Echt jetzt Microsoft?

von Andreas Wisler

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 vor allem Regierungsdaten in der Microsoft Government Cloud. Doch das weiss niemand so genau. Dass diese Schwachstelle auch für Microsoft als Hintertüre (Backdoor) genutzt wurde, wäre denkbar. Das Vertrauen in Microsoft ist auf jeden Fall weg.

Der Zwischenfall ist bis zum amerikanischen Präsidenten Biden eskaliert, der eine 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.

Erste Informationen, was genau passiert ist, sind inzwischen von Microsoft veröffentlicht worden. Der Hack durch die mutmasslich chinesische Gruppe Storm-0588 von Mai bis Juni 2023 war durch einen gestohlenen privaten MSA-Schlüssel und mehreren Schwachstellen möglich. Die Angreifer konnten diesen Schlüssel benutzen, um gefälschte Sicherheitstoken (für 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 vermutet, auch für Azure-Apps benutzt werden. Normalerweise werden Sicherheitstoken immer noch verifiziert, aber das funktionierte aus unerklärten Gründen nicht. Das Ganze blieb lange ungekannt, erst als ein Kunde ungewöhnliche Aktivitäten bemerkte, flog der Angriff auf. Sicherheitsforscher von Wiz gaben an, dass infolge der langen Dauer eigentlich die gesamte Microsoft Cloud-Infrastruktur als potenziell kompromittiert angesehen werden muss.

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 inzwischen 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 und das Unternehmenskonto eines Ingenieurs mit Zugriff auf dieses System wurde kompromittiert und so gelangten die Hacker via einen Umweg an den sensitiven Schlüssel.

In der Security-Welt gingen nach diesem Bericht die Wogen erneut hoch. Nicht erwähnt in dieser kurzen Zusammenfassung sind weitere Schwächen, die teilweise 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 nun Unternehmen einschlagen, 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 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. ●

Andreas Wisler ist Inhaber und Senior Security Consultant goSecurity AG ISO 27001, 27701 und 22301 Lead Auditor

www.goSecurity.ch | www.27001.blog | www.angriffslustig.ch