Einfache Zwei-Faktor-Authentisierung

Bürger- bzw. Kundennähe, Offenheit und Transparenz sind häufig kommunizierte Ziele der aktuellen Welle an Digitalisierung: Der Kundenkontakt der öffentlichen Verwaltung findet nicht mehr hinter verglasten Schaltern oder geschlossenen Türen statt, sondern in hellen und freundlichen Empfangsbereichen. Oder die Filiale einer Firma oder Verwaltungsstelle im Quartier oder ländlichen Raum wird nicht vollständig geschlossen, sondern als kleine Agentur in der Ecke eines lokalen Geschäfts weiterbetrieben.

So lobenswert diese Ziele auch sind, im Rahmen von Datenschutz und Datensicherheit bereitet ihre Umsetzung grosses Kopfzerbrechen. Das Vertrauen in die neuen Mitarbeiter ist dabei häufig das kleinste Problem. Erstens werden dabei bestehende IT-Arbeitsplätze ohne besonderes Schutzpotenzial neu um zusätzliche, teilweise privilegierte Funktionen erweitert. Zweitens entstehen neue IT-Arbeitsplätze mit privilegierten Funktionen in Räumlichkeiten ohne dauernde Überwachung. Letzteres trifft nicht nur auf Läden und Kleinfirmen mit neuen Agenturfunktionen zu, auch in Informationszentren von Hochschulen oder den Behandlungszimmern von Arztpraxen finden sich ähnliche Konstellationen.

Der korrekte Ansatz wäre, bei solchen Änderungen in Arbeitsablauf und -umgebung Schutzbedarf und Sicherheitsrisiken neu zu erfassen, zu bewerten und gezielte Massnahmen umzusetzen. Leider ist die Umsetzung vor allem in heterogenen Systemumgebungen beinahe unmöglich. Insbesondere bei älteren oder eingekauften Anwendungen fehlt Zugang zum Quellcode oder geeignetem Know-How, um die Anpassungen vornehmen zu können.

Ein typisches zusätzliches Sicherheitselement für diesen Fall ist die Einführung eines zweiten Authentisierungsfaktors neben Benutzername und Passwort. Damit kann in vielen Fällen die zusätzliche Gefährdung durch das ungesicherte Endgerät kompensiert werden.

Das Passwort-Dilemma

Die häufigste Art der digitalen Authentifizierung ist immer noch die Kombination von Benutzername und Passwort. Errät oder stiehlt ein Angreifer das Passwort eines Benutzers, erlangt er damit effektiv dessen digitale Identität und kann auf persönliche Informationen des Benutzers zugreifen sowie Aktionen in dessen Namen ausführen. Das Passwort ist daher ein sehr beliebtes Angriffsziel und leider oft das schwächste Glied der Sicherheitskette.

Organisatorische und technische Defizite kombiniert mit dem technischen Fortschritt führen zur kontinuierlichen Schwächung von Passwörtern:

- Passwörter werden wiederverwendet oder geteilt;
- sie sind Ziel von Angriffen auf Nutzer und Dienste;
- Maschinen werden immer besser darin Passwörter zu erraten.

Nutzer stehen daher vor einem für sie unlösbaren Dilemma: Zum einen soll das Passwort möglichst einfach zu merken und einzugeben sein, zum anderen muss es für Maschinen sehr schwer zu erraten sein.

Als Folge können Passwörter heute allgemein nicht mehr als sicher betrachtet werden. Für viele Anwendungen und Benutzergruppen mag das verbleibende Sicherheitsniveau ausreichen, jedoch erfordern sensible Informationen (wie Speicherung und Verarbeitung personenbezogener Daten) oder

kritische Aktionen (bspw. Finanztransaktionen) zusätzliche Sicherheitsmassnahmen. Entsprechend ermöglichen oder verlangen viele Dienstleister wie Banken die Nutzung von zusätzlichen Sicherheitsfunktionen.

