Das Schweizer Fachmagazin für das Gesundheitswesen

a|s|p

Interview: Prof. Dr. oec. Alfred Angerer

«brennpunkt»: eHealth

«brennpunkt»: Datensicherheit

arztspitalpflege.ch 39. Jahrgang | 1 | 2021

2-Faktor-Authentifizierung von Gesundheitsfachpersonen

Eine 2-Faktor-Authentifizierung der Benutzer sollte beim Zugriff auf Cloud-Services im Gesundheitswesen zur Selbstverständlichkeit werden. Damit dies gelingt, benötigen Spitäler und Heime ein elektronisches Äquivalent zum Personalausweis.

Thomas Kessler (IT-Sicherheitsarchitekt und Partner, TEMET AG)*

Passwörter sind die Achillesferse der IT-Sicherheit

Beim Log-in mit Benutzername und Passwort beweist der Benutzer seine Identität, indem er ein Geheimnis preisgibt, nämlich sein persönliches Passwort. Ein geteiltes Geheimnis ist bekanntermassen kein Geheimnis mehr. Diese fundamentale Schwäche von Passwörtern führt immer wieder zu erfolgreichen Angriffen auf unsere IT-Systeme und ist mit ein Grund dafür, dass der Identitätsdiebstahl eines der Top-Ten-IT-Sicherheitsrisiken ist.

Seit Langem ist bekannt, dass solchen Angriffen mit einer sogenannten 2-Faktor-Authentifizierung (nachfolgend mit «2FA» abgekürzt) begegnet werden kann, wie sie beispielsweise beim E-Banking gebräuchlich ist. Als 2FA bezeichnen wir Verfahren, die einen Faktor «Haben» mit einem Faktor «Wissen» oder einem Faktor «Sein» kombinieren. Der Faktor «Haben» wird in jedem Fall benötigt, wobei es sich hierbei um Hardware (eine Smartcard, eine SIM-Karte oder ein anderes Token) oder Software (zum Beispiel eine Authenticator App) handeln kann. Der Faktor «Wissen» ist üblicherweise ein Passwort, das zentral auf einem Server oder dezentral auf einem persönlichen Gerät verwaltet und gegengeprüft wird; Letzteres wird auch als PIN bezeichnet. Der Faktor «Sein» schliesslich ist ein individuelles Körpermerkmal wie ein Fingerabdruck oder das Gesichtsbild.

Wo ist eine 2-Faktor-Authentifizierung angebracht?

Das Risiko eines Identitätsdiebstahls wird bewertet, indem die Eintretenswahrscheinlichkeit eines Schadenfalles mit dessen Tragweite multipliziert wird. Die Tragweite ist im Gesundheitswesen naturgemäss hoch, da es in vielen Fällen um den Zugriff auf besonders schützenswerte Personendaten geht.

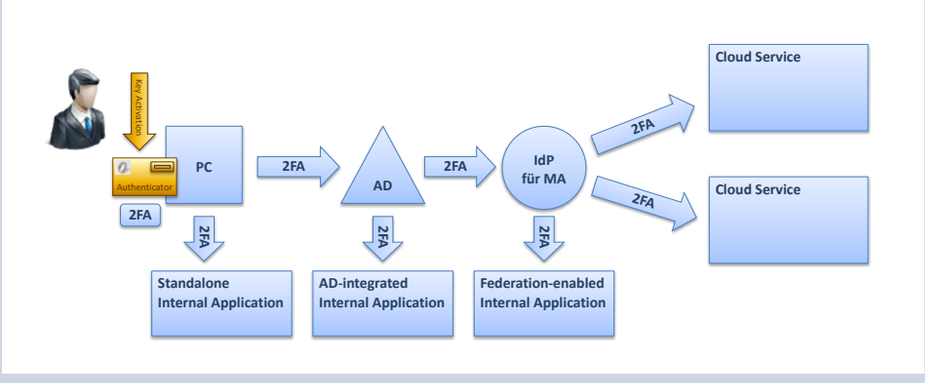

Abbildung 1: «2FA am Endgerät»

Die Eintretenswahrscheinlichkeit ist dann besonders gross, wenn ein IT-System im Internet exponiert und somit für die ganze Welt zugänglich ist. Dies trifft beispielsweise auf die meisten Remote-Access-Lösungen zu, weshalb eine 2-Faktor-Authentifizierung für diesen Anwendungsfall unbedingt zu empfehlen ist. Es trifft aber auch auf viele Cloud-Anwendungen zu wie beispielsweise das elektronische Patientendossier (EPD), wo deshalb aus gutem Grund eine 2FA gesetzlich vorgeschrieben ist.

