ARBEITSPAPIER

Multifaktor-Authentisierung

Arbeitspapier Nr.: 1

Datum: 1. Dezember 2022

Autoren: Dr. Stefan Steiger (Universitätsrechenzentrum Heidelberg),
Johannes Häbe (Universitätsrechenzentrum Heidelberg),
Aaron Neuner (Universitätsrechenzentrum Heidelberg).

Institution: Kernteam Informationssicherheit - bwInfoSec

Inhaltsverzeichnis

Einleitung 1

Multifaktor-Authentisierung: Funktionsweise und Wirkung 1

Multifaktor-Authentisierung in der Praxis 3

Limitationen 4

Fazit 4

Quellenverzeichnis 5

Executive Summary:

Universitäten und Hochschulen werden immer häufiger zum Ziel von folgenreichen Cyberangriffen. Dieses Arbeitspapier skizziert die Möglichkeiten der Multifaktor-Authentisierung (MFA), diesen Herausforderungen zu begegnen. Die MFA kann ein wertvolles Werkzeug sein, wenn es darum geht, Angriffe zu verhindern bzw. deren Schadenswirkung zu reduzieren. Sie stellt Angreifer:innen bei der Infiltration eines Netzes bzw. bei der Ausbreitung und Rechteerweiterung vor substanzielle Herausforderungen. Bei der Einführung einer MFA im akademischen Kontext empfiehlt sich ein risikoorientiertes Vorgehen, das besonders exponierte und kritische Dienste bzw. Accounts priorisiert in den Blick nimmt. Es bleibt aber festzuhalten, dass Angriffe nach wie vor möglich sind und dass die Einführung einer MFA nicht nur initial Ressourcen benötigt, da beständig Support für die Lösung angeboten werden muss.

Einleitung

In jüngerer Vergangenheit hat die Häufigkeit von Cyberangriffen auf Universitäten und Hochschulen nicht nur in Deutschland deutlich zugenommen. Die Bildungseinrichtungen rücken dabei vermehrt in den Fokus, da sie einerseits essenzielle gesellschaftliche Wissensbestände generieren und verwalten sowie andererseits Ziele mit potenziell hoher öffentlicher Wahrnehmung darstellen. Sie sind daher sowohl für ökonomisch motivierte als auch für reputationsorientierte Angriffe attraktive Ziele (ZDNet 2022a; Hochschulforum Digitalisierung 2022). Erfolgreiche Cyberangriffe haben in den letzten Jahren mitunter zu massiven Beeinträchtigungen im akademischen Betrieb geführt. Sowohl Forschung als auch Lehre leiden erheblich unter den potenziell langwierigen Folgen, die mit einem solchen Angriff verbunden sein können. Die Schäden sind dabei nicht nur auf die Störung des regulären Betriebs begrenzt, sondern umfassen potenziell auch den Abfluss (kritischer) Daten sowohl aus der Forschung als auch der Verwaltung (Inside IT 2022). Woraus wiederum institutionelle Reputationsverluste folgen können.

Aufgrund der heterogenen und über Jahrzehnte gewachsenen Informationsinfrastrukturen sind Hochschulen und Universitäten attraktive Ziele für Angreifer:innen. Zwar werden etwa durch Beschaffungsrichtlinien und Rahmenverträge gewisse Vorgaben beim Aufbau von IT-Ressourcen und -Strukturen gemacht, vielfach aber leiten Forscher:innen aus der grundgesetzlich gewährten Freiheit oder aus wissenschaftlichen Fragestellungen die Möglichkeit ab, ihr Arbeitsumfeld technisch selbst zu gestalten (Hochschulforum Digitalisierung 2022). Hieraus können sich unterschiedliche Angriffsvektoren ergeben.

