Zugangssteuerung

Der Zugang an Systeme, egal ob Computer, Laptop, Mobile Device oder Server, muss geregelt sein. Das Ziel ist kurz, aber prägnant: Der Zugang zu Informationen und informationsverarbeitenden Einrichtungen ist eingeschränkt. Dies ist einfacher geschrieben als umgesetzt.

In der ISO-Norm 27002, Kapitel 9, sind dazu 14 Massnahmen zu diesem Thema gefordert. Zudem steht in der Fussnote der Schweizer Version der ISO 27002: Der Zugang kann sowohl physisch als auch logisch erfolgen. Die physische Sicherheit behandle ich erst in Kapitel 11 der Norm (folgt in der MB-Ausgabe 5/2019). Von den Begrifflichkeiten her unterscheide ich:

- Zutritt: damit ist der physische Zutritt in ein Gebäude, einen Raum oder ähnliches gemeint
- Zugang: damit ist das Login an einem System gemeint, klassisch Benutzername und Passwort
- Zugriff: damit sind die Rechte gemeint, auf ein Programm, eine Datei oder ähnliches zugreifen zu können

Der klassische Ablauf bei einer Anmeldung an einem System und Zugriff auf eine Ressource umfasst die folgenden Schritte (Bild 1): In einem ersten Schritt erfolgt die Identifikation der Person. Das kann ein Benutzername oder eine eindeutige ID sein. Im zweiten Schritt wird überprüft, ob dies auch stimmt, zum Beispiel mit der Eingabe eines Passwortes oder einem biometrischen Merkmal (Fingerprint, Augen, Venen usw.). Nun weiss das System, wer sich angemeldet hat. Im dritten Schritt werden Zugriffe beziehungsweise Rechte gewährt; im untenstehenden Bild das Recht, etwas auszudrucken. Immer wichtiger wird das vierte A: die Nachvollziehbarkeit. In einem Log wird jeder Zugriff gespeichert und kann später ausgewertet werden.

Richtlinien

Im ersten Schritt gilt es eine Zugangssteuerungsrichtlinie zu erstellen. Diese basiert auf den geschäftlichen, vertraglichen und gesetzlichen Anforderungen und muss regelmässig, das heisst mindestens jährlich, überprüft werden. Als Basis können die definierten Rollen (siehe MB-Ausgabe 12/2018) und unsere Werte inkl. Klassifizierung (siehe Ausgabe 2019/2) zugezogen werden. Idealerweise wird das Prinzip «Alles ist verboten, nur bei Bedarf werden Rechte vergeben» angewendet. Auch wenn nur eine einzige Person auf ein Verzeichnis oder Programm zugreifen muss, sollte dafür immer eine Gruppe angelegt werden. Dies vereinfacht spätere Wechsel oder Hinzufügen von Personen. Ein Verzeichnisdienst (LDAP, Active Directory usw.) bietet hier eine einfache Möglichkeit dazu. Bei Microsoft wird das A-G-Dl-P Prinzip propagiert:

- (A) Für jeden Benutzer wird ein Account erstellt
- (G) Benutzer werden in eine oder mehrere Gruppen zugewiesen
- (Dl) Für jedes Verzeichnis wird eine lokale Verzeichnisgruppe erstellt
- (P) Die Benutzergruppe wird der Verzeichnisgruppe zugewiesen und entsprechende Rechte vergeben

Damit dieses Modell sauber umgesetzt werden kann, muss zwischen den Rollen Zugangsbeantragung, Zugangsgenehmigung und Zugangsverwaltung unterschieden werden.

Alle Ereignisse im Zusammenhang mit der Zugangssteuerung müssen geloggt und sicher aufbewahrt werden. Mehr dazu folgt in der MB-Ausgabe 6/2019).

Die zweite Richtlinie, die gefordert wird, ist die Regelung zum Zugang zu Netzwerken. Immer öfters sieht man Mikrosegmentierungen von Netzwerken, es gibt nicht mehr die klassische Unterscheidung Internet, DMZ, Intranet, sondern es werden viele kleine Netzwerksegmente definiert, zum Beispiel: Drucker, bestimmte Server, Netzwerkspeicher, WLAN usw. Damit kann eine sehr feine Unterscheidung gemacht werden, wer auf was zugreifen kann. Weiter hat es den Vorteil, sollte sich doch einmal ein Hacker Zugriff ins Netzwerk verschaffen, ist er im entsprechenden Segment gefangen und er muss einen weiteren grossen Aufwand betreiben, um weitere Systeme infiltrieren zu können. In diese Richtlinie gehört auch, wer und auf welches WLAN (zum Beispiel Gäste, Mitarbeitende, Interne Systeme) und wer via VPN zugreifen darf. Die bereits vorher definierten Anforderungen (Trennung der Rollen, nur was notwendig ist freigeben, Überwachung usw.) gelten selbstverständlich auch für diese Richtlinie.

