Ransomware – aus realen Fällen lernen

Die Tools und das Vorgehen zur Abwehr von Ransomware-Angriffen, Schutzmechanismen in Microsoft 365, Digitale Forensik und zwei Anwendervorträge über den Umgang mit Sicherheitsvorfällen und die Wiederherstellung nach einem Cyberangriff – die mbuf-Arbeitsgruppe IT-Security-Management hatte am 16. November 2023 ein umfangreiches Programm.

25 Teilnehmer der Arbeitsgruppe IT-Security Management haben sich bei der Südzucker AG versammelt. Zum Einstieg stellte der Gastgeber sein Unternehmen inklusive der Abteilung Informationssicherheit sowie das Projekt einer Multicloud-Firewall in Microsoft Azure vor. „Südzucker ist in Sachen Cybersecurity sehr aktiv, und alle Aktivitäten genießen die volle Rückendeckung durch den Vorstand“, berichtet Jonathan Haist, einer der Arbeitsgruppenleiter. „Das fängt an mit einer Multicloud-Firewall, die einen Schutz vor Distributed Denial of Service-Attacken bietet und über ein Load Balancing die Last zwischen den Systemen verteilt und geht weiter bei einem beauftragten Security Operations Center. In den vergangenen drei Jahren hat das Unternehmen sein Security-Team personell stark erweitert.“

Forensische Tools bei Microsoft DART

Der erste Microsoft-Vortrag hat aufgezeigt, mit welchen forensischen Tools und Verfahren das Microsoft Detection and Response Team (DART) nach einem Ransomware-Angriff die Systeme wiederherstellt. Der Umgang mit forensischen Werkzeugen erfordert tiefes Know-how, wie der zweite Arbeitsgruppenleiter Norbert Breidohr erläutert: „Mit ist in den letzten 10 Jahren nur ein Unternehmen begegnet, das einen eigenen Forensiker hat. Da aber ohne diese Spezialkenntnisse niemand diese Werkzeuge bedienen kann, ist es sinnvoll, sich eine entsprechende Dienstleistung zuzukaufen.“

Auch einige vorbeugende Maßnahmen hat der Microsoft-Spezialist beschrieben. So haben Unternehmen mit einem getesteten Backup die Chance, nach einem Angriff ihre Systeme mit einem vergleichsweisen geringen Schaden wiederherzustellen. Um zu verhindern, dass ein Backup selbst von Ransomware verseucht wird, muss man entweder den Speicher mit strengen Zugriffsrechten und einer Zwei-Faktor-Authentifizierung absichern oder ihn nach einem Backup komplett vom Netz trennen.

Sentinel und Defender XDR wachsen zusammen

Der zweite Microsoft-Vortrag hat den erweiterten Ransomware-Schutz in Microsoft 365 sowie das Zusammenwachsen der Lösungen Microsoft Sentinel und Microsoft Defender XDR (Extended Detection and Response) beschrieben. Für Microsoft 365 gibt es inzwischen die Sicherheitskomponente Backup 365, mit der man anhand von vordefinierten Service Level Agreements Backups in einer Microsoft-Umgebung durchführen kann. Microsoft Sentinel, eine Cloud-basierte Lösung für Security Information and Event Management (SIEM) und Microsoft Defender XDR werden künftig in einem gemeinsamen Portal gebündelt. Dank funktionaler Erweiterungen erkennt Microsoft Defender XDR Ransomware in SharePoint und OneDrive und sperrt dann den Zugriff.

Cloud-Systeme sind im Idealfall künftig sicherer als Inhouse-Komponenten, wie Breidohr erläutert: „Die Angebote von Microsoft sind ein Schritt in die richtige Richtung. Sofern ein

Unternehmen diese Lösungen mit allen aktuell möglichen Mechanismen der Authentifizierung aufsetzt, gibt es in der Cloud künftig einen Schutz, der durchaus den im hauseigenen Rechenzentrum übersteigen kann.“

Wenn Authentifizierung und Backups fehlen

Digitale Forensik war das Thema des folgenden Vortrags des rheinischen Security-Dienstleisters @-yet GmbH. Der Referent hat anhand von Praxisbeispielen beschrieben, wie sein Unternehmen nach einer Ransomware-Attacke vorgeht, und durch welche Einfallstore die Angreifer nach seinen Erfahrungen in Systeme eindringen. „Oft geht es dabei um Basics, dass beispielsweise ein Dienst aus dem Internet erreichbar ist, keine Multifaktor-Authentifizierung zum Einsatz kommt, oder dass kein abgesichertes Backup gefahren wird“, berichtet Haist. „Viele Angreifer verwenden Basis-Werkzeuge, um einen Server zu kapern und dann dort Ransomware zu installieren.“

Auch Maßnahmen, um eine erfolgreiche Attacke schnell zu entdecken, kamen zur Sprache: „Über ein Netzwerk-Monitoring lassen sich Anomalien aufdecken“, berichtet Haist. „Laufen beispielsweise nachts oder am Wochenende sehr viele Daten über die Firewall, obwohl kein besonderes IT-Projekt aktiv ist, sollten die Administratoren hellhörig werden.“

Ein Fehlalarm lässt die Taskforce schwitzen

Zwei Anwenderberichte von Mitgliedsunternehmen haben den Umgang mit Security-Alerts und das Wiederherstellen von kompromittierten Systemen beschrieben. Im ersten Bericht ging es um ein Unternehmen, das nach einer Sicherheitswarnung die Systeme heruntergefahren hat, und dann in einer Taskforce mit mehreren Mitarbeitern das Problem analysiert hat. „Die Kollegen sind davon ausgegangen, dass ihre Systeme gekapert wurden, weil das Skript, dass sie von einem Dienstleister bekommen haben, genau das angezeigt hat“, berichtet Haist. „In der Analyse haben sie dann gemerkt, dass das Skript fehlerhaft war und einen falschen Alarm gegeben hatte.“ Fazit daraus: Alarmmeldungen sollte man nicht blind vertrauen, sondern deren Echtheit möglichst früh verifizieren.

Der zweite Mitgliedervortrag hat beschrieben, wie ein Unternehmen nach einer Attacke seine Systeme wiederhergestellt hat. Ausgangspunkt war eine infizierte E-Mail, die ein Mitarbeiter angeklickt hatte, der sich anschließend beim IT-Support über eine hohe CPU-Last auf seinem Rechner beschwert hat. So wurde die Attacke schnell aufgedeckt und der Rechner vom Netz genommen. Dank eines Backups vom Vortag konnten die verschlüsselten Dateien im laufenden Betrieb wiederhergestellt werden. Dafür haben die Administratoren ein eigenes Skript programmiert.

Das nächste Treffen der Arbeitsgruppe IT-Security-Management findet am 14. März 2024 statt. Geplant ist ein Präsenztreffen mit Vorabend-Veranstaltung. Der Ort und die Themen werden noch festgelegt. *Jürgen Frisch*