Analysiert man gängige Angriffsmuster fällt auf, dass viele der digitalen Attacken durch besser geschützte Konten verhindert bzw. zumindest erschwert werden könnten, da nicht immer direkt Schwachstellen (Sicherheitslücken oder Fehlkonfigurationen) in der IT als Einfallstor dienen, sondern oft zuerst Konten von Nutzer:innen übernommen werden, um Zugang zum Netz der Institutionen zu erlangen und um sich dann nach erfolgter Infiltration im Netz zu bewegen (IBM 2020).

Die Angriffsfläche ist in diesem Kontext für akademische Institutionen potenziell besonders groß, da nicht nur Mitarbeiter:innen ein Zugang zum Netzwerk gestattet werden soll, sondern auch einer erheblichen Zahl von Studierenden, denen Dienste zur Verfügung gestellt werden. Die verbesserte Absicherung von Accounts mittels Multifaktor-Authentisierung (MFA) kann daher einen signifikanten Beitrag zur Verhinderung von erfolgreichen Cyberangriffen leisten bzw. zumindest dabei helfen, deren Schaden zu begrenzen, wenn besonders relevante Zugänge (bspw. von Admins) zusätzlich abgesichert werden.

Multifaktor-Authentisierung: Funktionsweise und Wirkung

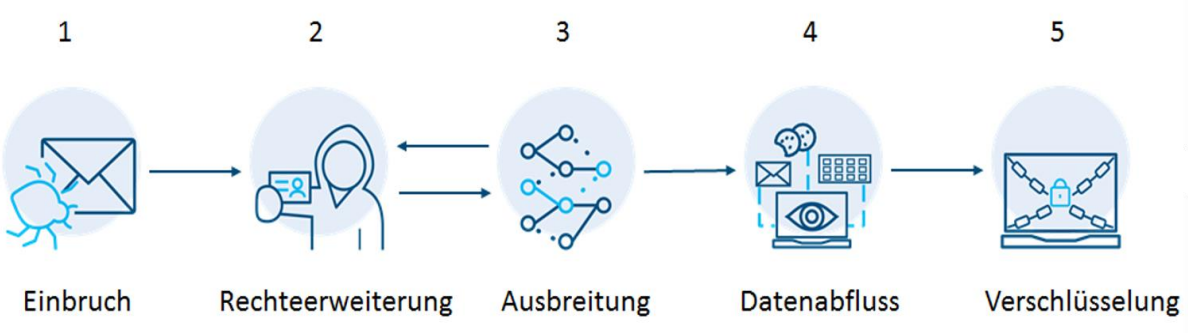
Die Einrichtung einer MFA schützt Accounts zusätzlich zum Passwort mit einem weiteren Merkmal, über das nur die/der Nutzer:in verfügt. Die Faktoren stammen dabei aus unterschiedlichen Kategorien: Wissen, Besitz oder Biometrie (BSI 2022e). Oftmals kommen in diesem Kontext bspw. auf das Smartphone übertragene, nur kurzfristig gültige Passwörter (TOTPs[1]) zum Einsatz. Der Besitz des Smartphones ergänzt in diesem Fall die Kennung und das Passwort (Wissen). Diese temporären Passwörter werden nach dem erfolgreichen „normalen" Login abgefragt, bevor Nutzer:innen die eigentlichen Dienste in Anspruch nehmen können. Angreifer:innen reicht dann zum Übernehmen eines Kontos nicht mehr nur eine Kombination aus Nutzerkennung und Passwort. Nationale wie internationale Institutionen

[1] Die Abkürzung TOTP steht für Time-based One-time Password Algorithmus.

weisen daher seit längerem wiederholt auf die Bedeutung von MFA zur Absicherung von Accounts im privaten wie beruflichen Kontext hin (BSI 2022b; Europol 2020; CISA 2022; NCSC 2022).