Benutzerzugangsverwaltung

Im vorherigen Kapitel wurden das Rollenmodell sowie die Vergabe von Rechten erwähnt. An die Verwaltung der Benutzer werden weitere Anforderungen gestellt:

– Es müssen eindeutige Benutzerkennungen vorhanden sein. Ob dies nun eine fortlaufende Zahl oder eine Kombination mit Vornamen und Nachname ist, muss jedes Unternehmen selber auswählen. Eine reine Zahl ist zwar sehr praktikabel, kann aber den Eindruck erwecken «ich bin ja nur eine Zahl hier». Eine Kombination aus zum Beispiel ein Zeichen Vorname, drei Zeichen Nachname stösst schnell mal an seine Grenzen: wenn das Unternehmen wächst, wird es zwangsläufig doppelte Kombinationen geben und dann muss wieder eine Zahl oder weitere Buchstaben hinzugefügt werden. Auch das komplette Ausschreiben mit Vor- und Nachname hat seine Tücken, zum Beispiel bei einer Heirat. Genau solche Ausnahmen müssen bereits im Vorfeld geregelt werden.

– Egal welches System verwendet wird, es darf auf keinen Fall doppelte Kennungen geben. Dies gilt es auch zu beachten, wenn eine Person das Unternehmen verlassen hat. Viele Systeme bekommen Mühe, wenn die entsprechende Kennung gelöscht wird (beispielsweise Wiki-Systeme). In diesem Fall werden Berechtigungen zwar entzogen (deaktiviert), die Kennung aber nicht gelöscht.

– Nicht nur die Vergabe und der Entzug von Berechtigungen müssen über diesen formalen Prozess erfolgen, sondern auch Änderungen. Ein wunderbares Beispiel sind die Auszubildenden. Diese lernen alle Abteilungen kennen, bekommen immer die dazu notwendigen Rechte, die vorherigen Rechte werden aber nicht entzogen. Am Ende der Ausbildung verfügen sie oft über mehr Rechte als teilweise der Abteilungsleiter.

– Ganz wichtig ist der Umgang mit privilegierten Rechten (Administrative Rechte). Administratoren dürfen niemals ständig mit dieser Kennung arbeiten. Für die normalen Tätigkeiten müssen sie ebenfalls einen unprivilegierten Account benutzen und nur wenn notwendig den zweiten mit höheren Rechten nutzen. Ich höre immer wieder, dass dies gar nicht möglich ist. Aus meiner Erfahrung habe ich aber noch nie eine Si-

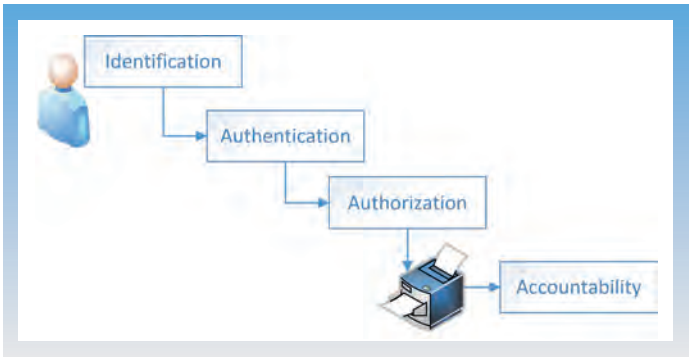


Bild 1: Der klassische Ablauf bei einer Anmeldung an einem System und Zugriff auf eine Ressource.

tuation angetroffen, wo dies nicht möglich gewesen wäre. Personen mit diesen höheren Rechten sind auf diesen Umstand zu schulen. Die Verantwortung muss ganz klar erwähnt sein. Als weitere Möglichkeit bieten sich Jump-Hosts an. Nur via diese kann mit privilegierten Rechten an Systemen (Betriebssystemen, Datenbanken usw.) gearbeitet werden. Heutige Systeme ermöglichen es dabei, jeden Tastenanschlag zu protokollieren oder gar ein Video aufzunehmen.

