2FA einführen – aber wie?

2FA einführen – aber wie?

Es ist nicht die Technik, die bei einer 2FA-Einführung zur Herausforderung wird. Es sind die Forderungen verschiedener Stakeholder und die Auswirkungen an vielen Stellen der Unternehmens-IT.

Von Christian Zander

-tract

- Technisch sind Unternehmensanwendungen meist schnell für den zweiten Faktor fit gemacht, die Hürden lauern in der Projektumsetzung.
- Stakeholder wie CISOs, Auditoren oder der Helpdesk haben ganz unterschiedliche Anforderungen; für Nutzer soll es vor allem einfach sein.
- Adaptive Authentication, Self-Service-Portale und umfangreiche Systemintegration erhöhen die Akzeptanz und sind schon bei der Anforderungsanalyse zu beachten.
- Ein schrittweises Rollout, begleitet von Feedbackschleifen und Monitoring, erlaubt das Gegensteuern bei Bedarf und führt am ehesten zum Erfolg.

Richtig implementiert, hat Zwei-Faktor-Authentifizierung für Unternehmensanwendungen nur Vorteile. 2FA erhöht die Sicherheit im Unternehmen, verbessert langfristig aber auch die User Experience: Auch für User ist es vorteilhaft, wenn nicht mehr alles an der Qualität der Benutzerpasswörter und der „Passworthygiene“ des Einzelnen hängt.

Selbst wenn ein zweiter Faktor Fehler und Nachlässigkeiten nicht ausschließt, nehmen durch ihn doch die Auswirkungen

erfolgreicher Passwortangriffe ab. Der jüngste DBIR-Bericht von Verizon (siehe ix.de/z7p8) aus dem Jahr 2022 zeigt, dass Credentials mit circa 50 Prozent und Phishingangriffe allgemein zu etwa 20 Prozent immer noch die wichtigsten Einfallstore für Angriffe sind.

Ein weiterer Vorteil von 2FA ist, dass es den Unternehmen hilft, Complianceregelungen umzusetzen. Hier helfen die Features der Zwei-Faktor-Authentifizierungswerkzeuge wie Policies, Adaptive Authentication und Reportings, die rechtlichen Risiken für Führungskräfte, Vorstandsmitglieder und die Unternehmen zu reduzieren.

Technisch ist die Einführung der Zwei-Faktor-Authentifizierung keine Zauberei mehr. Wenn Applikationen gut vorbereitet sind, kann eine neue Anwendung innerhalb von 30 Minuten mit 2FA und SSO (Single Sign-on) an Bord genommen werden. Entscheidend ist aber, dass die Umsetzung den Erwartungen aller Beteiligten entspricht, denn am Ende wollen alle nur, dass es funktioniert.

Die Auditoren wollen alle relevanten Informationen sehen und nachvollziehen können. Die User wollen eine einfache Handhabung, die nicht (zu sehr) nervt, wie erwartet funktioniert und sich schnell anpassen lässt, wenn es später doch mal hakt. Der Helpdesk und die IT-Leitung erwarten wenig Aufwand bei Betrieb und Updates, zudem Reports, die beim Debugging alle notwendigen Informationen liefern. Zu guter Letzt wollen CISOs, CEOs und Betriebsräte, dass alles ohne Sicherheits- oder Complianceverletzungen abläuft. Das alles muss jedem, der ein solches Projekt startet, von Anfang an klar und während des Verlaufs immer präsent sein: von der Planung, der Anforderungsanalyse, der Auswahl des Systems bis zur Umsetzung.

Vorab sind vor allem folgende Fragen zu klären: Müssen Zugriffe auf User-Level und global eingestellt werden können? Wird Application-Level-Authentifizierung benötigt oder soll es

sogar bis auf Session-Level gehen? Finden verschiedene Faktoren Berücksichtigung? Sind die (Geo-)Location, Gruppendefinitionen oder Authentifizierungstypen relevant? Soll ein gutes Dashboard das Mittel der Wahl sein, um das System zu konfigurieren, oder soll eine API die Regeln einspielen?