Das BSI unterteilt den Ablauf eines typischen Ransomware-Angriffs in fünf Phasen (s. Abb. 1). Die Phasen 1-4 stehen dabei aber exemplarisch nicht nur für die Verbreitung von Ransomware, sondern werden bei sehr vielen Cyberangriffen durchlaufen. Die Einrichtung einer MFA kann in den beiden Frühphasen von Attacken deren erfolgreiche Durchführung deutlich erschweren bzw. die Konsequenzen reduzieren.

Abbildung 1: Schematische Darstellung eines Ransomware-Angriffs



Quelle: BSI 2022d

Zum Einbruch in Systeme greifen Täter:innen oft auf erbeutete Zugangsdaten zurück. Sind die Netzzugänge mit einer MFA versehen, ist dies nicht mehr so einfach möglich. Ferner wird die Ausbreitung im Netz und die Erlangung von besonderen Rechten erschwert, wenn diese Accounts mittels MFA geschützt werden (BSI 2022d). Die MFA bietet damit einen vergleichsweise simpel zu implementierenden und je nach gewählter Technologie potenziell kostengünstigen Schutzmechanismus gegen die meisten Arten von Attacken auf Grundlage erbeuteter Kontoinformationen. So schützt MFA besonders effektiv gegen Angriffe mit in Datenleaks kompromittierten Zugangsdaten, da diese allein nicht mehr ausreichend sind, um sich Zugang zu Accounts zu verschaffen.

Empirisch lässt sich die Wirksamkeit der Maßnahme klar nachweisen. So berichtet Google von einer Reduktion kompromittierter Accounts um 50 %, nach Einführung der MFA für etwa 150 Millionen Nutzer:innen (Google 2022). Auch andere Quellen bestätigen die Effektivität einer MFA. Nach Angaben des Europol European Cybercrime Centre (EC3) konnte bei Ermittlungen beobachtet werden, dass Cyberkriminelle bei einer Ransomware-Attacke aufgaben, als sie mit einer MFA konfrontiert waren (ZDNet 2022b). Die MFA erhöht den Aufwand für Angreifer:innen also deutlich und kann so abschreckend wirken.

Technisch steht eine Vielzahl von Lösungen zur Verfügung, die jeweils unterschiedliche Sicherheitsanforderungen erfüllen, mit unterschiedlichen Aufwänden bei der Implementierung bzw. dem Betrieb verbunden sind und die unterschiedliche finanzielle Investitionen erfordern. Die Optionen reichen hier von Hardwaretokens bis zu softwaregestützten Verfahren, bspw. TOTP. Die hardwarebasierten Lösungen sind dabei meist mit größeren Investitionen verbunden als die softwarebasierten Verfahren, bringen aber in der Regel einen Sicherheitsvorteil. Das BSI hat diverse MFA-Verfahren mit Blick auf unterschiedliche Kriterien ausgiebig geprüft und deren Vor- und Nachteile evaluiert. Diese Betrachtung kann bei der Entscheidung über die Wahl einer passenden Lösung für die technische Ausgestaltung hilfreich sein und Orientierung geben (BSI 2022c).

Multifaktor-Authentisierung in der Praxis

Nicht alle im Kontext einer Universität oder Hochschule betriebenen Dienste können und müssen unmittelbar mit einer MFA versehen werden. Aus technischer Perspektive bieten viele gängige Authentifizierungsverfahren die Möglichkeit, eine MFA zu integrieren. Auch im akademischen Kontext gängige Verfahren wie LDAP, Shibboleth oder Kerberos bieten die Möglichkeit einer MFA-Anbindung.

Stehen einer Einführung keine technischen Gründe entgegen, bietet sich ein risikoorientiertes Vorgehen bei der Identifikation relevanter Dienste und Accounts an. Eine Risikoanalyse auf Basis des IT-Grundschutz kann hier die Entscheidungsfindung anleiten (BSI 2017). Prinzipiell kann der Netzzugang in fast allen Institutionen ein Ansatzpunkt sein. In allen Universitäten und Hochschulen werden Zugangsmöglichkeiten zur dezentralen Nutzung des Netzes der Institution via Virtual Private Network (VPN) angeboten. Diese stellen auch bevorzugte Angriffsvektoren dar, deren Absicherung daher generell sinnvoll sein kann. Ferner sind die Systeme der Finanzbuchhaltung für Angreifer:innen ebenso lohnende Ziele wie die Admins zentraler Dienste. In diesen Kontexten kann die Nutzung einer MFA daher ebenfalls lohnenswert sein.