– Besonderes Augenmerk sollte auf externe Personen gelegt werden (Lieferanten, Partner usw. mit Zugriff auf Systeme). Auch diese sollten immer persönlich sein und dürfen innerhalb des externen Unternehmens nicht geteilt werden. Ist dies nicht möglich, muss die externe Stelle gezwungen werden, alle Personaländerungen mit Wissen dieses Accounts umgehend mitzuteilen. In einem solchen Fall ist das Passwort ohne Verzögerung zu ändern, da es ansonsten passieren kann, dass die ausgeschiedene Person das Passwort immer noch kennt und allenfalls zugreifen kann.

– Berechtigungen sind immer über den beschriebenen formalen Prozess zu vergeben. Mindestens jährlich müssen die Berechtigungen auf allen Systemen überprüft werden. Administrative Rechte sollten noch häufiger kontrolliert werden. Idealerweise wird dazu an den Inhaber des Systems/Verzeichnisses ein Auszug mit allen vergebenen Berechtigungen zugestellt. Dieser überprüft diesen Auszug und gibt sein OK oder allfällige Änderungen zurück. Ein kostenloses Tool für diese Aufgabe in einem Active Directory ist José Active-Directory-Dokumentation (kostenlos unter www.faq-o-matic.net/jose/ zu finden). Gleichzeitig ist damit eine saubere Dokumentation erstellbar.

Benutzerverantwortlichkeiten

Allen sollten die Anforderungen an den Schutz ihrer elektronischen Identität bewusst sein. Dies sollte auch Bestandteil in den Mitarbeiterweisungen sein. Die Zugangsdaten zu allen Systemen sind persönlich und müssen vertraulich behandelt werden. Folgende Anforderungen an Passwörter gelten:

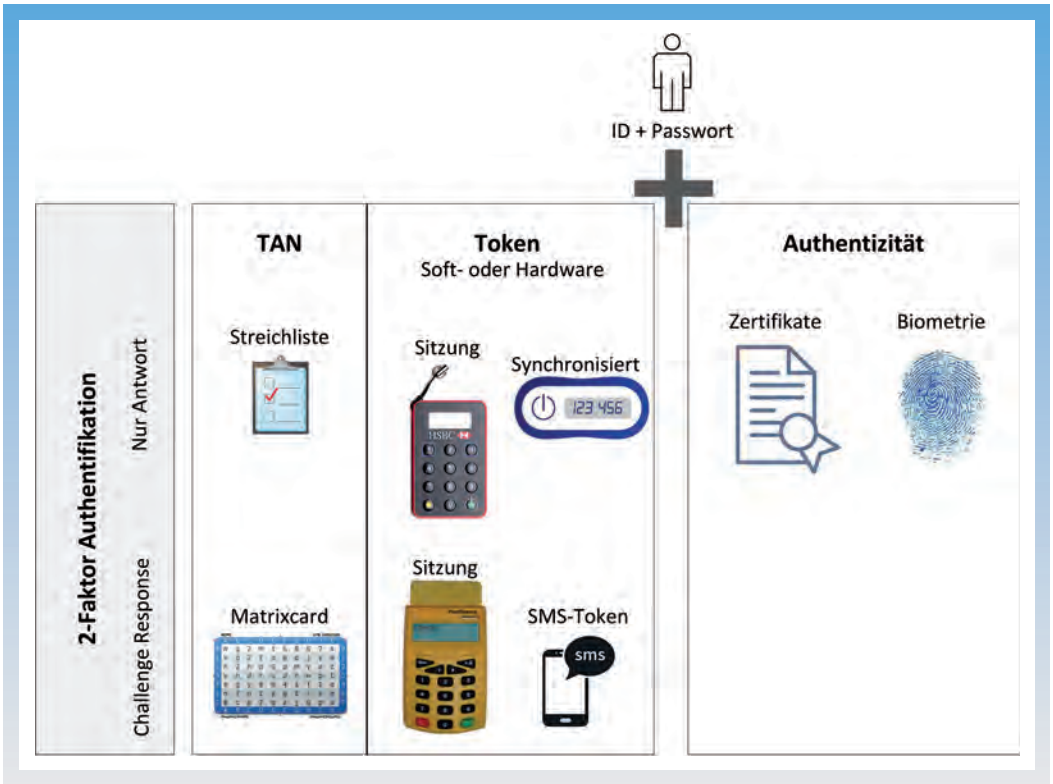
- Länge von mindestens zwölf Zeichen
- Benutzung mindestens einer Ziffer
- enthält mindestens einen Grossbuchstaben und einen Kleinbuchstaben
- enthält mindestens ein Sonderzeichen
- das Passwort darf nicht in einem Wörterbuch enthalten sein, darf kein Wort im Dialekt oder in der Umgangssprache irgendeiner Sprache oder irgendein solches Wort rückwärts geschrieben sein
- Passworte dürfen keine persönlichen Daten enthalten (zum Beispiel Geburtsdatum, Adresse, Name von Familienmitgliedern usw.)
- die letzten drei Passworte dürfen nicht wiederverwendet werden
- Passworte müssen alle sechs Monate geändert werden
- Das Passwort muss beim erstmaligen Anmelden an einem System geändert werden
- Passworte dürfen nicht in einem System zur automatischen Anmeldung gespeichert werden (zum Beispiel Makro oder Browser)
- Passworte, die für private Zwecke genutzt werden, dürfen nicht für Geschäftszwecke benutzt werden

