MULTI-FAKTOR-AUTHENTIFIZIERUNG

SCHÜTZEN SIE DEN RUF IHRES UNTERNEHMENS UND IHRE UNTERNEHMENSWERTE IN DER DIGITALEN WELT

«Es gibt zwei Arten von Unternehmen: diejenigen, die gehackt wurden und diejenigen, die nicht wissen, dass sie gehackt wurden.»[1]
– John Chambers, ex-CEO Cisco

EINLEITUNG

WAS MUSS GESCHÜTZT WERDEN?

Verstösse gegen die Datensicherheit sind alltäglich, schwer zu verhindern und zunehmend schwieriger zu erkennen. Die Studie des Ponemon Institutes über die Kosten von Verstössen der Datensicherheit von 2016[2] zeigt, dass:

- **die durchschnittlichen Gesamtkosten einer Datenschutzverletzung 3.57 Mio € betragen**
- **die Gesamtkosten einer IT-Sicherheitslücke sind seit 2013 um 29% gestiegen**
- **die durchschnittlichen Kosten je verlorenem oder gestohlenem Datensatz 144.– € betragen**

Ein Bericht des Identity Theft Ressource Center's vom Dez. 2015 deckte auf, das es im Jahr 2015 zu 780 Datenschutzverletzungen kam, im Zuge derer 177.866.236 Datensätze offengelegt worden sind.
Parallel dazu verwies das Identity Theft Resource Center in seinem Bericht vom Dezember 2015[3] auf 780 Datenschutzverletzungen in diesem Jahr, die zu 177.866.236 offengelegten Aufzeichnungen führten. IT-Sicherheitslücken und Datenschutzverletzungen hatten in der Vergangenheit Auswirkungen auf alle Branchen, von denen das Gesundheitswesen, der Banken- und der öffentliche Sektor am stärksten betroffen waren.

Wie die untenstehende Tabelle zeigt, haben Datenschutzverletzungen schwerwiegende Folgen für Mitarbeiter und Kunden gleichermassen:
Einige Unternehmen wie z. B. der Einzelhändler Target schätzten ihre Verluste aufgrund von Datenschutzverletzungen im Jahre 2013 auf mehr als 223 Mio €.[4]

MITARBEITER	KUNDEN
Bricht Datenschutzgesetze, das mögliche strafrechtliche Konsequenzen nach sich zieht	Potenzielles Risiko rechtlicher Konsequenzen und einer möglichen Sammelklage
Veröffentlichte sensible Daten über Gesundheit, Gehalt, Überprüfung und Bankverbindung	Negative Berichte in den sozialen Medien und in der Presse, mögliche Verweigerung des Versicherers, Versicherungsschutz zu leisten, wenn bereits bestehende Symptome aufgedeckt werden
Leistung, Effizienz und Moral beeinflusst - Manche könnten das Unternehmen verklagen	Erhöhte Arbeitsbelastung des Kundenservice (Bearbeitung von Anrufen/E-Mails unzufriedener Kunden)
Mitarbeiterhaltung beeinträchtigt – Mitarbeiter könnten den Glauben an die «Sorgfaltspflicht» der Organisation verlieren	Es könnte noch auf andere Konten zugegriffen werden - die Auswirkungen könnten über die anfängliche Datenschutzverletzung hinausgehen
Personalbeschaffung bedroht - Verstoss kann auf Webseiten wie glassdoor.com thematisiert werden, was die Anwerbung von Spitzenkräften beeinträchtigt	Verringertes Kundenvertrauen und Net Promoter Score

[1] http://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html
[2] Ponemon Institute «Cost of a Data Breach» Studie, 15. Juni 2016
[3] Identity Theft Resource Center December 2015 Report, veröffentlicht am 29. Dezember 2015
[4] https://www.internetretailer.com/commentary/2015/05/21/key-takeaways-target-settlement-retailer