Mit einer MFA ist für die Nutzer:innen ein aufwändigeres Anmeldeverfahren verbunden. Es kommt daher auch auf die Akzeptanz an. Eine repräsentative Umfrage der Verbraucherzentrale ergab, dass vielen MFA-Verfahren von Nutzer:innen eine gute oder gar sehr gute Nutzerfreundlichkeit attestiert wird. Die höchsten Zustimmungswerte erzielen hierbei Lösungen, die auf biometrische Merkmale (bspw. den Fingerabdruck) oder SMS zurückgreifen. Aber auch softwaregestützte Varianten wie TOTP sind aus Sicht von mehr als 60 % der User:innen nutzerfreundlich. Aus Sicht der Anwender:innen stellen Hardwaretokens die aufwändigsten Lösungen dar und erreichen die geringsten Zustimmungen (Verbraucherzentrale 2021). Auch wenn es naheliegend und kostengünstig ist, kann aber auch der Rückgriff auf die privaten Smartphones der Nutzer:innen zu Unzufriedenheit führen (Weidman und Grossklags 2017). Verschiedene Studien haben sich mit der Einführung einer MFA in einer akademischen Institution befasst und dabei auch die Akzeptanz der neuen Verfahren beleuchtet (Weidman und Grossklags 2017; Colnago et al. 2018). Die Studien haben sich dabei auf die Einführung einer MFA für Mitarbeiter:innen fokussiert und nicht die großflächige Implementierung im Kreis der Studierenden untersucht. Die analysierten Universitäten hatten sich gegen die Einführung der MFA für Studierende entschieden, da bei einem Rückgriff auf deren Smartphones mit substanzieller Kritik gerechnet wurde (Weidman und Grossklags 2017). Beide Studien zeigen aber, dass die MFA zwar mit einem erhöhten Aufwand bei Anmeldungen verbunden ist, dass Nutzer:innen aber relativ schnell an das neue System gewöhnt waren. Je mehr die Anwender:innen in unterschiedlichen Kontexten mit der MFA in Berührung kommen, umso mehr scheinen die Bedenken und Vorbehalte in den Hintergrund zu treten. Die Häufigkeit der Abfrage des ergänzenden Faktors beeinflusst ebenfalls die Bereitschaft zur Nutzung einer MFA. Eine der untersuchten Universitäten entschied sich bspw. dafür, den ergänzenden Faktor alle acht Stunden abzufragen, also etwa einmal pro Arbeitstag. Hier ist eine Abwägung zwischen Sicherheitsinteressen und Erwägungen der Nutzbarkeit erforderlich (Colnago et al. 2018). Insgesamt ist es wichtig, den Prozess der Implementierung kommunikativ eng zu begleiten und frühzeitig Akzeptanz zu schaffen.

Es sollte zudem bedacht werden, dass insbesondere zu Beginn die Support-Anfragen stark steigen können. Unmittelbar nach Einführung der MFA betrafen an einer Universität fast ein Viertel der Anfragen diese Thematik (Colnago et al. 2018, S. 8). Ferner bleibt auch nach der Einführung eine erhöhte Belastung des Supports, da einige Probleme kontinuierlich auftreten. So muss etwa ein Prozess zur Wiederherstellung von Accounts definiert werden, bspw. im Falle des Verlusts eines Smartphones. Dieser Wiederherstellungsprozess muss ebenfalls sicher gestaltet werden, da er potenzielles Ziel von Angrif-

fen werden kann. Ferner sollten Prozesse für den Fall einer Störung der MFA etabliert werden, insbesondere für besonders zeitkritische Dienste. Generell stellt die Einführung einer MFA damit zusätzlichen Aufwand bei der Administration von Accounts dar und ist mit erhöhtem Personalbedarf verbunden. Der Einsatz einer MFA ist letztlich nicht nur mit einem Initialaufwand verbunden, sondern bedarf einer kontinuierlichen Pflege.

