Bild: Andy Wong/AP/dpa

Wolkenbruch

Der kleingeredete GAU der Microsoft-Cloud

Eine Hackergruppe klaute Microsoft einen Master-Key, der ihnen Tür und Tor zur Microsoft-Cloud öffnete. Der Konzern versucht den Vorfall kleinzureden, doch es deutet sich eher ein Komplettversagen an.

Von Jürgen Schmidt

Am 11. Juli feierte sich Microsoft selbst mit einer Erklärung, man habe die Angriffe chinesischer Akteure auf Kunden-E-Mails entschärft. Allzu viele Angaben über das Ausmaß des Vorfalls machte der Unternehmen nicht. Doch inzwischen ist klar: Angreifer konnten wochenlang quasi beliebig auf nahezu alle Daten bei Microsofts Clouddiensten zugreifen – das betraf unter anderem Outlook, Sharepoint, Office365, Teams, OneDrive und Drittanwendungen, die die Funktion „Sign in with Microsoft“ anbieten.

Bis heute weigert sich der Konzern, die genauen Hintergründe und die sich daraus ergebenden Konsequenzen offenzulegen. Bekannt ist Folgendes: Den mutmaßlich chinesischen Angreifern, die Microsoft als Storm-0558 bezeichnet, war es gelungen, einen wichtigen Schlüssel zu stehlen. Und mit dem konnten sie unter anderem fremde E-Mails lesen.

Überblick

In der Azure-Cloud fungiert Microsoft als Identitätsprovider und verwaltet alle Informationen über Cloudnutzer im sogenannten Azure Active Directory – kurz Azure AD oder AAD. Bei der Anmeldung überprüft das AAD das Passwort und gegebenenfalls weitere Faktoren wie TOTP-Prüfcodes eines Benutzers. Hat das Erfolg, bekommt das zugreifende Programm ein Token mit Microsofts digitaler Unterschrift, das es ermächtigt, im Auftrag des Benutzers zu handeln – also etwa seine E-Mails abzurufen.

Den Angreifern gelang es offenbar, sich einen Schlüssel zu besorgen, der genau solche Tokens signieren konnte. Und mit diesen Tokens spionierten sie die in der Microsoft-Cloud gehosteten E-Mail-Zugänge mehrerer, vornehmlich europäischer Regierungsbehörden aus. Und das offenbar über mehrere Wochen völlig unbemerkt.

Die Opfer hatten auch kaum eine Chance, den Angriff zu bemerken. Zwar werden Zugriffe auf E-Mails protokolliert, aber wer diese Daten auswerten will, etwa um unautorisierte Zugriffe zu bemerken, benötigt Microsofts Zusatzprodukt „Purview Audit Premium“ – und das kostet.

Eine US-Behörde hatte diese kostenpflichtigen Logdateien jedoch lizenziert und fand darin verdächtige Aktivitäten. Sie informierte die Cybersecurity and Infrastructure Security Agency (CISA) und Microsoft über den vermutlichen Angriff. Die reagierten und sperrten den betroffenen Signaturschlüssel, sodass damit keine weiteren Zugriffe mehr möglich waren. Dem Drängen der CISA haben wir es übrigens zu verdanken, dass Microsoft diese Logdaten jetzt kostenfrei zur Verfügung stellen will [1].

Bei der Analyse des Vorfalls fand Microsoft heraus, dass weitere vornehmlich europäische Regierungsbehörden und auch einige Privatkonten vermutlich aus deren Umfeld ausspioniert wurden. Nach Microsofts Angaben habe man zu diesem Zeitpunkt bereits alle betroffenen Kunden informiert. Wer keine Nachricht von Microsoft erhalten habe, brauche sich auch keine Sorgen zu machen.

Was Microsoft alles nicht sagt

Diese Weigerung, zu konkretisieren, wer genau und welche Microsoft-Produkte betroffen waren, reiht sich ein in eine ganze Serie von Dingen, über die Microsoft ganz offensichtlich lieber nicht reden möchte. Da ist vor allem dieser Signaturschlüssel. Das ist das Kronjuwel eines Identity Providers, welches man deshalb so gut sichert, wie es irgend geht. Schließlich ist das ja das Versprechen der Microsoft-Cloud: Wir nehmen dir das mit der Verwaltung der Identitäten ab und unsere Security-Spezialisten machen das so sicher, wie du es selber nie könntest.