Wissen, haben, sein

Der Prozess der Authentifizierung besteht im Überprüfen mehrerer Parameter. Sie beruhen auf Wissen, Besitz und Präsenz. Wissen bezieht sich auf Credentials wie Passwörter oder PINs, die ausschließlich der autorisierte User kennt. Das ist die First Level Authentication. Besitz bezieht sich auf etwas, das der Anwender bei sich trägt. Dies kann ein Mobiltelefon, ein Hardwaretoken, eine Smartcard oder ein USB-Key sein. Präsenz bezieht sich auf biometrische Faktoren, die dazu verwendet werden, den Nutzer zu identifizieren: der Fingerabdruck, die Iris oder das Gesicht.

Genau genommen kann man schon bei einer Authentifizierungs-App von MFA sprechen, denn sie verwendet mehr als zwei Faktoren. User melden sich mit ihren Credentials an (Wissen), erhalten ein Authentifizierungsanfrage auf ihr Mobiltelefon (Besitz) und müssen es und die App entsperren (Präsenz) und die Authentifizierung bestätigen.

Neben diesen drei Standardparametern können weitere Parameter mit ins Rennen gehen, um die Sicherheit zu erhöhen. Einer davon wäre der Zeitpunkt, zu dem ein User etwas tut. Log-ins könnten etwa nur von 9 bis 17 Uhr möglich sein, für hochkritische Bereiche wie Tresore oder KRITIS-relevante Zugänge könnten festgelegte Öffnungszeiten existieren. Der Ort wäre ein weiteres Beispiel. Ist es erlaubt, von Amerika aus auf geschützte Daten zuzugreifen, oder nur wenn die Kollegen in Deutschland oder sogar im Firmengebäude sind? Dafür wird die IP-Adresse verwendet und falls möglich die Geo-Location. Beim mobilen Arbeiten sind allzu strenge standortbasierte

Policies aber hinderlich. Wenn Mitarbeiter plötzlich nicht mehr auf Applikationen zugreifen können, nur weil sie geraden in Schottland sind, ist das schwierig.

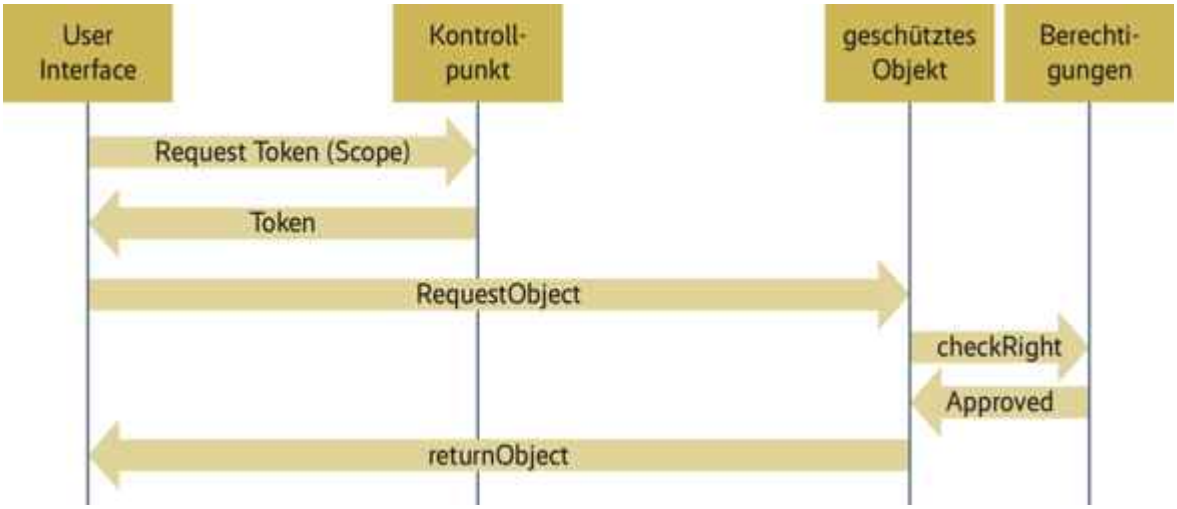
Gute Lösungen bringen weitere smarte Authentication-Parameter ins Spiel, die unplausibles Verhalten erkennen. Wenn ein Benutzer gerade in Peru war und sich 15 Minuten später in Rom befindet, ist das unlogisch und sollte zu einem Request Denied führen. Mit einer Prise KI oder maschinellem Lernen lassen sich auch das typische Verhalten, Fehlerraten, Anzahl von Zugriffsversuchen, Geschwindigkeit der Zugriffsversuche und ungewöhnliche Orte und Zeiten als Zugangsparameter verwalten. Damit lässt sich der Zugang bei untypischem Verhalten des Users und hohem Risiko-Score (vorübergehend) verwehren.