SECURITY SERVICES AG
CLUE

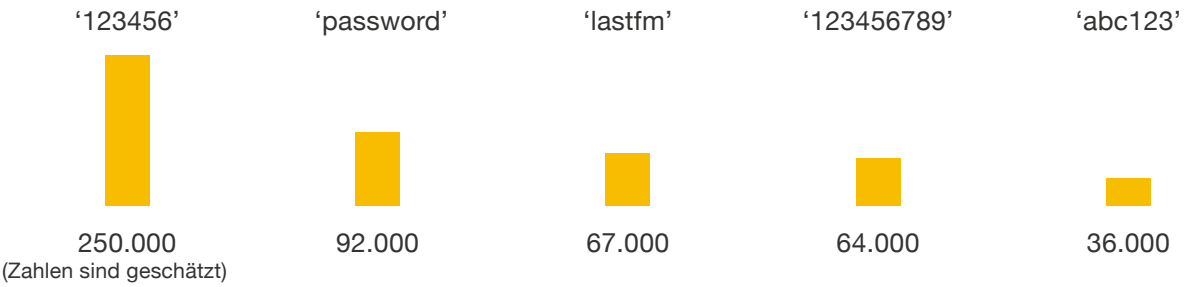
Eine aktuelle, im Auftrag von BAE Systems durchgeführte, Umfrage[1] von 300 Managern in der Finanzdienstleistungs-, Versicherungs- und IT/ Techbranche in den USA stellte fest, dass 85% der Befragten Rufschädigung als das auffälligste Ergebnis einer Datenschutzverletzung anführten, wobei 74% der Befragten eine gesetzliche Haftung als zweitgrösstes Problem benannten.

«Erstaunliche 397 Milliarden € kostet Cyber-Kriminalität die Weltwirtschaft hochgerechnet!» Um diesen Betrag in Relation zu setzen, Russlands Staatshaushalt betrug für das Jahr 2014 392 Milliarden €. Mit Gewinnen dieser Grössenordnung ist es nicht nur leicht zu verstehen, warum Cyberkriminalität eine solche zerstörerische Kraft für Unternehmen weltweit ist, sondern auch warum dieses «Geschäft» so lukrativ ist und warum sich immer mehr Kriminelle im Darknet aktiv werden.»[2]

WESHALB ALSO GESCHEHEN DATENSCHUTZVERLETZUNGEN?

«BEI 63% ALLER VERSTÖSSE LIEGT DIE VERWENDUNG EINES SCHWACHEN, STANDARDMÄSSIGEN ODER GESTOHLENEN PASSWORTS ZUGRUNDE.»
– Verizon Data Breach Investigations Report (DBIR), April 2016

Ein wichtiger Grund für eine grosse Anzahl von Datenschutzverletzungen ist immer noch die Nutzung von ausschliesslich Username & Passwort. Der Bericht der Verizon liefert handfeste Beweise die diese These untermauern. Im Fall der IT-Sicherheitsbruchs bei Last.fm[3] zeigte die Analyse der Passwörter ein wohl bekanntes Phänomen bei der Wahl des Passwortes:



(Zahlen sind geschätzt)

Auf der einen Seite könnte man Benutzer des Systems achtlos bezeichnen. Auf der anderen Seite muss man darauf hinweisen das im Zuge der zunehmenden Digitalisierung die Anzahl der zu merkenden Passwörter im privaten und im geschäftlichen Bereich immens zugenommen hat. Die Arbeitgeber erwarten von den Anwendern, dass sie Passwörter wählen, an die sie sich nicht mehr erinnern können und sagen ihnen anschliessend, dass sie diese nicht aufschreiben dürfen, sodass es vielleicht keine Überraschung ist, dass sie nicht den Organisationsrichtlinien folgen.

[1] https://hbr.org/2016/09/cybersecurity-is-every-executives-job
[2] https://www.lookingglasscyber.com/blog/the-global-cyber-crime-underground-what-are-they-and-what-do-they-sell/
[3] http://thehackernews.com/2016/09/lastfm-hacked.html

Durch die Befolgung der Best-Practice Richtlinien der OWASP1 verkomplizierten einige Unternehmen diesen Prozess noch zusätzlich, indem sie fordern, dass das Passwort mindestens 3 der folgenden 4 Komplexitätsregeln erfüllen muss:

- mindestens 1 Grossbuchstabe (A-Z)
- mindestens 1 Kleinbuchstabe (a-z)
- mindestens 1 Ziffer (0-9)
- mindestens 1 Sonderzeichen (Zeichensetzung)
- mindestens 10 Zeichen
- höchstens 128 Zeichen
- nicht mehr als 2 identische Zeichen in einer Reihe (z. B. ist 111 nicht erlaubt)

