Doppelt hält besser – die Multi-Faktor-Authentifizierung

Doppelt hält besser – Mit dieser Redensart ist man in den meisten Situation des Lebens gut beraten. Und, wie sollte es auch anders sein, natürlich auch in der IT.

Zu meiner Lehrzeit legte die Eisenbahn noch jede wichtige Leitung doppelt. Zwei Drähte zum Weichensignal, zwei Glühbirnen im Leuchtsignal. Die Sicherheit ging vor.

Zwei- oder gar mehrfach war und ist bis heute ein greifbares Mittel zur Absicherung.

Doppelter Aufwand

Wenn da nicht immer der einhergehende Aufwand wäre. In der Regel muss dazu auch alles mehrfach gemacht werden.

Sehen wir uns heute die Zugangssicherung eines PC oder mobilen Gerätes an:
Ehrlich gesprochen haben viele ihre technischen Helfer bis vor einiger Zeit noch ganz ohne einen Zugriffsschutz wie z.B. ein Passwort oder einen PIN genutzt.
Es ist einfach lästig, sich jedes Mal erst anmelden zu müssen, um das Gerät zu nutzen.
In aller Regel funktioniert das Anmelden auch heute noch über die manuelle Eingabe eines möglichst komplexen, weil dann vermeintlich sicheren Kennwortes.

Und eben dieses Kennwort ist dann der Schlüssel für möglichst viele Funktionen
und Berechtigungen.
Wir wollen ja nicht ständig nach neuen Zugangscodes gefragt werden.

Hier liegt natürlich auch eine große Gefahr. Wer Benutzernamen und Kennwort kennt, der hat in der Regel Zugang zu allen Funktionen und meist auch über alle möglichen Wege.

Das bedeutet, während Sie ahnungslos vor dem Computer sitzen, hat sich ein Fremder unter Umständen mit Ihren Daten zeitgleich in den Online-Zugang eingeloggt.

Es gibt viele Ansätze, diese Lücke zu schließen.

Multi-Faktor-Authentifizierung

Ein inzwischen sehr bekannter Weg ist über die sogenannte Biometrie.
Wenn das Gerät in der Lage ist, die Person anhand biometrischer Merkmale zu erkennen, so ist eine Nutzung durch einen Fremden weitestgehend ausgeschlossen.
Der Fingersensor auf dem iPhone ist eine populäre Umsetzung dieser Idee.

Was aber wenn der Fingerprint nicht funktioniert.
Kein Problem, dann melden wir uns eben wieder über das Kennwort oder den PIN an.
Ok, damit ist der Fingersensor zwar sehr komfortabel, aber sicherer ist er nicht.

Erst eine zwingende Kombination aus Fingerprint und PIN erhöht den Zugriffsschutz. Jetzt müssen zwei Faktoren erfüllt sein (der eigene Finger und das Wissen über den PIN bzw. das Kennwort) um den Zugriff zu erhalten.
Das nennen wir in der IT dann die Multi-Faktor-Authentifizierung.

Leider ermöglicht nicht jedes Gerät eine biometrische Erkennung. Aber es gibt ja noch mehr Erkennungsmöglichkeiten: Standort, Uhrzeit, Umgebung, zusätzliches Gerät, SMS-PIN und noch viele mehr.

Multi-Faktor bedeutet viele Faktoren. Und im Idealfall definieren wir aus der Vielzahl der möglichen Faktoren eine passende Schnittmenge um dem Benutzer die Anmeldung an einem System so einfach wie möglich zu gestalten.

Als Beispiel möchte ich Ihnen kurz aufzeigen, wie ich bei mir diese Methode verwende:

Das Smartphone als Schlüssel

Am Schreibtisch nutze ich eine Webcam mit Gesichtserkennung. Dazu habe ich die Nähe meines Smartphones als weiteren Faktor definiert.
Wenn ich also am Schreibtisch vor meinem Notebook sitze und gleichzeitig mein Handy in der Nähe ist, dann werde ich automatisch angemeldet. Sehr bequem.

Wenn ich unterwegs bin, dann habe ich die Webcam nicht dabei.
Also muss ich mich unterwegs mit meinem PIN anmelden.
Ist dann auch noch mein Handy in der Nähe, bin ich im Gerät.

Sollte ich mein Handy vergessen haben und meine Kamera funktioniert vielleicht auch gerade nicht, dann melde ich mich eben mit PIN und Kennwort an.

Warum ein einfacher PIN nun plötzlich so sicher sein soll wie ein Kennwort, können Sie hier von mir erfahren.

Wachsende Gefahren erfordern ständige Anpassungen

Nein, die Welt wird nicht einfacher, ganz im Gegenteil. Komplexe Bedrohungen machen unseren Alltag immer unsicherer und erhöhen ständig die Notwendigkeit die eigenen Sicherheitsmethoden anzupassen.

Die Multi-Faktor-Authentifizierung ist eine gute Antwort einige Sicherheitsfragen.
Und wenn wir sie intelligent nutzen, erhöhen Sie unsere Sicherheit ohne
uns in der Nutzung unserer Geräte einzuschränken.

Gerne helfe ich Ihnen bei Erkennung und Umsetzung der passenden Lösungen

Mit den besten Grüßen,