Multi-Faktor-Authentisierung

Die Multi-Faktor-Authentisierung (MFA) verlangt nicht nur das eine Merkmal Passwort für den Nachweis der Identität, sondern besteht auf der Vorlage mehrerer, voneinander unabhängiger Faktoren. Diese Faktoren können sein:

- etwas, was man weiss (Kenntnis eines Geheimnisses wie ein Passwort oder ein PIN),
- etwas, was man hat (Besitz eines Identifizierungsobjekt wie eID, Smartcard, oder Telefonnummer)
- etwas, was man ist (biometrische Merkmale wie Fingerabdruck oder Retina).

Diese zusätzliche Anforderung erhöht die Komplexität des Authentifizierungssystems und kann erheblichen finanziellen Aufwand zur Folge haben. Zudem erfordern Umsetzung und Betrieb Expertenwissen.

Ungenügende Kenntnis oder schlechte Designentscheidungen können tatsächlich zu einer Verringerung des Sicherheitsniveaus führen. Häufige Fehler sind u.a.:

- dasselbe Gerät wird sowohl für die Transaktion als auch zur Verifikation verwendet,
- Faktoren werden auf einem Gerät unter Kontrolle des zu authentifizierenden Nutzers (Client) statt beim Authentifizierungssystem (Server) geprüft (bspw. lokale Passwortüberprüfung bei Zertifikaten oder Schlüsseln; lokale Biometrieüberprüfung)
- es wird nicht überprüft, ob alle Faktoren zu demselben Nutzer gehören.

Die erhöhte Komplexität wirkt sich oft auch direkt auf das Nutzererlebnis aus. Benutzer müssen sich jetzt nicht nur das Passwort merken, sondern evtl. noch zusätzlich Authentifizerungstoken verwalten.

Um die Nutzerakzeptanz zu erhöhen und den Aufwand für Dienstleister zu reduzieren, haben sich einige bekannte Verfahren zur MFA etabliert.

Am bekanntesten ist wohl die *TransAktionsNummer (TAN)*, die prominent im Finanzsektor Verwendung findet. Hierbei wird die Vorlage einer einmal gültigen Nummer zur Authorisierung einer privilegierten Transaktion verlangt. Früher wurden TANs in Listen ausgegeben, heutzutage findet das SMS-TAN-Verfahren immer grössere Verbreitung.

Eine verwandte Methode ist das sog. *Einmalpasswort (One-Time Password, OTP)*. Dies ist ein Passwort, das nur einmal verwendet werden kann. Es unterscheidet sich von TANs in der Art wie es generiert wird. Während die TAN dem Nutzer vom Dienstanbieter über einen dedizierten Kanal mitgeteilt wird, werden OTPs sowohl vom Nutzer als auch vom Dienstanbieter unabhängig voneinander erstellt und dann verglichen. Dazu müssen die Parteien bzw. deren Geräte ein gemeinsames Geheimnis kennen, aus dem die OTPs abgeleitet werden können. Attraktiv sind OTPs aufgrund der relativ einfachen Handhabung. Nutzerseitig reicht ein Smartphone mit passender App.

Ein Neuling unter den Authentifizerungsmethoden ist der *Universelle 2. Faktor (U2F)*. Er basiert ähnlich wie Web- oder E-Mail-Verschlüsselung auf *asymmetrischer Kryptographie*. Der private Schlüssel wird auf einem sicheren Hardware-Token verwahrt. Der öffentliche Schlüssel wird dem Dienstanbieter mitgeteilt; dieser kann damit prüfen, ob der Nutzer tatsächlich im Besitz des passenden privaten Schlüssels ist. U2F ist ein Authentifizierungsstandard der FIDO Alliance , der vor allem die Handhabung für Nutzer erleichtern soll. Nutzer können auf dem Token ihre eigenen Schlüssel generieren und benötigen zusätzlich lediglich einen kompatiblen Browser, der die Schnittstelle zwischen Webservice und Hardwaretoken bereitstellt.

X.509-Nutzerzertifikate (bekannt aus der E-Mail-Verschlüsselung als S/MIME) sind für die Nutzerauthentifizierung noch nicht weit verbreitet. Man findet sie meist in Bereichen mit eingeschränktem Zugang, oft in Form von Smartcards. In der Regel handelt es sich hierbei allerdings nicht um MFA, der Nutzer muss meist lediglich den Besitz der Karte nachweisen, um Zugang zu erhalten.