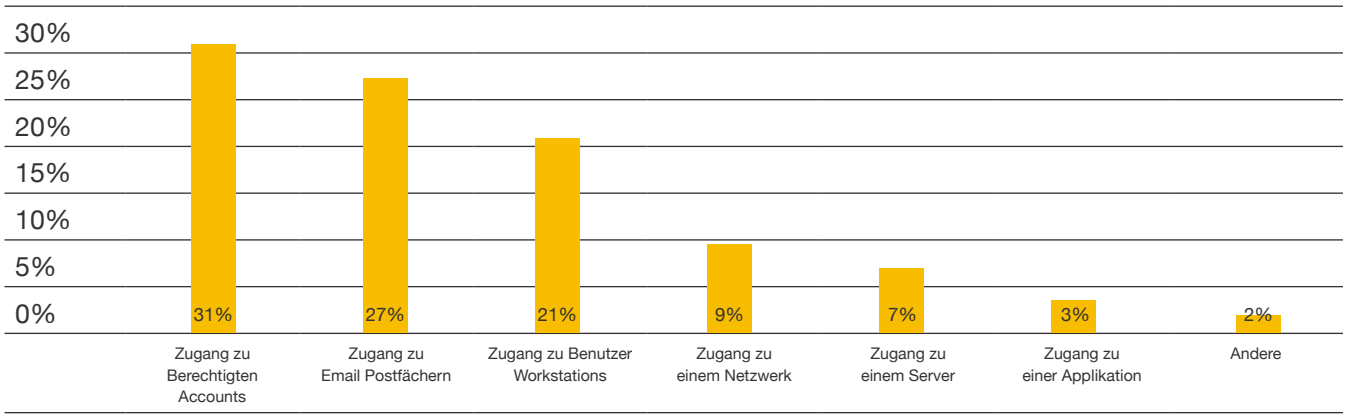
Allerdings verursachen diese Regeln tatsächlich noch mehr Probleme, weil sie es schwerer machen, sich an Passwörter zu erinnern.

Es bestehen noch zwei weitere wichtige Probleme, die von dem alten Denken herrühren, dass Passwörter oft gewechselt werden müssen. Das Erste ist ein ökonomisches Problem. Wie Cormac Herley[2] zeigte, sollten wir die Zeit des Anwenders nicht als «Freizeit» betrachten, da seine Zeit sehr kostspielig ist und regelmässig erzwungene Passwortänderungen nicht nur viel Geld kosten, sondern auch nichts bringen, wenn die Angreifer die Anmeldedaten nicht in der Zwischenzeit nutzen (was höchst unwahrscheinlich ist). Das zweite Problem konzentriert sich auf die Tatsache, dass Passwortänderungen dazu führen, dass Benutzer versuchen, auf die einfachste Art und Weise ein Passwort zu ändern, das heisst, dass diese bei der Aktualisierung sehr vorhersehbar sind. Eine Studie von Yinqian Zhang, Fabian Monrose und Michael K. Reiter[3] von der University of North Carolina führte aus: «Im Durchschnitt können wir bei einem Online-Angriff bei 41% aller Konten neue Passwörter anhand alter Passwörter mit einem erwarteten Zeitaufwand von weniger als 3 Sekunden pro Konto erraten». Vereinfacht ausgedrückt haben Anwender aller Voraussicht nach eine Zahl oder ein Symbol oder die nächstfolgende Nummer an das Ende des alten Passworts angehängt, z. B. wird MartinHenkel[1] zu MartinHenkel[2], was einen hohen Gradan Entropie aufweist (Passwortvorhersagbarkeit).

EINE UMFRAGE UNTER HACKERN

Auf der Hacking Konferenz BlackHat im Jahr 2017 in Las Vegas, USA wurden mehr als 250 WhiteHat und BlackHat Hacker dazu befragt, welche Mechanissmen wirklich funktionieren, um kritische Daten zu schützen.

Fast ein Drittel aller Befragten gaben an, Zugang auf privilegierte Accounts ist die erste Wahl für den einfachsten Weg um an sensitive Daten zu gelangen. Nah gefolgt gaben 27% der Befragten an, Zugang auf Email Konten eines Unternehmens wäre der leichteste Weg um an die Daten eines Unternehmens zu gelangen.



[1] https://www.owasp.org/index.php/Authentication_Cheat_Sheet
[2] http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf
[3] http://cs.unc.edu/~fabian/papers/PasswordExpire.pdf

DIE FRAGEN

Die Hacker wurden gefragt: Welche der Folgenden sind am häufigsten für Security-Breaches verantwortlich?
Da Perimeter Security Technologien bereits als irrelevant genannt wurden, fokusieren sich Hacker weitgehenst darauf, Zugang zu priviligierten Accounts und Email Passwörtern zu erhalten, indem sie Menschliche Schwachstellen ausnutzen. Mehr als 85% der befragten Personen gaben an, Menschen seien das grösste Sicherheits Risiko für die Unternehmens-IT.

