Passwort-Reset nach Hacker-Angriff am Universitätsklinikum Düsseldorf

Mit IDM auf Attacken besser vorbereitet

In den IT-Applikationen eines Krankenhauses sind Informationen gespeichert, die zu den sensibelsten überhaupt gehören: Patientendaten. Jeder unbefugte Zugriff auf sie ist mit aller Kraft zu verhindern. Hier helfen Lösungen für Identity-Management (IdM). Sie überwachen Benutzerkonten engmaschig und regeln zentral, wer mit welchen Systemen arbeiten darf. Als das Universitätsklinikum Düsseldorf im Herbst 2020 einen Cyber-Angriff größeren Ausmaßes entdeckte, konnte durch ein solches System ein entscheidender Beitrag zum zügigen Wiederanlauf geleistet werden.

Frank Zscheile, blaupause-Redaktion, und Dr. Lisa Zimmermann, Teamleiterin IDM am UKD

Für die Vergabe von Zugangsrechten und die Verwaltung von Nutzer-Accounts setzt das Universitätsklinikum Düsseldorf (UKD) seit 2017 auf SAP IDM. SAP verwendet für sein Produkt noch die ursprüngliche Abkürzung IDM, geläufig ist für die Produktgattung inzwischen das Kürzel IAM (Identity-Access-Management). Aufgabe von IDM-/IAM-Lösungen: Sie sammeln und stellen Informationen darüber bereit, welche Accounts es im IT-Netzwerk gibt. Außerdem erteilen, überwachen und entziehen sie Personen/Personengruppen dedizierte Zugangsrechte zu einzelnen Anwendungen. Nicht zuletzt sollen sie verwaiste Administrations- oder Service-Konten auffinden und eliminieren – letztere sind solche für technische User (also keine echten Personen). Sie sind besonders schützenswert und werden von Hackern häufig als erste ins Visier genommen.

Wenn Active Directory kompromittiert ist

Innerhalb weniger Stunden führte ein Hacker-Angriff im UKD am 10. September 2020 zu einem weitreichenden Shutdown der IT-Systeme und zwang das Krankenhaus zur Abmeldung von der Notfallversorgung. Einige Monate zuvor hatte der externe Angreifer eine Citrix-Lücke im IT-System genutzt, um eine User-Kennung abzulegen und später zu verwenden. Schnell wurde deutlich, dass die Schäden gravierend waren. Insbesondere der zentrale Verzeichnisdienst des Klinikums, das Active Directory (AD), welches für die Verwaltung der Netzwerkzugänge zuständig ist, war kompromittiert. Es war davon auszugehen, dass die kompletten Zugangsdaten bei dem Angriff gekapert und dadurch bekannt geworden waren.

Golden-Ticket-Angriff verhindern

Was war zu tun? Ein kompletter Reset aller Passwörter von Zugangsdaten im AD für mehr als 13.000 Konten, und dies parallel zum Wiederaufbau und Restart der IT-Systeme. Die Alternative wäre ein Neuaufbau des AD gewesen, wobei aber auch hier neue Zugangsdaten hätten erzeugt und verteilt werden müssen. Ferner galt es zu Beginn des Resets, zunächst den sogenannten AD-Kerberos-User zurückzusetzen. Dieser ist für die Verschlüsselung der AD-Zugangsdaten (der Authentifizierungs-Tokens) zuständig. Haben Angreifende Zugriff auf ihn, können sie sich darüber jederzeit Zugriff auf alle anderen Konten verschaffen, auch auf Domänenadministratoren (= Golden-Ticket-Angriff). Ohne Kerberos-User-Reset also kein Reset der übrigen Passwörter – eine Vorgehensweise, die auch das BSI empfiehlt.