Das Unternehmen kann den Mitarbeitenden Werkzeuge zur sicheren Aufbewahrung von Kennwörtern anbieten. Sehr verbreitet ist KeePass (https://keepass.info/ zu finden). Es ist Open Source und läuft auf praktisch allen Betriebssystemen. Diese Datei benötigt immer ein sehr sicheres Passwort, mindestens 20 Stellen sollten es schon sein. Die KeePass-Datei ist sicher verschlüsselt. Daher ist es möglich, diese auch auf einer Online-Plattform abzulegen und so auf jedem Gerät verfügbar zu haben.

Ob Passwörter aufgeschrieben werden dürfen, ist stark umstritten. Ich bin der Meinung, an einem sicheren Ort aufbewahrt, ist dies erlaubt. Sicher ist dabei nicht unter der Tastatur, direkt am Monitor angeklebt oder in der obersten Schreibtischschublade (alles bereits gesehen), sondern an einem Ort, wo niemand anderes drankommt. Passwörter dürfen auch nicht geteilt werden. In meinen Augen eine Unsitte ist beispielsweise während den Ferien das Passwort der Kollegin, des Kollegen, Chefs oder der Stellvertreterin usw. anzugeben, damit ein Zugriff auf die E-Mails möglich ist. Dazu gibt es andere Möglichkeiten. Neben dem klassischen Kennwort können folgende Möglichkeiten in Betracht gezogen werden:

– Biometrische Merkmale (Fingerprint, Iris, Retina, Venen usw.)
– Token
– Smartcards
– Kryptographische Schlüssel

Wo immer möglich sollte auf SSO (Single Sign On) gesetzt werden. Dabei muss die Anmeldung nur einmal gemacht werden und anschliessend ist der Zugriff auf diverse Ressourcen möglich. Die Berechtigungen werden zentral gesteuert und der Benutzer muss sich nicht mehr um weitere Logins kümmern. Bei Windows heisst dieser Dienst Active Directory in Kombination mit Kerberos.



Ein Passwort alleine genügt nicht mehr, es benötigt einen zweiten Faktor.

Systeme und Anwendungen

Alle Vorgaben machen nur dann Sinn, wenn es die Systeme und Anwendungen auch unterstützen. Die wichtigste Regel ist, dass ein Zugriff nur möglich ist, wenn auch eine Berechtigung dafür vorhanden ist. Bei der Evaluierung von Systemen und Anwendungen gilt es dies als Muss-Kriterium zu berücksichtigen. Idealerweise kann überall SSO verwendet werden.

Falls dies nicht möglich ist, muss die Anwendung die Möglichkeit zur Steuerung der Zugriffe anbieten. Minimal sollten die Berechtigungen Lesen, Schreiben, Löschen, Ausführen vorhanden sein. Systeme und Anwendungen sollten folgende Schutzmöglichkeiten aufweisen:

– Auf der Anmeldeseite werden keine vertraulichen Informationen angezeigt (zum Beispiel um was es sich handelt, welche Version der Software eingesetzt wird, die einzelnen Zeichen des Kennworts oder noch schlimmer das vorher falsch eingegebene Kennwort)

– Die Kontrolle von Benutzername und Kennwort erfolgt erst am Schluss. Ansonsten kann versucht werden, zuerst an gültige Benutzernamen zu kommen und erst dann das Kennwort «geknackt» werden.