Welche Art von IT-Security Mechanissmus ist am schwierigsten zu überwinden?
Da Hacker vermehrt privilegierte Accounts und Benutzer Passwörter attackieren, überrascht es nicht, dass die Technologien, welche am schwierigsten zu knacken sind, Multi Faktor Authentifizierung (38%) und Verschlüsselung (32%) sind.

EIN EINZELNES PASSWORT WEIST MEHERER SCHWACHPUNKTE AUF:

Leicht zu hacken: wie bereits erwähnt, verwenden die meisten Benutzer die gleichen Passwörter wieder und nehmen nur geringfügige Änderungen vor, wenn sie diese aktualisieren müssen oder ein neues Konto eröffnen sollen.

Teilen: insbesondere im Fall von unternehmensbezogenen Anwendungen können Anmeldeinformationen unter Umständen von einem Teammitglied an ein anderes in der irrigen Ansicht weitergegeben werden, dass dies weniger Zeitaufwand für die Administration bedeutet und möglicherweise Lizenzgebühren spart. Tatsächlich schafft dies die Möglichkeit, dass sowohl Informationen an Dritte weitergegeben werden als auch, dass nicht mehr eindeutig bestimmt werden kann, wer sich eigentlich zu einem bestimmten Zeitpunkt angemeldet hat.

Schwer zu merken: wie bereits erwähnt, birgt das Aufzwingen eines übermässig komplizierten Passworts das Risiko, dass ein Passwort nicht angenommen oder vergessen wird (sowie verlorene Produktivität oder einen frustrierten Kunden, der es zurücksetzen muss) oder Sicherheitsrisiken, wenn es irgendwo aufgeschrieben werden muss.

Credential stuffing: Sobald ein Passwort gehackt worden ist, ist sehr oft mehr als ein Konto in Gefahr. Eine Studie von Experian aus dem Jahr 2012[1] ergab, dass Anwender schon damals im Durchschnitt 25 Passwörter für verschiedene Zwecke/Systeme benötigen. Das ist eine grosse Anzahl an Passwörtern, die man sich zu merken hat und daher kommt es nicht überraschend, dass das gleiche Passwort für etwa fünf unterschiedliche Logins verwendet wurde. Diese Wiederverwendung von Passwörtern hat zu einem Anstieg von «Credential Stuffing» geführt, bei dem ein Hacker,sobald er sich erst einmal Zugriff auf ein Konto verschafft hat, versucht, auf andere populäre Konten zuzugreifen (man denke für den Anfang an bekannte soziale Media Portale und ISPs), indem er dasselbe Passwort oder eine Variation dessen verwendet.

Ein geringer Grad an Entropie: Forschungen haben ergeben, das die meisten Menschen der Meinung sind das Sie gut darin sind sich ein starkes und sicheres Passwort auszudenken. Aber wie Rick Redman[2] zeigte, wenden Anwender meist die gleichen Muster bei der Wahl der Passwörter an und schränken damit auch die Passwort-Entropie ein. Die am meisten zu beobachtende Muster waren:

ullllldd (8 Zeichen) ulllllldd (9 Zeichen) ullldddd

Anmerkung:

«u» steht für einen Grossbuchstaben
«l» steht für einen Kleinbuchstaben
«d» steht für eine Ziffer

Wenn ein Sonderzeichen benötigt wurde, hängten Anwender meist nur ein «!» an. Das bedeutet, dass die praktische Reichweite möglicher Passwörter viel niedriger als der theoretische Bereich möglicher Passwörter ist.

[1] http://www.dailymail.co.uk/sciencetech/article-2174274/No-wonder-hackers-easy-Most-26-different-online-accounts--passwords.html
[2] https://www.youtube.com/watch?v=zUM7i8fsf0g

Offen für Wörterbuchangriffe: Ein Angreifer kann die am häufigsten verwendeten Passwörter herunterladen und versuchen, sie gegen die Anwenderbasis des Unternehmens zu verwenden, was zu einer hohen Erfolgsrate führt. Eine Studie der Universität von Cambridge[1] hat ergeben, dass ein Angreifer, der zehn Versuche für das Erraten des Passworts pro Konto hat, etwa 1% der Konten kompromittiert.

