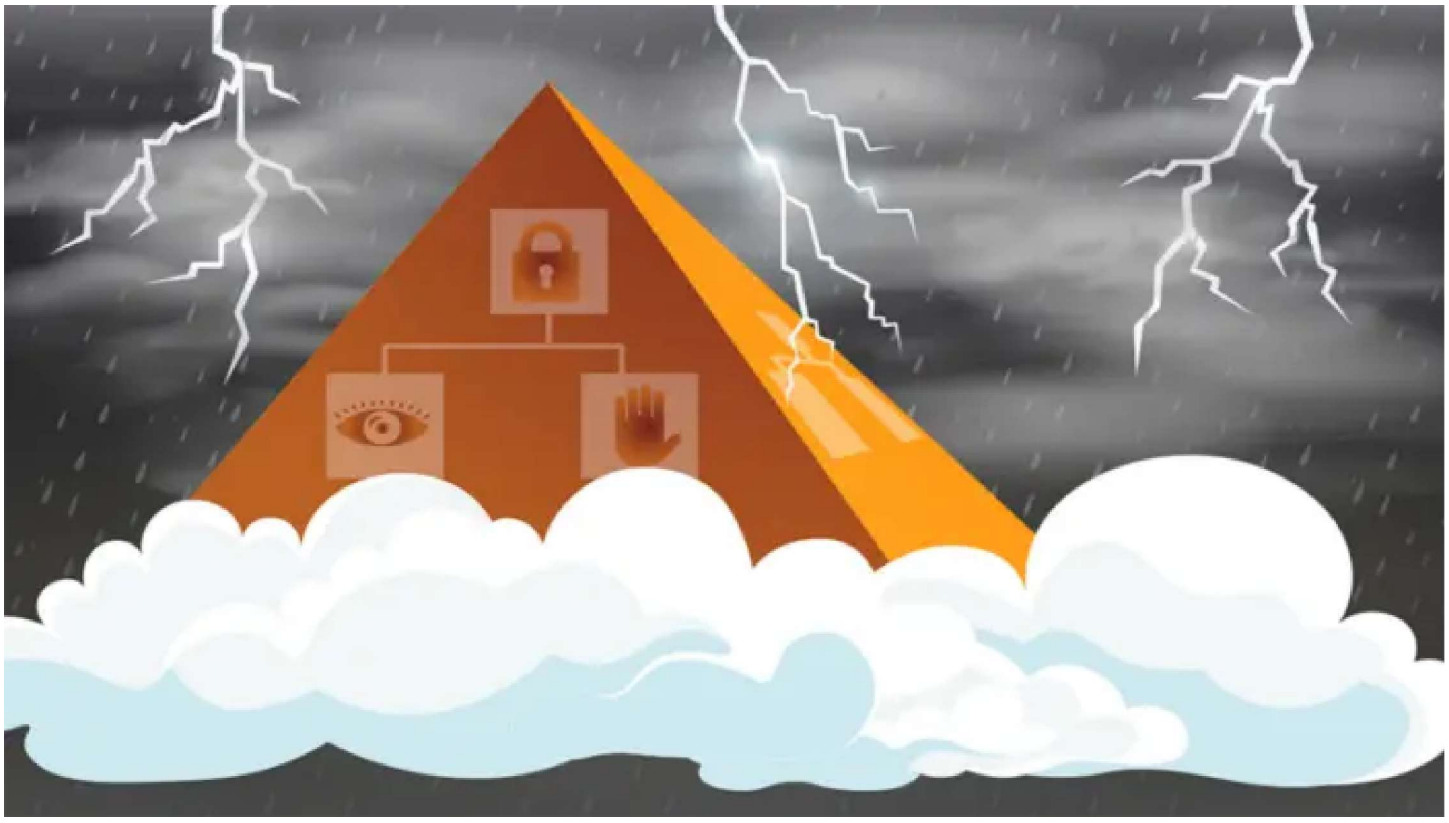
MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK

Fehlende MFA, Standardpasswort: So lief der Angriff auf die MS-Securityabteilung

26.01.2024 16:30 Uhr Moritz Förster



(Bild: iX)

Securityempfehlungen von Microsoft gibt es einige – die müsste der Konzern aber auch selbst umsetzen, wie die Analyse des Midnight-Blizzard-Angriffs zeigt.

