Die Top 10 Sicherheitstipps für Ärzte

Tipp 1
Vorsicht beim Umgang mit persönlichen Daten und Fotos

Zu den häufigsten modernen Straftaten gehört der elektronische Diebstahl persönlicher Daten. Die Motive für Kriminelle sind vielfältig. Hier einige der wichtigsten Beweggründe:

Jemand möchte Sie erpressen.
Jemand möchte Ihre Identität fälschen und damit Strafdaten begehen.
Jemand möchte bei Ihnen zu Hause oder im Büro einbrechen und benötigt Ihren Standort.
Jemand möchte Daten über Sie weiterverkaufen.
Jemand möchte Sie belästigen.

Diese Liste kann beliebig fortgesetzt werden und zeigt auf, dass Sie wachsam sein sollten, wem Sie diese wichtigen und wertvollen Daten in Programme oder Webformulare eingeben. Sie sollten dabei auch immer einrechnen, dass auch es zu einem Datendiebstahl beim Betreiber dieser Anwendungen kommt, und auch wenn dieser sorgfältig mit Ihren Daten umgeht, diese eventuell abhanden kommen können.

Die Eingabe der Sozialversuchungsnummer, von Kontoverbindungen oder gar die elektronische Versendung von Reisepasskopien per E-Mail kann im Falle von Datenlecks zu großen Problemen für Betroffene führen, da die Sperre und Änderung sehr aufwendig ist.

Missbrauch persönlicher Fotos

Häufig werden bei der Verwendung von Digitalkameras oder Smartphones die genauen Informationen über den Aufnahmeort mitgespeichert. Das erscheint für Benutzer sehr bequem, da man später die Bilder sortiert nach dem Ort ansehen kann. Allerdings können auch Kriminelle diese Informationen auslesen.

Für Bilder sollte man daher immer die Speicherung von Informationen über den Aufnahmeort abschalten (das so genannte "Geo-Tagging"), weil sonst Kriminelle über den Aufnahmeort des Fotos wertvolle Hinweise über Ihren Aufenthaltsort, Ihr Bewegungsprofil oder Ihre Wohnsituation erhalten können.

Häufig werden Fotos von Personen auch missbräuchlich als Profilbilder von anderen verwendet, um Scheinidentitäten aufzubauen. Eine interessante Möglichkeit, um herauszufinden, ob etwa das eigene Profilbild oder andere Fotos widerrechtlich von anderen verwendet werden, bietet die Google-Bildersuche. Dazu muss man ein Bild in die Google-Suche https://images.google.com hochladen. Diese Suche liefert dann als Ergebnis, ob sie eine Person erkannt hat bzw. ob das Bild in einem Profil verwendet wird.

Tipp 2
Überprüfung bestehender Datenlecks

Sie können mit verschiedenen unentgeltlich am Internet verfügbaren Tools herausfinden, ob Ihre E-Mail-Adresse schon einmal Teil eines Datenlecks war.

Über den HPI Identity Leak Checker https://sec.hpi.de kann ermittelt werden, ob zu einem E-Mail-Konto gehörige Informationen und Passwörter bereits in einem bekannten Hack enthalten sind. Diese Webseite verfügt derzeit über die Daten von fast zehn Milliarden gehackten Benutzerkonten aus 800 Datenlecks.

Zur Abfrage muss man die betroffene E-Mail-Adresse auf der Webseite angeben, das Ergebnis wird auf diese Adresse zugestellt.

Ein anderes Verfahren benutzt die Webseite https://haveibeenpwned.com, bei der man nach Eingabe der E-Mail-Adresse sofort ein Ergebnis angezeigt erhält. Sie verfügt über die Informationen über ca. 8 Milliarden Benutzerkonten, die gestohlen wurden.