MULTI FAKTOR AUTHENTIFIZIERUNG - DIE ANFÄNGE

Die Einschränkungen bei der alleinigen Verwendung eines Passworts sind schon seit langem bekannt und seit über 25 Jahren existieren bereits Multi-Faktor-Authentifizierungen in Form von Hardware-Token (typischerweise ein Hardware-Token mit einer gespeicherten Token-Liste/Algorithmus, um einen Einmal-Code zu erzeugen). Die Authentifizierung erfolgte über einen Token von einem Hardware-Gerät und der Kombination aus Benutzernamen und Passwort aus dem System. Hauptsächlich wurde diese Art der Authentifizierung zumeist nur in den Bereichen Finanzen (Transaktion mit einem hohen Wert), öffentliche Verwaltungen (sensible Daten), im Gesundheitswesen und bei Hochtechnologie- und Regierungsorganisationen eingesetzt. Hardware-Token waren damals und sind heute auch hauptsächlich die Domäne grosser Unternehmen mit grossen Sicherheitsabteilungen, die die Zeit und die Mittel für die Bereitstellung solcher Geräte an ihre oft mobil tätigen Mitarbeiter hatten und haben.

Die Nutzung dieser Systeme wurde dadurch limitiert das der Anwender immer ein zusätzliches Gerät mit sich führen musste. Wurde der Token vergessen oder gar verloren, konnte sich der Anwender nicht mehr in das System einloggen. Auch können diese Token meist nur EIN Authentisierungssystem bedienen und ermöglichen in vielen Fällen keine Skalierung für weitere Systeme.

Wenn Hardware-Token nicht «Event-basiert» sind, kommt es durch ein mehrfaches Drücken des Buttons (dies kann auch unabsichtlich in der Aktentasche geschehen) dazu dass die Token mit dem Server nicht mehr synchron laufen, was zu erheblichen Problemen führen kann. Zeitbasierte Tokensysteme haben das Problem der Synchronisierung.

Kürzlich ist bekannt geworden, dass aber auch Hardware-Token kompromittiert werden können. Eine Sicherheitslücke bei einem grossen und wohlbekannten IT-Security Anbieter deckte ein grundlegendes Sicherheitsproblem bei den von Werk vorprogrammierten Token eines sehr bekannten Token Herstellers auf. Der IT Security Anbieter verlies sich in diesem Fall natürlich auf die Integrität der Produkte des Token Herstellers.

Aber dies bedeutet nicht, dass MFA keine Existenzberechtigung hätten – ganz im Gegenteil sogar. Mehrere Regierungsbehörden unterstützen ihre Verwendung.

Die NIST Sonderveröffentlichung 800-63[2] empfiehlt die Multi-Faktor-Authentifizierung als Remote-Authentifizierung zur Erreichung der Sicherheitsstufen 3 und 4. In den USA ist eine Multi-Faktor-Authentifizierung Pflicht für Regierungsorganisationen und Bundesbehörden gemäss der Homeland-Security-Presidential-Richtlinie-12 (HSPD-12) und dem Office of Management and Budget (OMB) Memorandum M-06-16.

MFA-Verfahren bleiben in der Regel bestehen, sobald sie erst einmal eingeführt wurden. Eine Forschungsstudie von RAND2 stellte fest, dass es «in keinem einzigen Fall dazu kam, dass eine Organisation, die einmal ein MFA-Verfahren implementiert hatte, später wieder zurück fiel auf vorherige Verfahren. Es überwiegt die Verwendung von Token anstatt Biometrie-Faktoren. Im privaten Umfeld sind Token, die Einmalpasswörter generieren bei weitem die wichtigste Zwei-Faktor-Authentifizierungsmethode, welche im Einsatz ist (wenn man PINs/Passwörter als ersten Faktor definiert).»

