Hacker gelangen via Umwege an den sensitiven Schlüssel.

Echt jetzt Microsoft?

Wer mich kennt, weiss, dass mich selten etwas aus der Fassung bringt. Aber was da bei Microsoft passiert ist, macht mich sauer. Sinnbildlich mit dem Briefkastenschlüssel konnte das Schloss der Atombombe geöffnet werden. Oder etwas genauer: mit einem einfachen Zertifikat konnten alle anderen verschlüsselten Daten lesbar gemacht werden.

Betroffen waren gemäss ersten Ergebnissen Konten bei Exchange Online und Outlook.com von 25 Organisationen, vor allem handelt es sich um Regierungsdaten in der Microsoft Government Cloud. Doch ob dies alle gehackten Konten sind, weiss niemand so genau. Microsoft gibt nur teilweise und zurückhaltend Informationen preis. Ob diese Schwachstelle auch für Microsoft als Hintertüre (Backdoor) genutzt werden konnte (wurde), ist ebenfalls denkbar. Das Vertrauen in Microsoft ist auf jeden Fall weg.

Der Zwischenfall ist sogar bis zum amerikanischen Präsidenten Biden eskaliert, der eine umfassende Aufklärung verlangt. Andere Regierungsstellen, wie zum Beispiel die EU, schweigen sich aus. Wenn in der Schweiz das Nationale Zentrum für Cybersicherheit (NCSC) um Hilfe gefragt wird, heisst es nur «Wenn ihr betroffen seid, informiert euch Microsoft schon». Jedes Unternehmen ist also auf sich selbst gestellt, mehr darüber zu erfahren, ob auch von den eigenen Konten Daten entwendet wurden.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Zugriff auf die Logdaten

Erste Informationen, was genau passiert ist, wurden inzwischen am 6. September 2023 von Microsoft veröffentlicht. Der Hack durch die mutmasslich chinesische Gruppe Storm-0588 dauerte von Mai bis Juni 2023, und war durch einen gestohlenen privaten Microsoft Account (MSA) und mehreren Schwachstellen möglich. Die Angreifer konnten diesen Schlüssel unter anderem benutzen, um gefälschte Sicherheitstoken (für Outlook Web Access, OWA) zu generieren. Diese Sicherheitstokens konnten sowohl für Zugriffe auf private Microsoft-Konten (zum Beispiel outlook.com) als auch für Zugriffe auf Azure AD-Konten und, das wird von verschiedenen Security-Experten vermutet, auch für Azure-Apps benutzt werden. Normalerweise werden Sicherheitstoken vom Zielsystem immer noch verifiziert, aber das funktionierte aus unerklärten Gründen nicht. Das Ganze blieb lange unbekannt, erst als ein Microsoft-Kunde ungewöhnliche Aktivitäten bei Konten seiner Mitarbeitenden bemerkte, flog der Angriff auf. Dazu muss gesagt werden, dass der Zugriff auf die Logdaten mit den Hinweisen darin, eine kostenpflichtige Dienstleistung von Microsoft ist. Auf Grund der riesigen Kritik, bekommen aber nun alle Kunden kostenlosen Zugriff auf die Logdaten. Sicherheitsforscher der Firma Wiz gaben an, dass infolge der langen Dauer eigentlich die gesamte Microsoft Cloud-Infrastruktur als potenziell kompromittiert angesehen werden muss, sprich alle Daten als gestohlen oder manipuliert betrachtet werden müssen.

In der Untersuchung von Microsoft wird beschrieben, dass es im April 2021 in einer besonders geschützten Sicherheitszone zu einem Absturz des Signiersystems kam. Dabei wurde ein Schnappschuss (Crash Dump genannt) des abgestürzten Prozesses erzeugt. Normalerweise sind darin keine sensiblen Informationen enthalten. Durch einen Software-Fehler war aber genau dies der Fall. Dieser Fehler wurde, nach mehr als zwei Jahren, von Microsoft geschlossen. Unwissend, dass sensitive Informationen auf diesem System liegen, wurde es in der Folge ungeprüft in die Debugging-Umgebung von Microsoft

kopiert, also aus dem geschützten Bereich heraus in einen Bereich mit Internet-Verbindung.

Auch Microsoft-Mitarbeitende sind nicht gegen Phishing gewappnet

Weiter stellt Microsoft eine Bibliothek von Dokumentations- und Hilfs-Werkzeugen zur Verfügung, um damit die Signaturen kryptografisch zu validieren, aktualisierte diese Bibliotheken jedoch nicht, um die Validierung von Schlüsseln automatisch durchzuführen (dieses Problem wurde inzwischen ebenfalls behoben). Die E-Mail-Systeme wurden zu einem späteren Zeitpunkt mit diesen Bibliotheken aktualisiert.

Die Entwickler des E-Mail-Systems gingen fälschlicherweise davon aus, dass die Bibliotheken eine vollständige Validierung durchführen und dies nicht zusätzlich gemacht werden muss. So führten die E-Mail-Systeme keine zusätzliche Validierung des Ausstellers und des Geltungsbereichs durch. Daher akzeptierte das E-Mail-System eine Anfrage für Unternehmens-E-Mails mit einem Sicherheits-Token, das mit dem, eigentlich nicht gültigen, Schlüssel signiert war (dieses Problem wurde mit aktualisierten Bibliotheken behoben).

Auch Microsoft-Mitarbeitende sind nicht gegen Phishing gewappnet und das Unternehmenskonto eines Ingenieurs mit Zugriff auf dieses System wurde kompromittiert. Microsoft legt für dieses Szenario zwar keine Beweise offen, meint aber im Bericht, dass dies der einzig vorstellbare Weg sein kann. Und so gelangten die Hacker via viele Umwege an den sensitiven Schlüssel.

In der Security-Welt gingen nach diesem Bericht erneut die Wogen hoch. Nicht erwähnt in dieser kurzen Zusammenfassung der Ereignisse sind weitere Schwächen, die inzwischen aber durch Microsoft mit Patches geschlossen wurden. In der Summe sind es doch etwas gar viele Zufälle, die zu diesem Super-Gau geführt haben. Erschwerend kommt dazu, dass der erwähnte MSA-Schlüssel bereits im Jahr 2021 abgelaufen ist und eigentlich gar nicht mehr funktionieren sollte. Weiterhin unklar ist, warum Microsoft überhaupt über einen solchen Generalschlüssel verfügt.

Bei der grossen Abhängigkeit von Microsoft stellt sich schon die Frage: «Und was nun?». Bei meinen Nachfragen, welche Schritte ein Unternehmen verfolgen wird, war bei allen die Antwort: mit den zur Verfügung gestellten Tools und Informationen ist es kaum möglich herauszufinden, ob das eigene Unternehmen betroffen ist.

Und wie sieht es mit einem Wechsel zu einem anderen Anbieter aus? Die einstimmige Rückmeldung: «Es gibt ja keine Alternativen». Ist das aber wirklich so? Ich kann diese Frage nicht pauschal beantworten. Aber jedes Unternehmen sollte sich spätestens jetzt mit geeigneten Alternativen auseinandersetzen, auch wenn es nicht einfach ist.

Bericht von Microsoft: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/