Die damit verbundenen Restriktionen stellten sich allerdings als schwierig heraus. Der Kerberos-Reset muss nämlich zweimal stattfinden, weil er eine Historie für die zwei zuletzt genutzten Passwörter besitzt. Nach dem ersten müssen zunächst alle alten Sessions ein- →

SAP IDM im IT-Netzwerk des UKD

Seit 2017 arbeitet das Universitätsklinikum Düsseldorf mit **SAP IDM als Berechtigungssystem**. Darin hat die IT-Abteilung die komplette Netzwerkstruktur des **Microsoft Active Directory (AD)** abgebildet, welches somit die wichtigste Datenquelle für das Berechtigungs-Management darstellt.
Hintergrund: Viele wichtige **Krankenhaus-Applikationen** (Dokumenten-Managementsystem, Patienten-Managementsystem) **authentifizieren sich über AD** und werden so automatisch mit den richtigen Daten versorgt. SAP IDM ist quasi der **Single-Point-of-Truth** und das zentrale **Informationssystem** für alle Personen, die im Klinikum IT-Ressourcen nutzen, solche aus dem medizinischen ebenso wie solche aus dem universitären (Forschungs-)Bereich.

mal abgelaufen sein, um das erste neue Passwort zu verwenden, erst dann darf das zweite Passwort zurückgesetzt werden. Theoretisch kann jemand, der noch Zugriff auf andere User hat, zwischen beiden Resets erfolgreich ein Golden Ticket verwenden.

Das BSI rät daher, während des gesamten Resets alle anderen Active-Directory-Konten zu deaktivieren sowie nach dem Kerberos-Reset sofort die übrigen auf einen Schlag zurückzusetzen. Das hätte jedoch dazu geführt, dass sich kein User bzw. keine Userin mehr am System hätte anmelden können – ein immenses Risiko für das Klinikum, vor allem wegen nicht mehr funktionierender Service-Konten.

Folgt auf „Stunde null“ „Stunde minus eins“?

Bezeichnet man den Moment eines Hacker-Angriffs gerne als „Stunde null“, wären die Auswirkungen dieser Reset-Maßnahme mit hoher Wahrscheinlichkeit noch verheerender gewesen – quasi die Stunde „minus eins“! Aus diesem Grund ist stets eine Risikoabschätzung vorzunehmen, ob auch eine abgeschwächte Variante möglich wäre. Dafür sprach die Tatsache, dass das UKD seit dem Angriff vom Internet getrennt war. So war davon auszugehen, dass die Angreifenden keinen eventuell noch vorhandenen Fernzugriff auf die IT-Systeme verwenden und den gesamten Vorgang zunichtemachen konnten. Auf die Deaktivierung der AD-Konten während des Kerberos-Resets wurde daher verzichtet. Die Passwortrücksetzung der übrigen Konten sollte sich zeitlich zwar direkt daran anschließen, aber nicht auf einen Schlag, sondern nur sukzessive durchgeführt werden.

Dem IAM-Team der IT-Abteilung des Universitätsklinikums oblag die Durchführung dieser Säuberungsmaßnahmen, die mit einem großen Planungsaufwand verbunden waren. Es war sicherzustellen, dass alle Zugangsdaten, die kompromittiert worden sind, ersetzt wurden. Außerdem musste garantiert werden, dass kein Angreifer bzw. keine Angreiferin mehr in der Lage war, sich neue Zugangsdaten zu verschaffen. Eine exakte Analyse aller AD-Konten und des mit dem Reset verbundenen Risikos war notwendig. Schließlich waren auch BSI-Vorgaben zu beachten, damit der Reset schlussendlich ein Erfolg werden konnte.

AD liefert zu wenig Überblick

Passwörter zurücksetzen ist für sich genommen keine Kunst, dies funktioniert auch mit Bordmitteln des Active Directory. Dazu braucht man allerdings einen detaillierten Überblick, welche Konten es gibt und in welchen Zusammenhängen diese auch zurückgesetzt werden dürfen, ohne irgendetwas zu zerstören – eine Abgrenzung, wie sie im Active Directory selbst zwar grundsätzlich möglich, in der IDM-Lösung aber viel umfangreicher zu verwalten ist. Sie hilft damit nicht per se gegen Angriffe, ist aber Gold wert bei der Vorbereitung auf einen solchen – indem mit ihr schon lange vor der Attacke kritische Accounts, die besonders kompromittierbar sind, aufgespürt und rechtzeitig deaktiviert werden.