[1] https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf
[2] https://pages.nist.gov/800-63-3/sp800-63-3.html
[2] http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR937.sum.pdf

MOMENTUM DER MFA DURCH SMARTPHONES

Was hat sich seit den frühen Anfängen der Schlüsselanhänger-/Hardwarebasierten Token getan?
Sowohl die Geschäftswelt als auch die Endverbraucher, die auf etablierte einzige Passwörter angewiesen ist, hat Schwierigkeiten mit den mannigfaltigen Angriffen und der rapiden Technologieentwicklungen. Die Anzahl der Angriffe, die Häufigkeit und die Art der Ausprägung haben sich erhöht. Die Verkettung dieser Umstände führt dazu, dass es Sinn macht, sich noch einmal eindringlicher mit dem Thema der Multi-Faktor-Authentifizierung zu beschäftigen:

- Die weite Verbreitung von Smartphones und darauf installierbarer MFA-Anwendungen macht es überflüssig, ein weiteres Gerät wie einen Hardware-Token mit sich zu führen. Erst die Kombination aus Smartphones und Push-Token Applikation stellt ein überzeugendes Argument dar.

- Ein APP-zentrierten Gesellschaft fordert von Firmen und Organisationen Ihre digitalen Daten mit sicheren Authentifizierungsverfahren zu schützen.

- In ihrem Privatleben sind Anwender bereits daran gewöhnt, sich bei Online-Diensten wie Home-Banking, Social Media und E-Mail-Providern mit einem Authentifizierungsverfahren, basierend auf ihrem mobilen Endgerät, zu legitimieren.

- Apple, Google, Twitter und viele andere führende Techologie-Unternehmen bieten zusätzliche Sicherheit durch den Einsatz eines 2FA-Verfahrens. Dies hat zu einer Steigerung der Akzeptanz bei den Anwendern geführt, was wiederum die mit dem 2FA-Konzept verbundenen Vorteile, durch die hohe Anzahl der Nutzer, in den Vordergrund rückte.

- Cloud-basierte Dienste, die eine sichere Authentifizierung eines Benutzers auch dann gewährleisten müssen, wenn der Benutzer der App (oder dem Betreiber der App) nicht bekannt ist (Federation-Services).

- Biometrie als Authentifizierungsoption (einschliesslich Fingerabdrücke, Retina, Gesichtserkennung und Ähnliches).

- Eine wachsende Zahl von verschiedensten Token-Formaten, wobei sich das «Telefon als Token» trotz einiger Bedenken bezüglich SMS-basierter Anmeldeverfahren zunehmender Beliebtheit erfreut.

- Die Anzahl von Logins und damit auch das die Anzahl der Passwörter (Komplexität und Unterscheidung) nimmt zu.

«Mobiltelefone sind Fluch und Segen zugleich. Ein Segen in der Form, dass das Mobiltelefon dazu eingesetzt werden kann das Haupt-Authentifizierungsgerät zu werden, dass zum einen den Anforderungen der Geschäftswelt und den Bedürfnissen des privaten Lebens gerecht wird. Ein Fluch in der Art und Weise wie diese immer verbundenen und sehr weit verbreiteten mobilen Endgeräte für eine Firma von der zuständigen IT-Sicherheit adäquat zu verwalten sind.

Es ist essentiell, zum einen eine eindeutige Strategie bei dem Umgang mit Sicherheitsrisiken von mobilen Geräten vorzuhalten und zum Anderen es zu ermöglichen, das mobile Endgeräte zur eindeutigen und sicheren Identifizierung und Authentifizierung eingesetzt werden. Dies ist unbedingt erforderlich, damit die Welt mobile Endgeräte als primären Zugangspunkt in die digitale Welt annimmt. Die Frage, wie eine starke Anwenderauthentifizierung auf mobilen Geräten durchzuführen ist, wird somit zwingend notwendig.»

– Alan Goode, Gründer und Geschäftsführer von Goode Intelligence

WICHTIGE ABWÄGUNGSKRITERIEN

Jede Organisation, die eine Einführung der MFA oder eine Migration zu einem neuen MFA-System erwägt, sieht sich einer unüberschaubaren Anzahl von verschiedenen Anbietern und Technologieoptionen entgegen gestellt. Dieses Dokument beschreibt einige der Abwägungskriterien bei der Überprüfung einer potenziellen Authentifizierungslösung. Diese können wie folgt zusammengefasst werden: Sicherheit, Flexibilität, Implementierungsgeschwindigkeit und Einfachheit der Bedienung.

SICHERHEIT

Es gab viele Diskussionen über die Kritikalität von «Hintertüren» (Backdoors) in properitärer Software mancher Hersteller.