Tipp 3
Sichere Passwörter

Ein wichtiges Einfalltor für Computerkriminalität sind zu einfache und leicht ausspähbare oder errechenbare Passwörter. Über die Webseite *https://howsecureismypassword.net* kann man die Sicherheit von Passwörtern überprüfen. Dabei wird nach Eingabe des Passwords die Zeit errechnet, die benötigt wird, um das angegebene Passwort mit modernen Programmen zu „cracken“. *Hinweis: Bitte geben Sie hier nicht Ihr wirkliches Password ein, sondern nur ein diesem ähnliches!*

Eine Empfehlung für sichere Passwörter ist umfangreich. Folgt man den folgenden fünf Regeln und ändert die Passwörter auch laufend, lebt man aber bestimmt sicherer:

- Länge von mehr als 15 Zeichen
- Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen verwenden
- Möglichst keine Wörter aus dem Wörterbuch
- Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Anwendungen und Diensten
- Passwortwechsel bei Sicherheitsvorfällen und für Passwörter, welche die obigen Regeln nicht erfüllen

Für viele Benutzer ist es schwierig, den Überblick über viele verschiedene und lange Passwörter zu behalten. Dabei kann man inzwischen aus einer großen Anzahl von *Passwort-Managern* auswählen, die neben Passwörtern und Benutzer-IDs auch andere sensible Informationen wie PIN-Codes und andere geheime Informationen verschlüsselt speichern.

Tipp 4: Zwei-Faktor-Authentifizierung

Der Einsatz von Zwei-Faktor-Authentifizierung wird von vielen Anwendungen angeboten und macht für die Anmeldung an ein System neben dem Passwort einen weitern „Faktor“ notwendig.

Dieser zweite Faktor kann ein Zahlencode sein, der als SMS zugesandt wird, oder ein PIN-Code, der auf einer Smart-Card angezeigt wird, aber auch ein Fingerabdruck.

Zwei-Faktor-Authentifizierung ist viel sicherer als ein einfaches Passwort, da es dann nicht mehr ausreicht, ein solches abzufangen (z.B. durch Phishing oder über den Einsatz von Keyloggern), um illegal in ein System zu kommen. Es steht auch für die meisten Kreditkarten zur Verfügung (z.B. Mastercard „Secure Pay“ oder „Verified by Visa“) und verhindert deren Missbrauch.

Für wichtige Systeme im Gesundheitsbereich wie ELGA wäre die durchgängige Verwendung von Zwei-Faktor-Authentifizierung dringend angebracht!

Tipp 5: Einsatz von Schadsoftware-Scannern und regelmäßige Updates

Jeder Computer und auch jedes Smartphone benötigen einen guten Virenscanner und eine Firewall, damit laufend die Gefahr der Infektion mit Schadsoftware überprüft und abgewendet werden kann. Auf den Webbrowsern sollten Möglichkeiten, Programme auszuführen (z.B. mittels JavaScript) oder Informationen auszulesen (mittels Cookies), so weit möglich deaktiviert werden.

Überdies muss regelmäßig das Einspielen von Updates und Patches für alle verwendeten Systeme geprüft und durchgeführt werden. Dazu gehören vor allem Betriebssystem-Updates und ab und zu auch der Wechsel der Hardware, um ein neues, besseres Betriebssystem mit neuen Sicherheitsmerkmalen zu installieren.

Aber nicht zu vergessen sind auch die vielen Geräte, die das "*Internet der Dinge*" ausmachen. Auch diese müssen regelmäßig einem Update unterzogen werden.

Tipp 6: Backups von allen wichtigen Systemen

Gerade die Angriffe mit Ransomware zeigen, wie wichtig es ist, laufend Backups der Systeme zu machen und diese über lange Zeit sicher aufzubewahren. Die Aufbewahrung sollte auf keinen Fall am Ort der Systeme erfolgen, da etwa bei einem Brand die völlige Zerstörung aller Daten droht, falls nicht noch ein zusätzliches Cloud-Backup existiert.

Wichtig ist hier auch, dass Backups über mehrere Monate bis zu Jahren hin aufbewahrt werden. Oft ist es nämlich schwierig, den Zeitpunkt des Befalls durch Schadsoftware zu ermitteln, die sich über Monate im System einnistet.

Backups sollten immer verschlüsselt abgespeichert werden. Das gilt besonders auch für Cloud-Backups!