Herausforderung bei den Personen-Accounts war es, die Zugangsdaten sicher an die einzelnen Beschäftigten zu bringen. Als Teil der KRITIS (Kritische Infrastrukturen) darf das UKD nämlich nicht einfach alle AD-Passwörter bei

Dr. Lisa Zimmermann, Teamleiterin IDM am Universitätsklinikum Düsseldorf

der nächsten Anmeldung ändern lassen. Dann hätte die Gefahr bestanden, dass sich jemand mit den vorhandenen Zugangsdaten direkt wieder die neuen Zugänge verschafft. Ein beträchtlicher Teil der Planung befasste sich daher damit, wie die neuen Passwörter erzeugt und so verteilt werden konnten, dass die User:innen sie sich zeitnah um den Zeitpunkt des Resets herum gegen Vorlage des Personalausweises abholen können – eine vor allem logistisch herausfordernde Aufgabe, denn zu diesem Zeitpunkt gab es noch keine COVID-19-Impfmöglichkeiten und es bestand erhebliche Ansteckungsgefahr.

Zwischen System- und Funktionskonten trennen

Der zweite Teil der Planung bezog sich auf die Vorbereitung des eigentlichen Resets. Es musste ein Zeitplan erarbeitet werden, in welcher Reihenfolge die Konten angefasst werden sollten. Hierzu wurden alle im Active Directory vorhandenen Konten erneut kategorisiert und im Hinblick auf den Reset priorisiert. Dabei half SAP IDM, durch dessen Einführung und Betrieb bereits umfassende Aufräumarbeiten dieser Art an den Benutzerdaten durchgeführt worden waren. Das so generierte Wissen über die Konten war bei der Planung von großem Nutzen, und das IAM-Team konnte sauber zwischen persönlich genutzten und sogenannten System- oder auch Funktionskonten trennen. Nur die persönlich genutzten Konten wurden für die klinikweite Passwortbriefausgabe genutzt. Die neuen Passwörter der Funktionskonten wurden hingegen nur in der IT selber ausgegeben und die Ausgabe entsprechend dokumentiert.

Auch den Passwort-Reset selbst führte das UKD mit SAP IDM durch und stellte darin entsprechende Funktionen bereit, so dass die Passwörter direkt in AD geschrieben und von dort Rückmeldungen zurückgeschrieben wurden. Das IDM-System bietet einen Standardweg für eine Passwortrücksetzung, der aber nicht für Massenrücksetzungen gedacht ist. Über den direkten Weg sollte vermieden werden, dass Fehlerbehebungen im Rahmen des Standardwegs zu Verzögerungen führen. So ließ sich sicherstellen, dass Konten nicht mehrfach zurückgesetzt oder vergessen wurden bzw. auf der Ausschlussliste standen.

Gelegenheit zum Aufräumen genutzt

Neben allen Herausforderungen, die der Reset mit sich brachte, gab es aber auch positive Nebenwirkungen. So wurde die Gelegenheit genutzt, notwendige Aufräumarbeiten in der Zugangsverwaltung vorzunehmen und wichtige Dokumentationen von Nutzerkonten zu ergänzen. Mit den gesammelten Erfahrungen im Hinterkopf entstand zugleich ein Notfallplan. Sollte also in Zukunft noch einmal ein Passwort-Reset dieses Umfangs nötig werden, dürfte er noch einmal um ein Vielfaches schneller ablaufen als der jüngste. ■

„Die Gremien der DSAG bieten eine exzellente Gelegenheit, mit Gleichgesinnten zu sprechen, welche die Erfahrungen zu 100 Prozent nachvollziehen können. Dies hat sich im UKD-Projekt als äußerst hilfreich erwiesen. Es geht uns in der Arbeitsgruppe darum, deutlich zu machen, wie wichtig Identitäts-Management ist, um auf Gefährdungssituationen künftig noch besser vorbereitet zu sein.“

Aydin Tekin, Sprecher der DSAG-Arbeitsgruppe IDM