Dieses zentrale Versprechen entpuppt sich jetzt mehr und mehr als glatte Lüge. Zu dem eigentlichen Diebstahl macht Microsoft selbst auf hartnäckiges Nachfragen keine Angaben. Die Methode, wie der Angreifer den Schlüssel entwendet habe, sei „Gegenstand laufender Ermittlungen“. Nicht einmal, wo der Schlüssel gestohlen wurde, möchte man preisgeben.

Doch die jetzt angepriesenen Verbesserungen lassen erahnen, was da vorher alles schiefgelaufen ist: Man habe den Nachfolger dieses Schlüssels jetzt in den Key Store für Enterprise-Systeme umgezogen und das Monitoring und Alerting wesentlich verbessert, heißt es in der Analyse. Das bedeutet im Umkehrschluss, dass es bisher weder um den Aufbewahrungsort noch um die Überwachungsmaßnahmen so richtig gut bestellt war. Und zwar nicht in irgendeiner unwichtigen Ecke der Cloud, sondern es geht wohlgemerkt um die Sicherheit der Kronjuwelen.

Gestohlene Schlüssel und kaputte Schlösser

Apropos Enterpise-Systeme: Das Stichwort bringt uns zum zweiten dunklen Fleck, zu dem Microsoft die Auskunft verweigert: Der gestohlene Signaturschlüssel hätte eigentlich gar keine gültigen Zugangstoken für die im Enterprise-Umfeld angesiedelten Dienste wie Exchange Online ausstellen dürfen.

Es handelte sich nämlich um einen Signaturschlüssel aus dem Endkundenbereich der Microsoft-Accounts (MSA), die man etwa als Endanwender anlegen soll, um sein Windows Home zu benutzen. Solch ein MSA-Schlüssel darf eigentlich keine AAD-Tokens beglaubigen. Microsoft spricht in diesem Kontext verharmlosend von einem „Überprüfungsproblem“ (Validation Issue). Genauere Informationen gibt es auch auf Nachfragen nicht.

Gemäß einer Analyse der auf Cloud-Security spezialisierten Firma Wiz funktionierte dieser MSA-Schlüssel in nahezu der gesamten Microsoft-Cloud. Also für das Outlook-Konto von Privatkunden genauso wie für Teams, Sharepoint oder eigene Cloud-Apps für Firmen mit „Login with Microsoft“ – abgesehen von wenigen Ausnahmen wie der sogenannten Single-Tenant-Konfiguration. Microsoft erklärte dazu, die Wiz-Analyse beruhe auf Spekulationen und nicht auf Fakten, jedoch ohne ihr konkret zu widersprechen oder die fehlenden Fakten zu liefern.

Und nun?

Mittlerweile ist der gestohlene Schlüssel gesperrt; weitere Zugriffe sollten also damit nicht mehr möglich sein. Trotzdem ist die Gefahr noch nicht ganz gebannt. Denn die Angreifer hatten mehrere Wochen weitgehend Carte Blanche für große Teile der Microsoft-Cloud. Sie hätten während dieser Zeit dort fast nach Belieben Hintertüren platzieren können. Ob das passiert ist beziehungsweise wie man sein eigenes Konto jetzt sinnvoll auf solche Hintertüren prüfen kann, kann letztlich nur Microsoft beantworten. Doch die sagen im Wesentlichen nur: „Vertrau uns, wir haben das im Griff.“

Es ist kein Wunder, dass Microsoft sich mit konkreten Details so zurückhält. Die Überprüfung von Zugangsberechtigungen ist **das** zentrale Element von Azure AD und überhaupt der Sicherheit von Microsofts Cloud. Wenn da tatsächlich, wie es sich andeutet, nicht nur ein fast allmächtiger Master-Schlüssel gestohlen wurde, sondern auch noch die Schlösser Schrott waren (das „Validation Issue“), dann ist das eine Bankrotterklärung für die so vollmundig angepriesene Sicherheit der Microsoft-Cloud.