Ein weiterer Punkt ist die Flexibilität: Es sollte möglich sein, unkritische Bereiche mit nur einem Faktor erreichbar zu machen und erst beim Zugriff auf sensible Informationen mehrere abzufragen. Der erste Faktor könnte auch genügen, wenn etwa ein Request erstens aus einem gesicherten Netzwerk, zweitens von einem bekannten und gesunden Gerät und dazu drittens zu einer gewöhnlichen Zeit kommt.

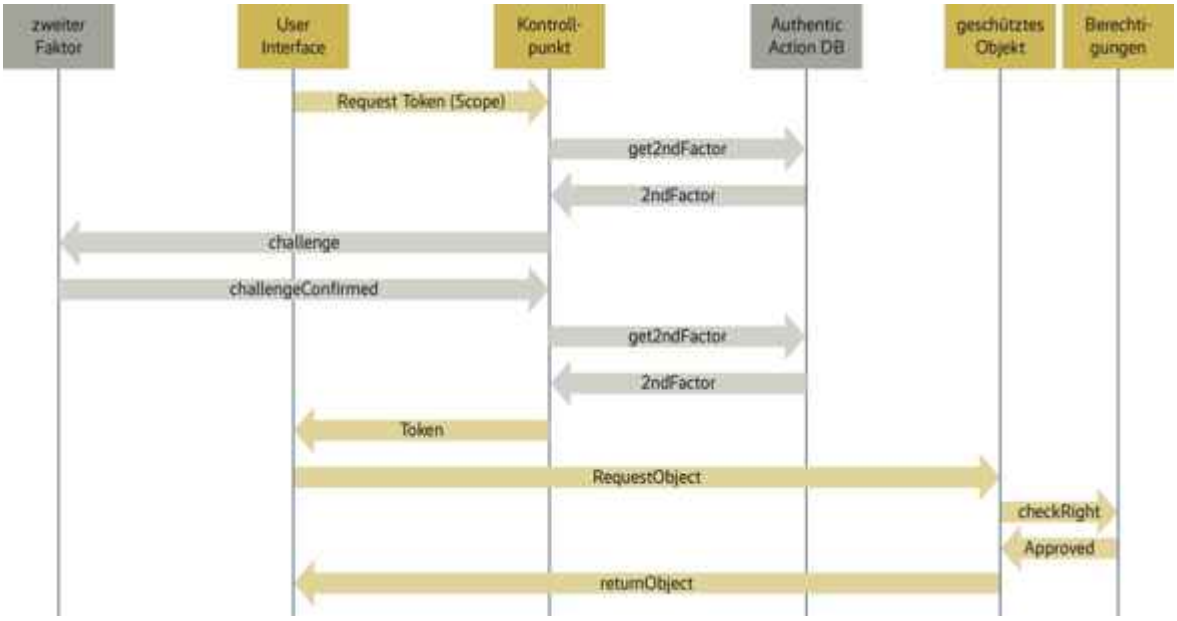
Erweiterter Anmeldeprozess

Der Anmeldeprozess verändert sich durch die Einführung eines zweiten Faktors nicht, er wird nur erweitert. Leicht vereinfacht zeigt Abbildung 1 die Anmeldung ohne 2FA. Es gibt ein User Interface, an dem sich die Benutzer anmelden. Sie holen sich ein Token ab und benutzen es künftig dafür, auf Datenobjekte zuzugreifen. Genügt das Token nicht den Anforderungen, die das geschützte Objekt stellt, bekommt das User Interface ein Access Denied zurück und ist dafür verantwortlich, sinnvoll damit umzugehen. Bei 2FA läuft es nicht viel anders ab (siehe Abbildung 2). Noch während das Token angefragt wird, stellt die Software fest, dass Zwei-Faktor-Authentifizierung gefragt ist. Nun holt man sich den zweiten Faktor aus einer Authentication-Datenbank und startet

die Challenge beim Anwender. Er muss die Challenge annehmen und beantworten, dann prüft die Applikation die Antwort und gibt das Token frei. Der Rest erfolgt dann wie vorher.



Bei der einfachen tokenbasierten Authentifizierung fragt das User Interface ein Token bei einem Kontrollpunkt an (Abb. 1).



Kommt ein zweiter Faktor ins Spiel, wird das Authentifizierungsverfahren erweitert. Aber auch hier wird ein Token überreicht. Der prinzipielle Ablauf bleibt gleich (Abb. 2).

Self-Service kommt gut an

Sicherheit darf nicht nerven, sonst finden Mitarbeiter einen Weg darum herum. Optimalerweise macht sie sogar Spaß. Wichtig ist es, den Usern die Wahl zu lassen und ihnen etwas Hilfe zur Selbsthilfe anzubieten – die zusätzlich den Aufwand im