Wie konnten Angreifer bei Microsofts Cybersicherheitsabteilung einsteigen? Aufgrund einer fehlenden Mehrfaktor-Authentifizierung und durch Ausnutzung eines Standard-Passworts, wie Microsoft jetzt selbst zugeben muss.

Der Hintergrund: Vor wenigen Tagen gab Microsoft bekannt, dass die von Russland unterstützte Gruppe **Midnight Blizzard erfolgreich auf E-Mails von Security-Mitarbeitern zugreifen** [1] konnten. Die auch als Nobelium bekannten Kriminellen nahmen Microsoft seit Ende November 2023 unter Beschuss und konnten währenddessen Daten von Führungskräften erbeuten. Ihr primäres Ziel: bei Microsoft gespeicherte Informationen über die eigene Gruppe erbeuten.

So macht man's nicht

Aber wie kann es sein, dass dies ausgerechnet bei einer Cybersicherheitsabteilung gelang? Microsoft hat nun Details zum Vorgehen veröffentlicht, aufgrund derer andere Organisationen ihre Sicherheitsinfrastruktur verbessern sollen. Bereits bekannt war, dass sich Midnight Blizzard dem Password Spraying bedient. Hierbei nutzen die Angreifer eine begrenzte Anzahl an Kennwörtern, die jedoch am beliebtesten sind oder am wahrscheinlichen verwendet werden. Anders ausgedrückt: Der Einstieg gelang mit einem Standardpasswort.

Durch die eigene Zurückhaltung und indem sie sich hinter einer Proxy-Infrastruktur verbargen, konnten die Kriminellen einem frühen Entdecken entgehen. Allerdings sollte das normalerweise nicht genügen, denn Microsoft selbst propagiert schließlich den standardmäßigen Einsatz einer Mehrfaktor-Authentifizierung. Ein Passwort in Nobelium-Hand sollte nicht ausreichen. Jedoch beschreibt jetzt der Konzern selbst, wie diese bei einem Legacy-Test-Tenant-Konto schlicht nicht aktiviert war. Und über dieses gelang Midnight Blizzard der Erstzugriff.

Anschließend konnten sich die Angreifer dank einer alten OAuth-Testanwendung mit höheren Zugriffsrechten ausrüsten und eigene OAuth-Anwendungen sowie einen eigenen Zugang einrichten. Mit passenden Exchange-Online-Rechten ausgestattet, konnten sie über diesen E-Mails aus anderen Postfächern abgreifen.

Schwachstellen gab's keine, waren auch nicht nötig

Schon bei Bekanntwerden des Angriffs beteuerte Microsoft, dass Midnight Blizzard keine Schwachstellen ausgenutzt habe. Stattdessen sei ein Testsystem geknackt worden. Noch nicht bekannt war allerdings, welche Sicherheitsmaßnahmen Microsoft selbst hierbei nicht umgesetzt hatte. Offen ist weiterhin, ob der kurz darauf bekannt gewordene **Angriff derselben Gruppe auf HPE [2]** durch Microsoft aufgedeckt wurde – der Konzern gibt nur an, andere Betroffene informiert zu haben.

Damit sich andere Organisationen gegen dasselbe Vorgehen wappnen können, empfiehlt Microsoft folgendes: Sie müssen bösartige OAuth-Applikationen identifizieren können und sich gegen Passwort-Spraying-Attacken verteidigen können. Details zu den einzelnen Schritten **finden sich in Microsofts Blogbeitrag [3]**. Darüber hinaus beschreibt Microsoft, wie Verantwortliche solche Angriffe aufspüren können.

[4]

(fo [5])

URL dieses Artikels:

https://www.heise.de/-9610189

Links in diesem Artikel:

[1] https://www.heise.de/news/Cyber-Angreifer-erbeuten-E-Mails-von-Microsoft-Mitarbeitern-9603710.html

[2] https://www.heise.de/news/Cybercrime-Hewlett-Packard-Enterprise-legt-Attacke-auf-E-Mail-System-offen-9608278.html

[3] https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

[4] https://www.heise.de/ix/

[5] mailto:fo@heise.de