Limitationen

Auch wenn der Einsatz einer MFA einen deutlichen Gewinn bei der Absicherung von Accounts bedeutet, macht sie Angriffe nicht unmöglich. Generell ist eine MFA leicht auszuhebeln, wenn die Faktoren nicht getrennt und bei einem Angriff zusammen erbeutet werden. Ferner können die Mechanismen der MFA unterlaufen werden, wenn bspw. Smartphones, die als ergänzender Faktor verwendet werden, mittels Schadsoftware bereits von Angreifer:innen übernommen worden sind. Die Schwachstelle Mensch kann nach wie vor via Social Engineering ausgenutzt werden. Die Nachbildung von Anmeldeseiten bildet hier einen potenziellen Angriffspunkt. In einem solchen Szenario können bspw. abgegriffene Logindaten von Nutzer:innen inkl. des ergänzenden Faktors (bswp. bei TOTP, HOTP[2] oder SMS-Codes) sofort weitergeleitet und zur Anmeldung genutzt werden, wie bei einem prominenten Angriff auf Twitter im Jahr 2020 (ZDNet 2020). Phishing-Angriffe können hier aber nur noch in Echtzeit erfolgreich sein, was einen Angriff deutlich erschwert. Bei besonders hohem Schutzbedarf ist ein Security-Token gegenüber einer Smartphone-Authenticator-App zu bevorzugen. Ein Security-Token verfügt über keine Internetschnittstelle und bietet damit einen Angriffsvektor weniger als eine Smartphone-Authenticator-App. Außerdem können Security-Tokens (FIDO2[3]) laut BSI Schutz gegen Real-Time-Phishing bieten (BSI 2022a).

Fazit

Auch wenn die MFA kein Allheilmittel gegen Cyberangriffe darstellt, ist sie ein wertvolles Werkzeug zur Verhinderung erfolgreicher Angriff bzw. zur Reduktion der potenziellen Schäden. Sie kann den Zugang zum und die Ausbreitung im Netz einer Institution signifikant erschweren und so Angriffe ggf. sogar gänzlich abschrecken. Hochschulen und Universitäten sollten angesichts steigender Angriffszahlen und potenziell erheblicher Schäden bei erfolgreichen Attacken die Einführung einer MFA für besonders exponierte bzw. kritische Dienste erwägen. Es ist allerdings wichtig, darauf zu achten, dass die Akzeptanz der Nutzer:innen gewahrt bleibt und dass die, mit der Nutzung einer MFA verbundenen, zusätzlichen Aufgaben dauerhaft Ressourcen in Anspruch nehmen.

[2] Die Abkürzung HOTP steht für HMAC-based One-time Password Algorithmus.
[3] Die Abkürzung FIDO steht für Fast IDentity Online.

Quellenverzeichnis

BSI (2017): BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf.

BSI (2022a): Bewertungstabellen 'IT Sicherheit' im Rahmen der Technischen Bewertung von Verfahren zur Zwei-Faktor-Authentisierung. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/2FA/it-sicherheit.pdf.

BSI (2022b): Die Lage der IT-Sicherheit in Deutschland 2022. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf.

BSI (2022c): Technische Betrachtung: Wie sicher sind die verschiedenen Verfahren der 2-Faktor-Authentisierung (2FA)? Online verfügbar unter https://www.bsi.bund.de/dok/11693908.

BSI (2022d): Top 10 Ransomware-Maßnahmen. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/Top-10-Ransomware-Massnahmen/top-10-ransomware-massnahmen.html.