Weniger klar ist die Situation bei der Nutzung von IT-Systemen innerhalb einer Organisation. Weil es immer schwieriger wird, die internen IT-Systeme vom Internet abzuschotten, sollte die 2-Faktor-Authentifizierung mittelfristig auch beim Log-in am Arbeitsplatz und an den internen Applikationen angestrebt werden. Die betrieblichen Anforderungen (Stichwort «Stations-PC») können eine solche Lösung allerdings sehr anspruchsvoll und zeitraubend machen.

Wie kann eine 2-Faktor-Authentifizierung erreicht werden?

Die Einführung einer 2FA einzeln für jedes IT-System sollte tunlichst vermieden werden, damit die Benutzer nicht von einer Flut von zusätzlichen «Log-in-Faktoren» überschwemmt werden: Eine übergreifende Infrastruktur tut Not! Hierfür gibt es zwei strategische Vorgehensvarianten:

- Bei der Variante «2FA am Endgerät» erfolgt die 2-Faktor-Authentifizierung bereits beim Log-in am Arbeitsplatz, typischerweise mittels Smartcard und PIN. Die mit zwei Faktoren authentifizierte

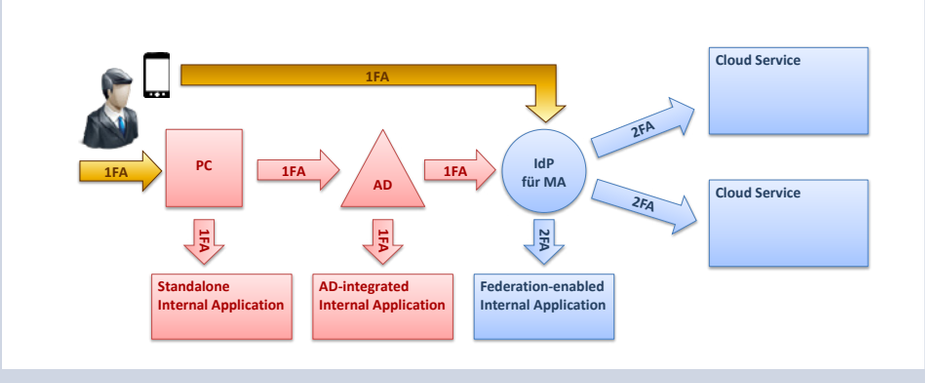

Abbildung 2: «2FA am IdP»

Identität des Benutzers wird anschliessend durch Infrastrukturkomponenten wie das Active Directory an alle daran angeschlossenen IT-Systeme weitergereicht (Single SignOn).
- Bei der Variante «2FA am IdP» meldet sich der Benutzer zunächst mit seinem Passwort oder einem biometrischen Merkmal am Arbeitsplatz an. Der zweite Faktor, häufig der Besitz einer Authenticator App, wird zu einem späteren Zeitpunkt auf einem sogenannten Identity Provider (IdP) geprüft.

Die betriebliche Einführung der zweiten Variante ist normalerweise deutlich einfacher. Sie bietet allerdings auch einen geringeren Sicherheitsnutzen, weil sich nur moderne IT-Systeme an einen IdP anschliessen lassen.

Die Sache mit dem digitalen Ausweis

Für die effiziente Implementierung einer 2-Faktor-Authentifizierung benötigen Spitäler und Heime das digitale Äquivalent zum Personalausweis: einen digitalen Personalausweis, der für die 2FA genutzt wird. Dieser wird von einer betriebsinternen Fachstelle (z.B. im HR) ausgestellt und enthält Informationen wie die Personalnummer oder die Organisationszugehörigkeit, die bei der Nutzung von IT-Systemen im beruflichen Kontext typischerweise benötigt werden.

Der digitale Personalausweis basiert zwar auf derselben Technologie wie der digitale Ausweis für Privatpersonen, der im Zusammenhang mit dem E-ID-Gesetz derzeit rege diskutiert wird. Die erheblichen Unterschiede zwischen einem Personalausweis und einem Reisepass in Bezug auf die Verantwortlichkeiten, die Verwaltungsprozesse und die Anwendungsfälle bestehen aber auch in der digitalen Welt und müssen bei einem 2FA-Einführungsprojekt unbedingt berücksichtigt werden. ■

***Thomas Kessler**
Thomas Kessler studierte Physik an der ETH Zürich und ist seit 30 Jahren als Projektleiter und Lösungsarchitekt in der IT-Sicherheit tätig. Er ist Gründer und Partner der TEMET AG in Zürich.