Obwohl es eine Vielzahl von verfügbaren Methoden und Produkten für MFA zur

Auswahl gibt, hat sich gezeigt, dass die meisten sich nicht für einen breiten Einsatz eignen. Besonders problematisch sind heterogene Strukturen, wie man sie in Bildungs- und Forschungseinrichtungen findet. Entweder werden die Produkte nicht von allen Plattformen unterstützt, oder sie haben sehr hohe Anforderungen an Betrieb und Pflege. Auch führen manche Verfahren zusätzliche Abhängigkeiten zu neuen, evt. externen Diensten ein.

Trotzdem muss gute Multi-Faktor-Authentisierung nicht teuer oder komplex sein. Wir stellen eine Methode vor, die gewöhnliche X.509-Nutzerzertifikate als Beweis für die Identität des Benutzers und damit als ersten Faktor für die Authentifizierung verwendet. Erst nach Vorlage des Zertifikats wird der Nutzer nach seinem Passwort gefragt. Dieses Schema entspricht etwa dem Vorgang beim Geldabheben an einem Bankautomaten. Auch hier muss man erst seine Identität durch Vorlage der Bankkarte nachweisen und wird dann nach seinem Geheimnis (der PIN) gefragt. Es ist daher sehr benutzerfreundlich, kann leicht implementiert werden und ist zudem flexibel mit unterschiedlichen Hard- und Softwarelösungen kombinierbar.

MFA mit X.509-Nutzerzertifikaten

Damit sich MFA auch in der Breite durchsetzen kann, muss sie

- wenig Änderungen an bestehenden Anwendungen benötigen,
- wenig bis keine zusätzliche Benutzerverwaltung einführen,
- in heterogenen Umgebungen funktionieren,
- möglichst frei verfügbar sein und offenen Standards folgen.

Unsere Lösung basiert auf der Erkenntnis, dass die überwiegende Mehrheit der Webanwendungen die Emailadresse des Benutzers oder Teile daraus als Loginname des Benutzers verwendet; erstens, weil die Mailadresse global eindeutig ist und zweitens, weil der Benutzer sich diese sowieso schon gemerkt hat. Dies gilt nicht nur für die meisten öffentlichen Webdienste, sondern auch innerhalb vieler Organisationen.

Auch X.509-Zertifikate müssen für jeden Nutzer eindeutig sein und enthalten meist ebenfalls genau diese Mailadresse als ein Merkmal. Durch diese Gemeinsamkeit ergibt sich nun die Möglichkeit einer zertifikatsbasierten MFA. Ein erfreulicher Nebeneffekt ist die Möglichkeit zur Kombination mit dem Rollout einer sicheren Mailinfrastruktur mit digitalen Signaturen und Ende-zu-Ende-Verschlüsselung mittels S/MIME, das ja auch auf X.509-Zertifikaten beruht.

Die Änderungen, die notwendig sind, um das Zertifikat als Nachweis der Identität des Nutzers gegenüber einer Webanwendung einzusetzen, sind flexibel aus den folgenden Komponenten kombinierbar:

Am einfachsten ist die Einführung von Zertifikaten, die in der Zertifikatsdatenbank des Browsers vorgehalten werden ("Softwarezertifikate"). Dafür sind weder Zusatzhardware noch Treiber notwendig; auch Änderungen an der Webanwendung sind unnötig. Für die Verifikation des Zertifikats reicht eine Änderung an der Konfiguration des Webservers, hinter dem die Webanwendung läuft. Bei vielen Webanwendungen kann bereits mit dieser Methode der zweite Faktor nur für gewisse (z.B. privilegierte) Funktionen aktiviert werden.

Ein möglicher zweiter Schritt ist die Modifikation der Anwendung, damit das Zertifikat mit dem Benutzernamen abgeglichen wird. Bisher wird nämlich nur überprüft, ob ein gültiges Zertifikat vorliegt und noch nicht, ob sein Username mit den Logindaten der Anwendung übereinstimmt.