BSI (2022e): Zwei-Faktor-Authentisierung: Mehr Sicherheit für Online-Konten und vernetzte Geräte. Online verfügbar unter https://www.bsi.bund.de/dok/11693908.

CISA (2022): Multifactor Authentication. Online verfügbar unter https://www.cisa.gov/mfa.

Colnago, Jessica; Devlin, Summer; Oates, Maggie; Swoopes, Chelse; Bauer, Lujo; Cranor, Lorrie; Christin, Nicolas (2018): “It's not actually that horrible”: Exploring Adoption of Two-Factor Authentication at a University. In: Regan Mandryk, Mark Hancock, Mark Perry und Anna Cox (Hg.): Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. CHI '18: CHI Conference on Human Factors in Computing Systems. Montreal QC Canada, 21 04 2018 26 04 2018. New York, NY, USA: ACM, S. 1–11.

Europol (2020): Safe Teleworking: Tips and Advice for Businesses. Online verfügbar unter https://www.europol.europa.eu/cms/sites/default/files/documents/safe-telework_employers.pdf.

Google (2022): Google auto-enabled 2SV for over 150M people leading to 50% decrease in compromised accounts. Online verfügbar unter https://9to5google.com/2022/02/08/google-account-2sv/.

Hochschulforum Digitalisierung (2022): Hochschulen im Visier von Cyberkriminalität: Warum Lehr- und Forschungsinstitutionen zu Zielen werden. Online verfügbar unter https://hochschulforumdigitalisierung.de/de/blog/hochschulen-im-visier-von-cyberkriminalitaet.

IBM (2020): IBM X-Force: Stolen Credentials and Vulnerabilities Weaponized Against Businesses in 2019. Online verfügbar unter https://newsroom.ibm.com/2020-02-11-IBM-X-Force-Stolen-Credentials-and-Vulnerabilities-Weaponized-Against-Businesses-in-2019.

Inside IT (2022): Nach Cyberangriff: Universität Neuenburg bestätigt Datenabfluss. Online verfügbar unter https://www.inside-it.ch/nach-cyberangriff-universitaet-neunburg-bestaetigt-datenabfluss.

NCSC (2022): Setting up 2-Step Verification (2SV). Online verfügbar unter https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv.

Verbraucherzentrale (2021): Zwei-Faktor-Authentisierung. Online verfügbar unter https://www.vzbv.de/sites/default/files/2022-03/21-08-31_2FA-Chartbericht_freigegeben_0.pdf.

Weidman, Jake; Grossklags, Jens (2017): I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. In: Proceedings of the 33rd Annual Computer Security Applications Conference. ACSAC 2017: 2017 Annual Computer Security Applications Conference. Orlando FL USA, 04 12 2017 08 12 2017. New York, NY, USA: ACM, S. 212–224.

ZDNet (2020): How the FBI tracked down the Twitter hackers. Online verfügbar unter https://www.zdnet.com/article/how-the-fbi-tracked-down-the-twitter-hackers/.

ZDNet (2022a): Ransomware attacks are hitting universities hard, and they are feeling the pressure. Online verfügbar unter https://www.zdnet.com/article/ransomware-attacks-are-hitting-universities-hard-and-they-are-feeling-the-pressure/.

ZDNet (2022b): These ransomware hackers gave up when they hit multi-factor authentication. Online verfügbar unter https://www.zdnet.com/article/why-you-really-need-multi-factor-authentication-these-ransomware-hackers-gave-up-when-they-saw-it/.

bwInfoSec

bwInfosec
Kernteam Informationssicherheit

https://bwinfosec.de

Standorte:

Universitätsrechenzentrum Heidelberg
Im Neuenheimer Feld 330
69120 Heidelberg
kernteam@urz.uni-heidelberg.de

Hochschulservicezentrum Baden-Württemberg
Alteburgstraße 150
72762 Reutlingen

Dezember 2022