Ransomware bleibt ein Hauptphänomen für IT-Sicherheitsverletzungen

Das IT-Sicherheitsunternehmen Tenable veröffentlichte vor einigen Tagen in einem ausführlichen Report eine fundierte Analyse der signifikantesten Datensicherheitsverletzungen aus dem vergangenen Jahr.

Für diesen Bericht hat Tenable die veröffentlichten Meldungen über Sicherheitsverletzungen von Januar bis Oktober 2020 analysiert, um Trends zu erkennen. In den ersten zehn Monaten des Jahres 2020 gab es 730 Sicherheitsverletzungen, bei denen über 22 Milliarden Datensätze offengelegt wurden.

Tenable hat die Daten auf elf Branchenkategorien aufgeteilt, um ein umfassendes Bild davon zu erhalten, welche Branchen am meisten betroffen waren. Demnach entfiel der grösste Anteil der analysierten Datenschutzverletzungen auf das Gesundheitswesen und das Bildungswesen (25 Prozent bzw. 13 Prozent). Allein im Gesundheitswesen waren fast 8 Millionen Datensätze betroffen. Behörden (12,5 Prozent) und Technologieunternehmen (15,5 Prozent) waren ebenfalls häufige Ziele.

Aufgrund der Häufigkeit von Sicherheitsverletzungen im Gesundheitswesen in diesem Jahr hat Tenable eine weitere Ursachenanalyse durchgeführt und festgestellt, dass über 46 Prozent der Sicherheitsverletzungen in diesem Sektor durch Ransomware-Angriffe verursacht wurden. Andere führende Ursachen für Sicherheitsverletzungen im Gesundheitswesen waren die Kompromittierung von E-Mails (24,6 Prozent), Insiderbedrohungen (7,3 Prozent) und die Fehlkonfiguration von Anwendungen (5,6 Prozent).

Obwohl Ransomware im Jahr 2020 für Einrichtungen im Gesundheitswesen ein grosses Problem darstellt, ist keine Branche gegen diese Bedrohung immun. Zwei der wichtigsten Schwachstellen, die von Ransomware-Gruppen ausgenutzt werden, sind zwei VPN-Schwachstellen, die im Citrix ADC-Controller gefunden wurden und Gateway-Hosts (CVE-2019-19781) und Pulse Connect Secure (CVE-2019-11510) betreffen. Diese Schwachstellen sind ein Dreh- und Angelpunkt für nationalstaatliche Bedrohungsakteure, durchschnittliche Cyberkriminelle und Ransomware-Banden, die einen ersten Fuss in jede Art von Organisation setzen wollen.

Ungepatchte Schwachstellen stellen lukrative Möglichkeiten für kriminelle Akteure dar. Sophos-Forscher spekulieren, dass die Ransomware-Gruppe NetWalker, die sich im Jahr 2020 durch ihre erfolgreichen Datendiebstähle einen Namen gemacht hat, auf Schwachstellen in «weit verbreiteter, veralteter Server-Software» abzielt und nennt Apache Tomcat und Oracle WebLogic als Beispiele. (Beide Anwendungen erhielten 2020 Patches für kritische, schwerwiegende Sicherheitslücken). Sophos geht davon aus, dass NetWalker nicht nur diese Schwachstellen ausnutzt, sondern auch auf schwache RDP-Kennwörter abzielt. ■

Über Tenable

Tenable, Inc. ist das Cyber-Exposure-Unternehmen. Mehr als 30 000 Kunden auf der ganzen Welt vertrauen auf Tenable, wenn es darum geht, Cybersicherheitsrisiken zu verstehen und zu reduzieren. Als Erfinder von Nessus hat Tenable sein Fachwissen über Schwachstellen erweitert, um die weltweit erste Plattform zu liefern, die jedes digitale Asset auf jeder Computerplattform erkennen und schützen kann. Zu den Kunden von Tenable zählen mehr als 50 Prozent der «Fortune 500» Unternehmen, mehr als 30 Prozent der «Global 2000»-Unternehmen und grosse Regierungsbehörden. Erfahren Sie mehr unter www.tenable.com