Interview auf medinside.ch, dem Portal für die Gesundheitsbranche,
vom 06. Dezember 2017

„Ihre gesamten Sicherheitsvorkehrungen bringen nichts, wenn Ihr Passwort leicht zu erraten ist!“

Die Bedrohungslage nimmt zu: Cyberkriminelle nehmen vermehrt Einrichtungen des Gesundheitswesens ins Visier. Ein starkes Passwort kann vor solchen Angriffen schützen. IT-Sicherheitsexperte Oussama Zgheb verrät die wichtigsten Tipps.

Legende: Oussama Zgheb: „Verwenden Sie ein komplexes, einzigartiges Passwort und benutzen Sie Passwörter niemals mehrfach“

Herr Zgheb, ein Passwort dient zur Bestätigung der eigenen Identität bei unzähligen Internetdiensten wie E-Banking, sozialen Medien oder E-Mail. Mit der rasanten Ausweitung neuer Internet-Technologien hat der Missbrauch und der Diebstahl von Passwörtern erheblich zugenommen. Was kann den passieren, wenn jemand mein Passwort knackt?

Ihre gesamten Sicherheitsvorkehrungen bringen nichts, wenn Ihr Passwort leicht zu erraten ist! Und das kann sehr schlimme Folgen haben: Abhängig von der jeweiligen Webseite, kann sich der Dieb mit Ihrer Identität ausgeben und die sensiblen Daten ihrer Patienten missbrauchen, Mobbing tätigen, auf Ihre Kosten teure Gegenstände bestellen oder – noch schlimmer – Ihren Ruf schädigen. Kurz: Er kann alles machen, was auch Sie im Internet machen. Es kann also zu einem schweren finanziellen oder Image-Schaden für Sie oder Ihre Firma kommen.

Weshalb sind Menschen und Organisationen mit kriminellen Absichten genau an meinen Personendaten, beziehungsweise an den Personendaten meiner Praxis / meiner Abteilung interessiert?

Solche Angriffe sind meistens nicht gezielt. Hinter dem Angriff steckt oft ein Automatismus, welcher der Täter programmiert hat. Für den Angreifer ist es kein grosser Aufwand, diesen Automatismus für alle ihm bekannten Adressen auszuführen. So ist es für ihn auch ein leichtes Spiel, irgendeine Arztpraxis in seinen Adressraum aufzunehmen. Und: Jeder hat irgendetwas Interessantes auf seinem Gerät, auch Sie! Fakt ist, die Bedrohungslage nimmt zu und Cyberkriminelle nehmen vermehrt Einrichtungen des Gesundheitswesens ins Visier. Betraf dies bislang grössere Player wie Spitäler, sind auch zunehmend kleinere Institutionen wie Arztpraxen betroffen.

Ein starkes Passwort ist also zentral für die digitale Sicherheit. Was sind in Ihren Augen die häufigsten Passwortsünden?

Die grösste Sünde ist, ein Passwort für alle Dienste zu haben. Das hat zur Folge, dass wenn das Passwort abhandenkommt (und auf irgendeiner kriminellen Liste auftaucht), alle Ihre anderen Accounts auch betroffen sind. Zudem ist ein schwaches Passwort sehr schnell geknackt und auch die Aufbewahrung der Passwörter ist ein Punkt, welchem Beachtung geschenkt werden muss. Es ist ein No-Go, ein Passwort auf ein Post-it zu schreiben und dieses an den Bildschirm oder unter die Tastatur zu kleben. Das ist vergleichbar mit einer Kreditkarte, auf welcher der Code notiert ist. Vor Missbrauch und Diebstahl des eigenen Passwortes ist man am besten geschützt, wenn man folgende Grundsätze beachtet:

- Verwenden Sie ein **komplexes, einzigartiges Passwort** und verwenden Sie Passwörter niemals mehrfach. Jedes Passwort darf ausschliesslich für ein einziges Benutzerkonto verwendet werden. Diese Passwörter können Sie sich von einem **Passwort Manager** generieren lassen und darin auch gleich speichern. Ein Beispiel hierfür ist „Keepass": das ist ein grosser Safe, der alle Passwörter speichert. Zugang zu diesem Safe erhält man mit einem Masterpasswort.
- **Passwörter sind geheim**, diese sollen nie preisgegeben werden. Verrät man jemandem sein Passwort ist das, also ob man jemandem seinen Hausschlüssel gibt. Nur kann man den Hausschlüssel wieder zurückverlangen, das Passwort jedoch nicht.
- Die Mindestlänge für ein Passwort liegt bei **10 bis 12 Zeichen**. Alles darunter kann mit den richtigen Ressourcen in kurzer Zeit geknackt werden. Ab 12 Zeichen ist man auf der sicheren Seite. Nutzen Sie dabei in jedem Passwort auch Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen.
- Ein Passwort soll **nie in Bezug zur Person** stehen. Verwenden Sie für Ihr Passwort weder Ihren Namen, noch Ihren Wohnort oder Ihr Geburtstag.
- Sobald bei einem Dienst eine **2-Faktor Authentisierung** vorhanden ist (was im Gesundheitswesen state-of-the-art und von Gesetzes wegen zwingend ist): Nutzen Sie diese! So kann selbst wenn jemand Ihr Passwort kennen würde, nicht auf den Dienst zugegriffen werden.

All die Vorteile, die man durch den Computer hat, haben auch ihren Preis. Klar ist es mühsam und anstrengend, so viel Wert auf gute Passwörter zu legen – aber es wird noch viel mühsamer und anstrengender, sobald eine fremde Person Zugriff auf Ihren Account hat!

Ich muss mir schon privat sehr viele Passwörter merken. Jetzt muss ich das auch noch fürs Geschäft. Wie mach ich das am besten?

Am besten installiert man sich dafür – wie oben erwähnt – einen Passwort Manager auf dem Smartphone. Darin kann man sich verschiedene Ordner anlegen, zum Beispiel für privates und geschäftliches. Dadurch hat man seine Passwörter immer dabei. Und selbst wenn das Smartphone verloren geht, sind die Passwörter sicher, da der Passwort Manager durch ein Masterpasswort geschützt ist. Heute müssen Sie sich somit nur noch ein einziges Passwort merken, alles andere erledigt der Passwort Manager. Ziemlich einfach und zugleich sehr sicher!

Oussama Zgheb ist als Solution Architekt und Security Officer mitverantwortlich für die Bereitstellung und Weiterentwicklung der sicheren IT-Architektur für die HIN Plattform und deren Dienste. Dabei verbindet er IT-Trends, IT-Excellence, Innovation und Service Delivery-Themen mit Informationssicherheit.