«Eine Hintertür ist ein absichtlicher hinterlassener Fehler in einem Verschlüsselungsalgorithmus oder einer Implementierung, der es einem Individuum ermöglicht, die Sicherheitsmechanismen zu umgehen, zu deren Verstärkung das System entwickelt wurde. Eine Hintertür ist eine Möglichkeit für jemanden, Daten aus dem System zu erhalten, wozu er sonst nicht in der Lage gewesen wäre. Wenn die Wand eine Art Sicherheitssystem wäre, dann ist der Tunnel die «Hintertür», die unter der Mauer hindurch führt.»

Wie die NSA eine Hintertür in ein RSA-Kryptosystem implementiert hat (oder implementiert haben könnte):
Eine technische Einführung von Nick Sullivan, 6. Januar 2014

- Für jede Organisation, die sich Sorgen über die Möglichkeit macht, dass eine kryptographische Hintertür in die Authentifizierungslösung, in die sie investiert, eingebaut ist, kann Open-Source-Software (OSS) aus mehreren Gründen als Alternative angesehen werden:

- Während proprietäre Anbieter argumentiert haben, dass ihre Software sicherer weil geheim ist, kann dem mit der Ansicht entgegengetreten werden, dass es bei Closed Source einfach ist, schwache Kryptographie oder ein Backdoor zu implementieren, während dies bei OSS nicht möglich ist.

- Ein Closed-Source-System ist anfälliger dafür, fehlerhaften Code zu enthalten, während OSS ein grösseres Potenzial hat, dass jegliche Risikobereiche von der Open-Source-Community entdeckt werden.

- Im Gegensatz zu der Ansicht, dass die Code-Freigabe den Angreifern Vorteile verschafft, weil sie den OSS-Code sehen können, sind Angreifer durchaus in der Lage, Updates oder Patches binnen kurzer Zeit zu untersuchen und Expolits zu integrieren. Sicherheit durch Verscheleierung («Security by Obscurity») Mehrere wissenschaftliche Arbeiten zeigen, wie einfach es ist, «Closed Source-Code zu untersuchen und mit Schadsoftware zu infizieren.»[1]

- OSS bietet dem IT-Sicherheitsteam die Möglichkeit, den Code zu überprüfen und eine angemessene Sorgfaltspflicht walten zu lassen.

- OSS gibt dem IT-Sicherheitsteam die Möglichkeit, soweit wie möglich den Code sogar an ihre eigenen Bedürfnisse anzupassen. Kunden können sich, aber müssen sich nicht, an der Entwicklung des Codes beteiligen.

[1] https://isc.sans.edu/forums/diary/The+Patch+Window+is+Gone+Automated+PatchBased+Exploit+Generation/4310/

FLEXIBILITÄT

Vorbei sind die Zeiten, in denen eine Fünf-Jahres-IT-Strategie aufgebaut und starr eingehalten werden konnte. Die durchschnittliche Lebensdauer eines Unternehmens aus dem S&P 500 Index der führenden US-Unternehmen ist im letzten Jahrhundert um mehr als 50 Jahre von 67 Jahren, in den 1920er Jahren auf nur 15 Jahre heute zurückgegangen, laut Professor Richard Foster von der Yale University.[1]

Gegen dieses «im Dunkel tappen» benötigen IT-Security Abteilungen Lösungsansätze die Folgendes anbieten:

- Eine Möglichkeit, sich mit der Integration in eine Vielzahl von anderen Tools zu beschäftigen – die Erstellung einer breiten Palette an APIs ist essentiell.
- Eine modulare Architektur, die auch die Verwendung nur der benötigten Teile ermöglicht.
- Ein skalierbares Design, das in Bezug auf die Anwenderbasis vertikal und in Bezug auf Funktionen/Möglichkeiten/zukünftige Standards horizontal skaliert.
- Eine schnelle und einfache Möglichkeit der Bedienung und Instandhaltung.

SCHNELLE IMPLEMENTATION

Time-to-Market ist für alle Unternehmen von entscheidender Bedeutung und angesichts der Geschwindigkeit, mit der sich Unternehmen heute bewegen, sollte eine Investition in eine Sicherheitslösung erste Ergebnisse nach Wochen und nicht erst nach Monaten oder Jahren liefern. Eine Automatisierte Installation und ein modularer Ansatz, der bestehende Authentifizierungsdienste non-invasive integriert, beschleunigt die Implementierungsdauer ihrer MFA-Lösung.