Helpdesk reduziert. Ein Self-Service kann es Nutzern erlauben, ihre Authentifizierungswerkzeuge auszuwählen, zu aktualisieren oder bei Verlust oder beim Austausch eines Gerätes zu sperren.

Wird ein Token gesperrt, ist es sinnvoll, alle aktiven Sessions zu sperren, alle dem Device zugeordneten Services zu unterbinden und ihm seine Zugriffsrechte zu entziehen. Wenn möglich, ist ein automatisches Remote Wipe eine gute Option.

Mit Self-Service Registration (SSR) können sich Nutzer selbst registrieren. Sollte ein Self-Service zum Passwort-Reset noch nicht verfügbar sein, bietet es sich an, auch diesen mit im Projekt einzuführen und bei der Auswahl der Tools zu berücksichtigen.

Ein Aktivitätenplan sollte das Problem verlorener oder vergessener Authentifizierungstoken adressieren und potenzielle Sicherheitsprobleme thematisieren. Zum Beispiel sollte man niemals denselben Kanal für die Recovery verwenden, über den eine Anfrage zu einem vergessenen Passwort eingeht. Dieser muss immer als kompromittiert gelten. SMS als Recovery-Kanal wird zunehmend unsicher, denn Hacker finden auf Social Media möglicherweise genügend Informationen, um beim Mobilfunkanbieter eine Kopie der SIM und damit auch alle Mobile-Authentifizierungstoken zu erhalten.

Third-Party-Integration – mehr ist mehr

Als ich kürzlich bei einem großen deutschen Anbieter Ersatzteile bestellte, wurde ich gefragt, ob ich mich auch registrieren wolle. Na klar – dann muss ich nicht immer alle meine Daten eingeben und kann gegebenenfalls später schneller Ersatzteile bestellen. Gesagt, getan. Der Registrierungsprozess ging voran: E-Mail-Adresse und ein sicheres Passwort, klar. Zwei-Faktor-Authentifizierung? Aber gern. Und dann kam es: Das ginge nur mit „ihrem“ Zwei-Faktor-Authentifizierungstool. Schade. Ich habe es erst gar nicht in Erwägung gezogen. Dass Banken ihre eigenen Tools verwenden,

ist lästig, aber noch verständlich, doch für das Bestellen von Ersatzteilen gilt das mit Sicherheit nicht.

