprechen die Kombinationen aus Passwort und SMS oder einem Anruf. Besser sind jedoch ein Passwort und eine Push-Benachrichtigung oder ein Einmalkennwort, das per Software oder Hardware generiert wurde. Die beste Schutzwirkung sollen Windows Hello, ein FIDO2 Security Key oder der Microsoft Authenticator bieten. Die letzteren beiden Optionen befinden sich derzeit in einer Preview-Phase.

Blacklist optional fürs eigene Unternehmen modifiziert

Auf dieser Basis empfiehlt Microsoft insbesondere Konten mit administrativen Berechtigungen umgehend per MFA abzusichern. Auch für reguläre Benutzer sollten Systemverwalter dringend eine starke Authentifizierung erzwingen. Schon jetzt verhindert Microsoft automatisch das Setzen besonders schwacher Passwörter über eine Blacklist. Diese kann der Administrator auf Wunsch selbst pflegen, um Phrasen mit Bezug zum Unternehmen oder den Standort aufzunehmen.

Im nächsten Schritt kann die IT mit verschiedenen AAD-Funktionen die Angriffsfläche weiter reduzieren. Beispielsweise lässt sich mit Conditional-Access-Regeln einschränken, dass

sicherheitskritische Anmeldungen nur von konformen, zentral verwalteten Computern erfolgreich sind. Des Weiteren kann das Prinzip von Just-in-time-Administration implementiert werden.

Mit Funktionen zum Lifecycle-Management unterstützt das AAD die Organisation zum Beispiel auch dabei, Ausnahmen von Conditional-Access-Regeln nur für eine bestimmte Zeit zu konfigurieren, die Notwendigkeit einer Ausnahme regelmäßig zu prüfen oder Ausnahmen für einen Benutzer nur nach Durchlaufen eines Genehmigungsprozesses zu implementieren. Die Conditional-Access-Regeln erlauben ebenfalls eine automatisierte Reaktion auf eventuell von Angriffen betroffene Anwender, etwa durch das Erzwingen einer Passwortänderung oder Blockieren riskanter Anmeldungen.