Ebenso wichtig ist es On-Premise Lösungen und/oder cloudbasierte Systeme abzudecken, was dabei hilft den Bedürfnissen der Kunden nach integrem Datenhosting und sicherer Zugangsregulierung nachzukommen. Eine Störung von bereits existierenden Systeme erzeugt meist viel Spannung innerhalb einer Organisation, die bestehende IT-Landschaft sollte, wo immer möglich weiterbestehen und nicht deinstalliert werden.

EINFACHE BEDIENUNG

Einer der wichtigste Punkt bei grossen 2FA-Implementierungen, ist die Akzeptanz der Anwendung durch die End-Anwender. Der MFA Prozess muss für den Endverbraucher so einfach und leicht wie nur möglich sein. Die einfache Bedienung benötigt gemäss den Risikoniveaus, das durch die Anwendung der 2FA-Authentifizierung abgedeckt ist, einekonstante Balance in Verbindung mit dem erforderlichen Schutz.

Diese Überlegungen beginnen mit dem Rollout der Token und befassen sich damit, wie man das Handling für die Organisation so einfach und reibungslos wie nur möglich gestaltet. Sie erstrecken sich später auf viele verschiedene Aspekte, wie zum Beispiel dazu in der Lage zu sein, eine Vielzahl von verschiedenen Typen von Token für unterschiedliche Anwendungsfälle zu unterstützen oder die Integration zu optimieren, um die negativen Auswirkungen auf die Arbeitsabläufe der Anwender zu minimieren.

Neue aktuelle und zukünftige Typen von Token und Methoden werden eine höhere Anwenderakzeptanz ermöglichen, während sie die Sicherheitsstufen erhalten, die für eine konforme und vertrauenswürdige Identitätsauthentifizierung erforderlich sind.

[1] http://www.bbc.com/news/business-16611040

WAS KOMMT ALS NÄCHSTES?

Für IT-Sicherheitsexperten sind dies anspruchsvolle, aber aufregende Zeiten. Mitarbeiter und Kunden suchen gleichermassen die Gewissheit, dass das Unternehmen oder die Organisation alles Erdenkliche tut, um die Risiken für eine Datenschutzverletzung und die rechtlichen, persönlichen und finanziellen Folgen davon zu reduzieren. Die Balance zwischen Benutzerfreundlichkeit und Sicherheit auf Grundlage des Unternehmensrisikos muss definiert und umgesetzt werden.

Eine starke, modulare Authentifizierungslösung sollte ein wesentlicher Bestandteil der Sicherheitsinfrastruktur eines jeden Unternehmens sein. Der weitverbreitete Ansatz der einfachen Kombination aus Benutzername und Passwort ist heutzutage nicht mehr ausreichend. Das Nichtergreifen von Massnahmen, setzt Ihre Organisation, Ihre Mitarbeiter, Ihre Kunden und die Daten all Derer einem unnötigen Risiko aus.

Glücklicherweisse gibt es eine Reihe von Authentifizierungsoptionen und Ebenen, die der jeweiligen Risikostufe zugeordnet werden können – von einer Banktransaktion (ob gross oder klein) oder Gesundheitsaktendatenbank bis hin zu einer Online-Gaming-Community-Seite. Jeder dieser Anwendungsfälle kann verschiedene Ebenen der Authentifizierung, Token und so weiter benötigen.

HÜTEN SIE SICH VOR DEN KOSTEN DER UNTÄTIGKEIT!

«... unsere globale Studie befasst sich mit der Wahrscheinlichkeit einer oder mehrerer Datenschutzverletzungen eines Unternehmens in den nächsten 24 Monaten. Wir schätzen eine 26-prozentige Wahrscheinlichkeit.[1]»

Wir danken KeyIdentity für die Unterstützung.

CLUE

Clue ist für jedes Unternehmen mit IT-Sicherheits Bedürfnissen der flexibelste Managed Service Provider mit einem garantiert tiefen TCO, weil wir Enterprise fähige Security Lösungen erschwinglich machen, unsere Services genau auf Ihre Bedürfnisse zuschneiden und Sie nicht durch fixe Servicepläne binden.

KEYIDENTITY

Mit Hauptsitz in Deutschland ist KeyIdentity ein globaler Anbieter von skalierbaren, schnell betriebsbereiten Multi-Faktor-Authentifizierungslösungen (MFA) der Enterprise-Klasse. Im Kern steckt bewährte Open-Source-Technologie. Die LinOTP-Suite bietet unternehmensweite Funktionen durch SVA, LAP und andere Produkte.

[1] http://www.paymentscardsandmobile.com/cost-data-breach-study-global-analysis/