Mitarbeiter von Unternehmen greifen schon lange nicht mehr nur auf die interne Office- und Betriebssystemwelt zu, sondern nutzen viele Dienste und Anwendungen von Drittanbietern oder aus der Cloud. Auch diese sollen den Policies entsprechen und so sicher wie möglich sein. Privat verwenden Benutzer ebenfalls etliche Applikationen. Die Akzeptanz wird erhöht, wenn das Zwei-Faktor-Authentifizierungswerkzeug in der Lage ist, sich auch mit diesen zu verbinden. Die Administration wird damit einfacher. Es gibt weniger Stellen zur Verwaltung von Sicherheitsaspekten und idealerweise lässt sich das Ganze in ein vorhandenes Enterprise Service Management integrieren.

Im Zusammenspiel mit Single-Sign-on (SSO) gibt es allerdings einige Fallstricke, die zu beachten sind. Das Alignment der Gruppen, die beispielsweise im Active Directory (AD) zu finden sind, mit den Berechtigungen in den Produkten sollte man gründlich testen. Effekte wie „und plötzlich hatte ich auf alles Zugriff“ können sehr unerfreulich sein. Bei Applikationen, die sensible oder kritische Daten beherbergen, sollte bereits beim Testen immer jemand dabei sein und diesen Vorgang überwachen, um unerwünschten Datenabfluss oder bloß den Verdacht, dass dies geschehen könnte, zu vermeiden.

Wer schreibt, der bleibt: Logs, Reports und Dashboards

Insbesondere für das Einhalten von Complianceanforderungen und Richtlinien sind Dashboards, Reports und Logs wie Business- und Policy-Impact-Übersichten maßgeblich. Schon bei der Toolauswahl sollte klar sein, welche Informationen benötigt werden, um diesen Anforderungen gerecht zu werden.

Bei den Features des Dashboards sind zwei Fragen relevant: Erstens, welche Probleme können entstehen, wie sind sie erkennbar und wie relevant sind sie für das Business? Und

zweitens, welche Informationen sind nötig, um für die Probleme Handlungsfelder zu erkennen, Auswirkungen zu ermessen und Risiken im Falle eines Problemeintritts abzuwägen? Nötig ist einerseits ein Helikopter-Überblick über den Zustand des Systems, andererseits aber auch die Möglichkeit, sich schnell und effektiv in die Details hineinzubohren.

Problembehebung bei Zwei-Faktor-Authentifizierung kann kompliziert werden. Policies, die sich gegenseitig ausschließen oder überlagern, dynamische Regeln und adaptive Authentifizierung müssen einfach sichtbar gemacht und schnell erkannt werden können. Risiko-Scores sollten ebenfalls deutlich gemacht und gegebenenfalls direkt administriert werden. Systemadministratoren brauchen Dashboards, die das massenhafte Konfigurieren und Ausrollen von Regeln ermöglichen und Probleme aufzeigen. Bestenfalls kann man die zugehörigen Helpdesk-Tickets, weitere Telemetriedaten und Statistiken anzeigen. Für das Ausrollen ist es sinnvoll, den Deployment-Fortschritt übersichtlich dargestellt zu bekommen.

Um die Akzeptanz zu messen, ist es wichtig, den tatsächlichen MFA-Einsatz im Blick zu behalten und zu verfolgen, wie häufig Nutzer die Authentifizierungsfaktoren verwenden und ob sie bestimmte Software möglicherweise nicht mehr so häufig wie vorher einsetzen. Das könnte ein Hinweis für Akzeptanzprobleme sein.