Zunächst schien Microsofts Strategie aufzugehen. Die Medienberichte konzentrierten sich vor allem auf die abgewehrten, angeblich chinesischen Staats-Hacker. Die Dramatik dieser Vorgänge und Microsofts dabei ans Tageslicht kommende Schlamperei war nur in Insiderkreisen ein Thema. Das mag auch an den still schweigenden europäischen Regierungen liegen, die ja laut Microsoft die Mehrzahl der konkret Betroffenen stellen. Vom BSI war selbst drei Wochen nach der Bekanntmachung der Angriffe weder zu erfahren, ob deutsche Behörden betroffen waren, noch bekamen wir eine Einschätzung zu Relevanz und Bedeutung des Vorfalls.

Es stellt sich die Frage, was man als möglicherweise Betroffener jetzt tun kann. Wiz gibt dazu Tipps, wonach man suchen könnte, um Zugriffe von Storm-0588 aufzuspüren. Doch eigentlich ist Microsoft in der Pflicht, konkrete Antworten zu liefern, was da jetzt wirklich Sache ist und wie man sinnvoll damit umgeht. Die passenden Fragen dazu haben wir bereits bei heise Security veröffentlicht [2].

Überdies sollte man diesen Vorfall zum Anlass nehmen, die eigene Einstellung zur Cloud und deren Nutzung nochmals auf den Prüfstand zu stellen. Und zwar unter Berücksichtigung der Tatsache, dass es mit der angeblichen Sicherheit der großen Cloudanbieter nicht so weit her ist, wie die uns glauben machen wollen. Wäre es vielleicht nicht doch sinnvoller, den ein oder anderen Dienst selbst zu betreiben? Gibt es vielleicht kompetente, lokale Dienstanbieter, mit denen man noch auf Augenhöhe kommunizieren kann? Oder sogar: Wie könnte ein Ausstieg aus der Cloud aussehen? *(wid@ct.de)* c't

Literatur

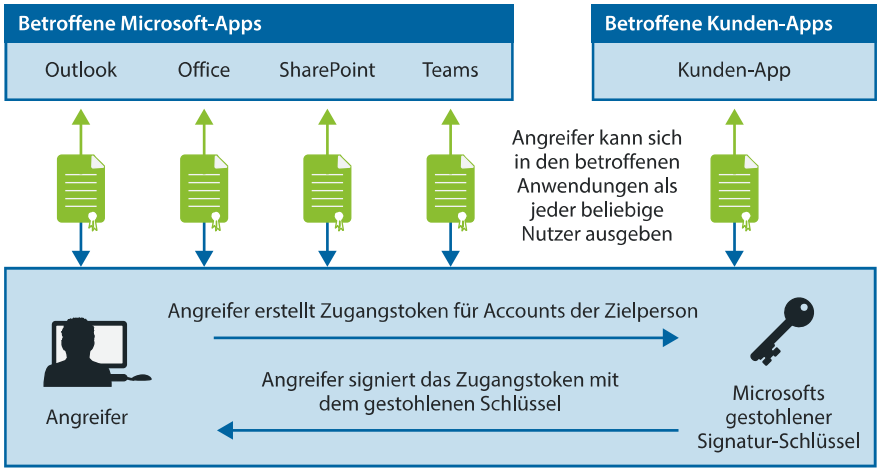
[1] Jürgen Schmidt, Microsofts gestohlener Schlüssel mächtiger als vermutet: https://heise.de/-9224640

[2] Jürgen Schmidt, Gestohlener Cloud-Master-Key, Microsoft schweigt – so fragen Sie selbst: https://heise.de/-9229395

Statements von Microsoft: ***ct.de/yghf***

Generalschlüssel

Bei dem gestohlenen Schlüssel handelt es sich um einen OpenID Signing Key für das Azure Active Directory (AAD). Das ist Microsofts Cloud-Verzeichnisdienst, also eine Art Telefonbuch der bekannten Cloud-Nutzer. Mit diesem konnten sich Angreifer Zugang zu den Benutzerkonten aller betroffenen Cloud-Applikationen verschaffen. Es war zudem möglich, mit dem Schlüssel Zugangstoken für Outlook, Office, Sharepoint und Teams zu erstellen.



Quelle: Wiz-Research