CONNECT

Newsmagazin der iNetWorx AG

04 | 2023

MFA & OTP

Doppelt genäht hält besser.

Vielen mögen die beiden Abkürzungen MFA und OTP auf den ersten Blick wenig sagen. Ausgeschrieben bedeuten sie **M**ulti **F**actor **A**uthentication beziehungsweise **O**ne **T**ime **P**assword. Das Konzept wird allgemein als Zwei-Faktor-Authentifizierung bezeichnet und besteht darin, dass man einen Faktor weiss (Passwort) und einen zweiten, meist variablen Faktor besitzt (z.B. Token in Form einer zufälligen Zahl). Mit MFA ist es kaum mehr möglich, ein Login zu missbrauchen. Bei eBanking-Zugängen kommt oft das sogenannte mTAN-Verfahren (mobile Transaktionsnummer) zum Einsatz, was einem ähnlichen Ansatz entspricht.

Viele Applikationen mit einem Online-Login unterstützen mittlerweile das MFA-Verfahren. Bei einigen Diensten erhält man ein SMS auf seine Handy-Nummer, andere benötigen den Einsatz einer sogenannten Authenticator-App auf dem Smartphone. Die beiden am meisten verbreiteten Apps hierfür sind der Google-und der Microsoft-Authenticator, welche sich bequem aus dem Play bzw. App Store installieren lassen.

Das Einrichten von MFA wird von den Anbietern der Dienste möglichst einfach gestaltet. Auch wenn Sie das Smartphone wechseln, müssen Sie die bereits erfassten Zugänge nicht wieder neu aufschalten. Der Transfer dieser Zugänge auf das neue Gerät unterscheidet sich je nach Anbieter leicht.

Unser Tipp: Aktivieren Sie das MFA-Verfahren überall, wo es möglich ist. Der Schutz Ihrer Daten wird mit wenig Zusatzaufwand massiv erhöht.

KONTAKT
iNetWorx AG
044 510 04 00

Netzwerk Zonen

Gärtchendenken

Es ist eine Krux mit der IT-Sicherheit: Je sicherer eine EDV-Infrastruktur konzipiert ist, desto komplexer und kostspieliger ist sie. Wer dafür nicht ein unbeschränktes Budget einsetzen kann, ist zwangsläufig mit einer Risikoabwägung konfrontiert: Mit wieviel Datenverlust kann die Firma im schlimmsten Fall leben? Wie lange können die IT-Systeme ausfallen, bevor ein empfindlicher Schaden entsteht? Es gilt also, Massnahmen umzusetzen, welche in einem guten Kosten-Nutzen-Verhältnis stehen.

IT-Sicherheit ist eine mehrschichtige Aufgabe. Sie beginnt bei geschulten Benutzern, die nur mit den notwendigen Benutzerrechten versehen sind. Weiter muss von den Daten ein sicheres Backup vorhanden sein. Die verwendeten Software und Betriebssysteme müssen durch regelmässige Updates gewartet werden, damit Sicherheitslücken geschlossen werden. Kommen lokale Server hinzu, ist auch eine Unterteilung des Netzwerks in verschiedene Zonen Pflicht.

Der letzte Punkt wird in kleineren Umgebungen leider oft vernachlässigt. Die Aufteilung eines Netzwerks in funktionale Zonen ist eine kostengünstige Massnahme zur Erhöhung der IT-Sicherheit. Was versteht man aber unter solchen funktionalen Netzwerkzonen? Zum Beispiel gibt es eine Zone ausschliesslich für Arbeitsstationen. Die Server-Dienste werden in einer zweiten Zone bereitgestellt, die Telefonie, welche heutzutage meist auch ein Teil des Netzwerks ist, in einer dritten und das Backup in einer weiteren. Bildlich gesprochen erhält jeder Dienst oder Funktion seine eigene Parzelle im Schrebergarten. Das zentrale Verbindungsglied zwischen den Zonen bildet die Firewall. Zur Kernaufgabe einer Firewall gehört es, den Netzwerk-Verkehr zwischen Zonen genau zu regeln (siehe auch Rubrik «Kurz erklärt» auf der Rückseite). So lässt sich beispielsweise konfigurieren, dass Arbeitsstationen nur auf ganz bestimmte Server-Dienste zugreifen können und alle anderen Anfragen von der Firewall geblockt werden.

Das Konzept der Zonierung folgt dem Need-to-know-Prinzip, sodass nur die zur Erfüllung der Aufgabe erforderlichen Informationen und Dienste verfügbar sind. Ist ein Gerät, z.B. eine Arbeitsstation, mit Schadsoftware infiziert, kann dank diesem Prinzip der potentielle Schaden begrenzt und ein «Flächenbrand» im Netzwerk verhindert werden. Ganz allgemein versuchen Angreifer oder Schadsoftware zur weiteren Infiltration des Netzwerks vor allem Sicherheitslücken von Server-Diensten auszunutzen. Auch wenn diese Dienste mit Passwörtern geschützt sind, ist es doch besser, dass in der Zone nicht benötigte Dienste erst gar nicht verfügbar sind.

Viele kleine Hindernisse erhöhen die IT-Sicherheit.