Schütze, was wichtig ist

Bei der Zwei-Faktor-Authentifizierung ist es ähnlich wie beim Identity and Access Management (IAM). Was soll geschützt werden? Alle Orte, an denen kritische und sensible Daten und Rechte liegen. Pragmatisch und leicht verständlich heißt das: Kritische Daten sind Daten, die, wenn sie verloren gehen oder in die falschen Hände geraten, unmittelbare und schwerwiegende Schäden für das Unternehmen nach sich ziehen könnten, während sensible Daten solche sind, deren Abhandenkommen mittelfristig Schäden verursachen könnte. Der Rest an Daten ist in dieser

Hinsicht mehr oder weniger egal.

Die Einführung von 2FA betrifft das ganze Unternehmen: Das Sicherheitsteam, die IT-Abteilung, die Benutzer, die Personalabteilung und der Betriebs- oder Personalrat und nicht zuletzt die Unternehmensführung müssen dahinterstehen, damit das Projekt eine gute Chance auf Umsetzung hat.

Mitnehmen und überzeugen

Alle Nutzer müssen verstehen, dass die Zwei-Faktor-Authentifizierung dazu da ist, sie zu unterstützen. Mitarbeiter fürchten oft Veränderungen, neue Behinderungen und noch mehr Überwachung. Präsentationen, kurze Erklärvideos und Schulungen verringern die Vorbehalte. Auch Einladungen, an der Pilotgruppe teilzunehmen, und Mitarbeiter, die als Multiplikatoren und Botschafter der Sache fungieren, fördern die Akzeptanz.

Die Umstellung sollte mit den Adminkonten starten, das schlägt zwei Fliegen mit einer Klappe: Man schützt kritische Rechte zuerst und erbringt einen Konzeptnachweis. Von hier aus kann das Ausrollen beginnen, wobei es auch hier wichtig ist, das IAM im Auge zu behalten. Dabei fällt möglicherweise auf, wie viele Konten es gibt und dass sie zu mehr berechtigt sind, als sie sein müssten.

Als Nächstes ist die Pilotgruppe an der Reihe. Admins verstehen in der Regel die technischen Gegebenheiten und Notwendigkeiten schnell. Bei der Pilotgruppe, die Mitarbeiter aus allen Sicherheitsstufen und Unternehmensbereichen umfassen sollte, ist das anders. Wenn Zwei-Faktor-Authentifizierung nicht nur intern, sondern auch bei Geschäftspartnern und Auftragnehmern zum Einsatz kommen soll, ist auch hier eine Pilotgruppe sinnvoll.

Langsam und stetig voran

Bei der schrittweisen Umstellung – eine Applikation nach der anderen, ein Bereich nach dem anderen – sollte man jede Anwendung testen, auch wenn anscheinend keine Probleme zu erwarten sind. Der Teufel steckt im Detail und Details machen alles kaputt. Es tauchen auch möglicherweise Applikationen auf, die keine Zwei-Faktor-Authentifizierung beherrschen. Solche älteren internen Programme oder Clients können eventuell nachgerüstet werden. Falls das nicht möglich ist, ist es Zeit, einen Change Request für diese Anwendungen zu stellen, um das Projekt dadurch nicht zu blockieren. Neue Mitarbeiter sollten ab diesem Zeitpunkt immer mit Zwei-Faktor-Authentifizierung ausgestattet sein.

Nicht überall hat man Netz, wer viel Bahn fährt, weiß das. In solchen Fällen ist es gut, alternative Authentifizierungsmethoden anzubieten, wie automatische Sprachanrufe oder die Aufforderung, eine Taste auf dem Telefon zu drücken. Wenn der Benutzer seine präferierte Methode im Self-Service-Portal auswählen kann, führt das zu mehr Akzeptanz. Die Wahl zu haben ist immer besser als der „Friss oder stirb“-Ansatz. Auch etwas Augenmaß beim Zwang zur Autorisierung schätzen die Nutzer. Zugriff auf kritische Daten sollte also öfter autorisiert werden als der auf den Speiseplan der Kantine.

Wenn die mobilen Geräte, die den zweiten Faktor bereitstellen, noch nicht verwaltet werden, ist jetzt ein guter Zeitpunkt, ein Mobile Device Management einzuführen. Das stellt sicher, dass die mobilen Geräte ohne Jailbreak bleiben und regelmäßig auf Malware untersucht werden.