– Vor allem in Amerika sind Warnhinweise vor der Anmeldung bekannt. Darin werden die Regeln angezeigt und auf Strafen bei Missachtung hingewiesen.

– Selbstverständlich sollten alle misslungenen, aber auch erfolgreichen Logins protokolliert werden. Viele misslungene Anmeldeversuche deuten auf einen Einbruchsversuch hin, erfolgreiche Logins dienen als Beweis, wer sich wann angemeldet hat.

– Von Online-Banking-Systemen her bekannt sind Hinweise, wann das letzte Login stattgefunden hat und allenfalls, wie viele fehlerhafte Versuche dazwischen erfolgt sind. In wie weit dies bei anderen Systemen Sinn macht, sollte in einer Risiko-Analyse betrachtet werden.

– Passwörter dürfen niemals unverschlüsselt über ein Netzwerk gesendet werden. Auch nicht im eigenen Firmennetzwerk. Bei Webseiten kann dies einfach mit

dem HTTPS überprüft werden. Erscheint dies in der Adresszeile der Webseite, werden die Daten verschlüsselt übermittelt.

– Inaktive Sitzungen müssen nach einer bestimmten Zeit automatisch beendet werden. Ob dies nun 5 oder 15 min. sind, muss jedes Unternehmen anhand der Kritikalität der Daten bestimmen.

– Das System sollte zudem Brute-Force-Angriffe erkennen und darauf reagieren. Einige Systeme verlängern zum Beispiel nach fünf fehlerhaften Eingaben die Dauer, bis das nächste Kennwort «ausprobiert» werden kann.

Für Systeme, die Kennwörter verwalten, gelten weitere Anforderungen:

- Unterschiedliche Benutzerkennungen sind notwendig.
- Sichere Kennwörter werden gemäss obenstehenden Anforderungen erzwungen.
- Bei der ersten Anmeldung muss das Kennwort durch den Benutzer geändert werden.
- Kennwörter müssen regelmässig gewechselt werden. Eine bestimmte Anzahl von vorherigen Kennworten dürfen dabei nicht mehr verwendet werden.
- Kennwörter werden niemals am Bildschirm angezeigt.
- Kennwörter werden verschlüsselt gespeichert. Idealerweise sogar als Salted Hash. Dabei werden vor der Verschlüsselung zusätzliche zufällige Zeichen vorangestellt und erst dann die Verschlüsselung ausgeführt. Sollte ein Hacker an die Kennwort-Datei gelangen, sind die Daten nur mit enorm grossem Aufwand wiederherzustellen.

Praktisch jedes Betriebssystem bietet eine Vielzahl von Werkzeugen für Administratoren an. Wenn der Zugang zu diesen nicht eingeschränkt ist, können diese auch von anderen Personen genutzt werden. Dabei besteht die Gefahr, dass die Schutzmöglichkeiten umgangen werden können. Unter Windows sind dies beispielsweise CMD oder PowerShell. Verantwortliche sollten daher immer bemüht sein, diese Werkzeuge so zu konfigurieren, dass ein Missbrauch nicht möglich ist. Zudem lohnt es sich, jede Verwendung sicher zu protokollieren. Die letzte Anforderung aus der Norm umfasst den Schutz von Quellcodes. Dieser muss gut geschützt werden. Der Zugriff darf nur denjenigen Personen möglich sein, die diesen auch benötigen. Gelangt dieser in die falschen Hände, kann unter Umständen die (Schutz-) Funktionsweise von Systemen ausgehebelt werden. Mit dem Kapitel A.9 der ISO-Norm werden Vorgaben an den Zugang und den Zugriff auf Systeme geregelt. Dabei werden neben den Systemen selbst auch Anforderungen an Kennwörter wie Erstellung, Speicherung und Änderung definiert. Werden die 14 Massnahmen konsequent umgesetzt, können Systeme und Anwendungen vor fremden Zugriffen geschützt und sicher betrieben werden.