SAFETY FIRST

DER GESCHÜTZTE ZUGANG ZU SYSTEMEN

von Andreas Wisler

Der Zugang zu Systemen, egal ob Computer, Laptop, Mobile Device oder Server, muss geregelt sein. Die ISO-Norm 27002 fordert dazu die Umsetzung von 14 Massnahmen. Dabei wird zwischen den Begrifflichkeiten Zutritt, Zugang und Zugriff unterschieden.

Der klassische Ablauf bei einer Anmeldung an einem System und Zugriff auf eine Ressource umfasst drei Schritte. 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). Nun weiss das System, wer sich angemeldet hat. Im dritten Schritt werden Zugriffe beziehungsweise Rechte gewährt.

RICHTLINIEN

Im ersten Schritt gilt es, eine Zugangssteuerungsrichtlinie zu erstellen. Diese basiert auf den geschäftlichen, vertraglichen und gesetzlichen Anforderungen und muss regelmässig, mindestens jährlich überprüft werden. Als Basis können die funktionalen Rollen in einem Unternehmen und die Firmen-Werte inklusive derer Klassifizierung 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.

Die zweite Richtlinie, die nach ISO 27002 gefordert wird, ist die Regelung zum Zugang zu Netzwerken. Dabei werden vermehrt Mikrosegmentierungen von Netzwerken definiert, zum Beispiel für Drucker, bestimmte Server, Netzwerkspeicher oder WLAN. Damit wird unterschieden, wer auf was zugreifen kann. Sollte sich einmal ein Hacker Zugriff ins Netzwerk verschaffen, ist er im entsprechenden Segment gefangen und muss einen grossen Aufwand betreiben, um weitere Systeme infiltrieren zu können. In diese Richtlinie gehört auch der Zugriff auf WLAN (zum Beispiel Gäste, Mitarbeitende, Interne Systeme) und VPN. Die bereits vorher definierten Anforderungen (Trennung der Rollen, nur was notwendig ist freigeben, Überwachung) gelten selbstverständlich auch für diese Richtlinie.

ZUGANGSVERWALTUNG

Im vorherigen Kapitel wurden das Rollenmodell sowie die Vergabe von Rechten erwähnt. An die Verwaltung der Benutzer werden weitere Anforderungen gestellt. So müssen eindeutige Benutzerkennungen vorhanden sein. Ob dies nun eine fortlaufende Zahl oder eine Kombination mit Vorname 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 Zeichen Vorname und dem Nachnamen stösst schnell an seine Grenzen: Wenn das Unternehmen wächst, wird es zwangsläufig

Zutritts-, Zugangs- und Zugriffssteuerung müssen geloggt und sicher aufbewahrt werden.

doppelte Kombinationen geben und dann muss wieder eine Zahl oder weitere Buchstaben hinzugefügt werden. Auch das komplette Ausschreiben mit Vorname 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. 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 der Abteilungsleiter.

Ganz wichtig ist der Umgang mit privilegierten Rechten. Administratoren dürfen niemals ständig mit dieser Kennung arbeiten. Für die normalen Tätigkeiten müssen sie einen unprivilegierten Account benutzen und nur wenn notwendig den zweiten mit höheren Rechten nutzen. Personen mit höheren Rechten sind auf diesen Umstand zu schulen. Als weitere Möglichkeit bieten sich Jump-Hosts an. Nur via diese kann mit privilegierten Rechten an Systemen (Betriebssystemen, Datenbanken) gearbeitet werden. Heutige Systeme ermöglichen es dabei, jeden Tastenanschlag zu protokollieren oder gar ein Video aufzunehmen. Besonderes Augenmerk sollte auf externe Personen gelegt werden wie Lieferanten oder Partner. 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 Okay oder allfällige Änderungen zurück.

Für Kennwörter gelten ganz besondere Anforderungen.

VERANTWORTLICHKEITEN

Die Anforderungen an den Schutz der elektronischen Identität sollte jedem 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 rückwärtsgeschrieben sein.
- Passwörter dürfen keine persönlichen Daten enthalten (zum Beispiel Geburtsdatum, Adresse, Name von Familienmitgliedern)
- Die letzten drei Passwörter dürfen nicht wiederverwendet werden
- Passwörter müssen alle sechs Monate geändert werden
- Das Passwort muss beim erstmaligen Anmelden an einem System geändert werden
- Passwörter dürfen nicht in einem System zur automatischen Anmeldung gespeichert werden
- Passwörter, die für private Zwecke genutzt werden, dürfen nicht für Geschäftszwecke und umgekehrt benutzt werden

Das Unternehmen kann den Mitarbeitenden Werkzeuge zur sicheren Aufbewahrung von Kennwörtern anbieten. Sehr verbreitet ist KeePass. Diese Datei benötigt immer ein sehr sicheres Passwort von mindestens 20 Stellen. 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. Gegen die Aufbewahrung an einem sicheren Ort spricht allerdings nichts. Passwörter dürfen auch nicht geteilt werden. Eine Unsitte ist beispielsweise den Kollegen während der Ferien das Passwort anzuvertrauen, damit ein Zugriff auf die E-Mails möglich ist. Werden die 14 Massnahmen aus der ISO 27002, Kapitel A9, konsequent umgesetzt, können Systeme und Anwendungen effektiv vor fremden Zugriffen geschützt und sicher betrieben werden. ■

ANDREAS WISLER

ist Inhaber und Senior Security Auditor bei der goSecurity GmbH.

www.gosecurity.ch