Support braucht Kapazität

Fehlgeschlagene Anmeldungen, verzweifelte Benutzer und gesperrte Konten sind gerade zu Beginn der Einführung von Zwei-Faktor-Authentifizierung normal. Der Helpdesk muss

genügend Zeit dafür haben, um den Benutzern in Ruhe und freundlich zu helfen. Es muss schnell gehen, denn wenn Benutzer nicht arbeiten können, sind sie in dieser Zeit nicht in der Lage, etwas zum Unternehmenserfolg beizutragen. Genervte Supportmitarbeiter, die unter Zeitdruck arbeiten und schlecht kommunizieren, werden dafür sorgen, dass die Akzeptanz von Zwei-Faktor-Authentifizierung sinkt, anstatt zu steigen.

Verlorene Hardware und Schlüssel sind Missgeschicke, für die es ein einfaches und von Vorwürfen freies Meldeverfahren braucht. Denn es ist wichtig, dass die Benutzer sofort Meldung erstatten, um die Geräte zu sperren und das Verhalten des Kontos auf verdächtige Aktivitäten zu überprüfen. Damit die Benutzer im Verlustfall trotzdem weiterarbeiten können, bis Ersatz zur Verfügung steht, ist es hilfreich, mehrere Anmeldemöglichkeiten bereitzustellen.

Begleiten, messen und monitoren

Während der Einführung sollte man permanent im Auge behalten, ob und wie sich die Zwei-Faktor-Authentifizierung auf die Produktivität und Sicherheit auswirkt. Dazu kann es notwendig sein, Richtlinien mehrfach anzupassen und den Einfluss dieser Veränderungen zu verfolgen.

Mitarbeiterbefragungen und Feedbackmeetings sind nützlich, um Erfahrungen zu sammeln und Verbesserungsvorschläge abzuleiten. Auch sie sollten mit der Pilotgruppe starten und so lange stattfinden, bis alles reibungslos läuft. Häufen sich in den Helpdesk-Tickets bestimmte Probleme, könnten diese mit Zwei-Faktor-Authentifizierung in Verbindung stehen, auch wenn es auf den ersten Blick nicht offensichtlich ist. Außerdem lässt sich erst nach einer ersten Implementierung wirklich kontrollieren, ob die Reports und Auditoranalysen den Anforderungen genügen. Software wird regelmäßig aktualisiert. Die Ansprüche an die Zwei-Faktor-Authentifizierung müssen in den Updateprozess einbezogen und getestet werden.

Alles ist auch Projektmarketing

Nicht erzählt ist wie nicht gemacht. Wenn sie nicht wissen, was passiert und was bereits getan ist, werden die Projektstakeholder unruhig und die User haben bereits wieder vergessen, dass da noch was auf sie zukommt. Berichte über Erfolge, aber auch über Dinge, die nicht funktioniert haben, erhöhen die Akzeptanz. Denn das, was nicht geklappt hat, hat meist ohnehin schon die Runde gemacht. Die Anwender sollten auch wissen, welche Applikationen womöglich ersetzt werden müssen, damit sie sich schon im Vorfeld damit anfreunden können. Auch nach dem Projekt ist Kommunikation wichtig, denn wer sich zu sicher fühlt, wird nachlässig. Regelmäßige Phishingübungen mit anschließenden Schulungen stärken das Security-Immunsystem des Unternehmens.

Security ist ein dauerhafter Prozess, das Sicherheitsbewusstsein der Mitarbeiterinnen und Mitarbeiter zu sensibilisieren und sie in das Wachstum der Firma miteinzubeziehen. Richtig eingesetzt, trägt auch das Projektmarketing ganz wesentlich dazu bei, das Unternehmen sicherer zu machen. (ulw@ix.de)

1. Quellen
2. Link zur erwähnten Securitystudie: ix.de/z7p8