Machen wir ein konkretes Beispiel: Die Benutzer in einer Firma greifen von ihrem PC auf Dateien auf einem Server-Laufwerk zu. PCs und Server werden je in einer eigenen Zone betrieben. Die Firewall wird nun so konfiguriert, dass nur der Zugriff auf die Daten aus der Zone der PCs möglich ist. Zusätzlich befindet sich das Backup in einer weiteren Zone, die nur für das Schreiben des Backups aus der Zone des Servers freigegeben ist. Die Benutzer in der Zone mit den PCs haben keinen Zugriff auf das Backup. Wird nun der PC eines Benutzers mit Schadsoftware infiziert,

Kurz erklärt

Firewall

Die Kommunikation von zwei Netzwerkgeräten beruht auf IP-Adressen und Ports. Die IP-Adresse identifiziert jedes Gerät in einem Netzwerk eindeutig. Über die Ports kommunizieren die Geräte und tauschen die Daten untereinander aus. Auf speziellen Ports warten Server-Dienste auf Anfragen von anderen Geräten im Netzwerk, auch Clients genannt. Trifft so eine Anfrage ein, verarbeitet der Dienst diese und gibt dem Client eine entsprechende Antwort zurück. So funktioniert es im lokalen Netzwerk zwischen PC und Server, aber beispielsweise auch im Internet beim Aufrufen einer Webseite.

Firewalls sind eine Art Verkehrsknotenpunkt im Netzwerk, und sie agieren dabei wie Polizisten, welche den Datenverkehr an der Netzwerk-Kreuzung regeln. Wer (IP-Adresse des Clients) darf mit Wem (IP und Port des Servers) kommunizieren? Netzwerk-Administratoren erstellen einen präzisen Satz an Regeln, nach welchen der Datenverkehr eingeschränkt oder freigegeben wird. Moderne und leistungsfähige Firewalls können zudem die übermittelten Daten selbst analysieren und gegebenenfalls blockieren. Der obigen Analogie folgend kontrolliert der Polizist beim Regeln des Verkehrs zusätzlich noch die Insassen im Auto, während es über die Kreuzung fährt.

«Trudi» bei der Arbeit.

kann diese zwar, wie der Benutzer selber auch, auf die Daten zugreifen. Doch das direkte Angreifen von potentiellen Sicherheitslücken des Servers oder des Backups ist unmöglich, weil die Verbindungsversuche von der Firewall abgeblockt werden. Der Angriff und das Schadenpotential sind somit also klar begrenzt.

In der IT gibt es keine 100%-ige Sicherheit. Eine sichere IT-Umgebung zeichnet sich dadurch aus, dass sie möglichst wenig zulässt und viele kleine Hindernisse aufbaut. Die Aufteilung des Netzwerks in Zonen ist ein Teil davon. Die Latten am Zaun zum Nachbargrundstück werden damit nochmals etwas höher.

Gerne beraten und unterstützen wir Sie im Aufbau von sicheren Netzwerken. Kontaktieren Sie uns.

KONTAKT
Samuel Alfano
s.alfano@inetworx.ch

H. Mahr AG

Wo ist «Trudi»?

«Trudi» ist ein 5-Achs-Kranwagen in Diensten der H. Mahr AG in Benken. Und die Frage, wo sie gerade steckt, stellt sich für die Disposition im Büro. Die Firma Mahr ist in den Bereichen Abfallentsorgung, Recycling und Transport tätig. Dazu stehen rund 20 Fahrzeuge im Einsatz. Bei dieser Anzahl von Sammelfahrzeugen, Kranwagen und Sattelschleppern ist es wichtig zu wissen, wo sie sich gerade befinden, damit sie alle möglichst optimal und effizient für den nächsten Auftrag disponiert werden können.

Wir wurden darum von der Firma Mahr gebeten, eine einfache, interaktive Karte mit den aktuellen Standorten der Fahrzeuge als Web-Applikation zu programmieren. Das komplette System, bestehend aus Server und Web-Applikation, wird in-house bei der Firma Mahr selbst betrieben.

H.Mahr
Abfallentsorgung
8717 Benken

In den Fahrzeugen wurden in der Folge kleine GPS-Tracker eingebaut, welche in regelmässigen Abständen die Daten mit dem aktuellen Standort über das Mobilfunk-Netz senden. Der Anwendungsfall eignet sich ideal für die IoT-Plattform von Sunrise. Die Datenmengen sind klein und das dazu passende Abo für die SIM-Karten kostet nur wenige Franken pro Monat.

Die von den Trackern übermittelten Daten werden von einer Server-Applikation empfangen und verarbeitet. Insbesondere wird anhand der Standortkoordinaten die Adresse, bestehend aus Strasse, Hausnummer und Ortschaft, ermittelt. Schliesslich wird der Standort-Marker des Fahrzeugs auf der Karte mit diesen Angaben aktualisiert und an die neue Position verschoben. So ergibt sich für die Disposition stets ein aktueller Überblick von den Standorten der Fahrzeuge, der sich dynamisch wie ein Film von selbst aktualisiert.

Den Mitarbeitern in der Disposition ermöglicht dies eine vorausschauende und effizientere Planung der nächsten Tour für das jeweilige Fahrzeug. Und auch die Chauffeure werden seltener abgelenkt, weil weniger Rückfragen von Seiten der Disposition anfallen. Durch diese Prozessoptimierung werden schliesslich Zeit gespart und weniger Kilometer gefahren, was nicht nur tiefere Betriebskosten zur Folge hat, sondern letztlich auch der Umwelt zu Gute kommt.

Wir danken der Firma Mahr für diesen spannenden Auftrag und wünschen «Trudi» und ihren zwei- und mehr-achsigen Kolleginnen allzeit gute Fahrt.

KONTAKT
Andreas Mahr
a.mahr@inetworx.ch

Weitere Informationen:
www.mahr.ch