Wenn der Quellcode der Anwendung vorhanden ist, kann diese Änderung häufig in wenigen Zeilen Codeänderung umgesetzt werden, teilweise sogar in einer einzigen Zeile. Falls eine Änderung an der Anwendung nicht möglich ist, kann die Überprüfung auch durch Konfigurationsänderungen am Webserver vorgenommen werden. Dafür ist aber eine Analyse des Loginprozesses der Anwendung notwendig. In beiden Fällen ist spezialisiertes Know-How notwendig, aber der Zeitaufwand relativ gering.

Bei höherem Schutzbedarf oder zeitweise unbeobachtet zugänglichen Rechnern (wie in Abb. 1) kann das Zertifikat statt auf dem Rechner auf einem geeigneten persönlichen Hardwaretoken abgelegt werden ("Hardwarezertifikat"). Neben der physischen Präsenz des Tokens (und damit typischerweise des Besitzers) ist damit gewährleistet, dass das Zertifikat nicht kopiert werden kann. Neben den Beschaffungskosten für die Zertifikate ist ein weiteres Hindernis die oftmals komplexe Installation von proprietären Treibern auf jedem Zugangsrechner.

Der beste Schutz wird durch Kombination aller drei Optionen erreicht (siehe Abb. 2).

Die Benutzerberatung in den Räumen der Bibliothek (Abb. 1) kann auch administrative Vorgänge wie das Zurücksetzen von Passwörtern vornehmen. Um diese Funktionen in dieser offenen Umgebung zu realisieren, wurden alle drei Massnahmen kombiniert. In einer User Study reagierten die Berater positiv auf die Umsetzung[1].

Fazit

Datenschutz und Datensicherheit gelten häufig als kompliziert, unfreundlich und teuer. Als Ergebnis werden sie deshalb häufig vernachlässigt oder gänzlich unter den Tisch gekehrt.

Es sollte daher das Ziel sein, dass Sicherheitsmassnahmen mittels weniger Tastendrücke installiert werden können und die Anwender auch möglichst nicht beeinträchtigt werden.

Die Benutzerfreundlichkeit für den Anwender ist bei unserer Lösung bereits sehr hoch und kann wohl kaum mehr signifikant optimiert werden.

Allerdings ist der Konfigurationsaufwand, so konkret und klein er auch sein mag, immer noch zu gross, um wirklich überall eingesetzt zu werden. Wir sind daher auf der Suche nach Ansätzen, um zukünftig MFA fast automatisch in Webanwendungen einbinden zu können.

Das Ziel ist klar: Der Trend zu mehr Kundennähe *und* Sicherheit darf nicht teuer sein.

Kurz&bündig

Der Trend zu Kundennähe und architektonischen Offenheit in Firmen und Behörden führt zu zusätzlichen Herausforderungen bei Datenschutz und -sicherheit. Viel zu häufig fehlen Know-How, Quellcode oder Ressourcen, um die betroffenen Anwendungen an die neuen Sicherheitsanforderungen anzupassen. Wir zeigen auf, wie gerade in diesen Fällen eine Zwei-Faktor-Authentisierung mittels X.509-Zertifikaten eine schnell umsetzbare, einfache, komfortable und trotzdem starke und erweiterbare Sicherheitskomponente sein kann, z.T. ohne Eingriff in die Anwendung[2].

Literatur

- Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-2: IT-Grundschutz-Methodik, 2017.
- Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3: Risikomanagement, 2017.
- Bundesamt für Sicherheit in der Informationstechnik, Massnahmenkatalog M4, 2016.
- https://fidoalliance.org/download/, abgerufen am 29.05.2018
- WALDVOGEL MARCEL/ZINK THOMAS, X.509 User Certificate-based Two-Factor Authentication for Web Applications, in: 10. DFN-Forum Kommunikationstechnologien, 2017.

Autoren

Marcel Waldvogel, Prof. Dr. sc. techn., Universität Konstanz, Deutschland
Marcel.Waldvogel@uni-konstanz.de

Thomas Zink, Dr., Universität Konstanz, Deutschland
Thomas.Zink@uni-konstanz.de

[1] Weitere technische Details sowie Konfigurationsbeispiele zu allen vorgestellten Mechanismen sind in (WALDVOGEL/ZINK 2017) beschrieben.

[2] Diese Arbeit wurde unterstützt durch das Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg im Rahmen des Projektes *bwITsec*.