Tipp 7: Verschlüsselung verwenden

Die meisten Webseiten bieten heute an, dass man mit ihnen sicher verschlüsselt über den Einsatz des HTTPS-Protokolls kommuniziert. Betreibt man eine eigene Webseite, muss man für die Verwendung dieses Protokolls lediglich ein Zertifikat anmelden und im WWW-Verzeichnis einspielen.

Nicht zu vergessen ist auch die Verschlüsselung von Festplatten und USB-Sticks, die meist sehr einfach mit den vom Betriebssystem zur Verfügung stehenden Mitteln möglich ist.

Tipp 8: Sichere E-Mails und mehr Mail-Disziplin

Der alte Spruch „Jedes Schrifterl ist ein Gifterl“ gilt besonders bei der Verwendung von nicht verschlüsselten E-Mails, die einfach von Unbefugten mitgelesen werden können. Sehr vertrauliche Inhalte sollten immer verschlüsselt ausgetauscht – oder überhaupt nicht elektronisch übermittelt werden.

Es empfiehlt sich auch die Verwendung eines E-Mail-Systems, das generell verschlüsselt arbeitet, wie beispielsweise ProtonMail vom Schweizer Anbieter Proton Technologies AG in Genf oder Hushmail vom kanadischen Anbieter Hush Communications Ltd.

Je nach Sicherheitsstandard sollte die Möglichkeit, über Webmail ins Mail-System einzusteigen, überlegt werden. Hier kann es beispielsweise vorkommen, dass man an einem öffentlichen Rechner (etwa in einer Flughafenlounge) in sein E-Mail-System einsteigt, ohne zu bemerken, dass ein Krimineller vorher einen Keylogger auf diesem Rechner installiert hat. Wird in diesem Fall keine Zwei-Faktor-Authentifizierung verwendet, könnte ein Krimineller nun ausreichende Anmeldeinformationen ausgespäht haben, sich in Ihrem Namen anmelden und alle Ihre Nachrichten lesen und neue versenden.

Tipp 9: Vorsicht mit unbekannten USB-Sticks

USB-Sticks oder das, was dafür gehalten wird, können großen Schaden anrichten und durch Anstecken den betroffenen Computer mit Malware infizieren.

Ein gutes Beispiel ist der „Rubber Ducky“, ein USB-Stick, der, an einen Computer angesteckt, ein Backdoor („Hintertür“) installiert, Dokumente und Passwort stiehlt und einen Angriffsvektor für spätere Penetrationstests aufbaut.

Man sollte nur USB-Sticks verwenden, deren Herkunft man kennt und die vor der Verwendung geprüft wurden!

Tipp 10: Abschluss einer Cyber-Versicherung

Viele Versicherungsunternehmen bieten inzwischen im Rahmen von Hausratsversicherungen oder als separat gekennzeichnete Cyberprodukte die Absicherung gegen die finanziellen Folgen von Cyberangriffen an.

Namhafte österreichische Versicherungen haben die umfangreiche Unterstützung bei Problemen mit Computern oder Unterhaltungselektronik bereits seit mehreren Jahren im Angebot. Sie werben mit folgenden Leistungsmerkmalen:

- Soforthilfe eines IT-Spezialisten per Chat oder Telefon bei Fragen zu Computer, Smartphone und Co.
- Hilfe bei Hard- und Software-, Netzwerk- oder Internetproblemen
- Beratung bei Identitätsdiebstahl und Cyber-Mobbing
- Services: Onlinedatensicherung und IT-Remoteunterstützung

- „Unterstützung beim Umgang mit den allgemeinen Gefahren des Internetgebrauchs, wie z.B. Cyber-Mobbing durch Verunglimpfungen in sozialen Netzwerken und Cyber-Crime durch das Ausspähen von Passwörtern oder Zugangsdaten (‚Phishing') oder Identitätsdiebstahl
- Qualifizierte Begleitung und Unterstützung bei der Beurteilung von Cyberrisiken und Organisation der Einleitung von rechtlichen Schritten – wenn notwendig
- Koordination und Organisation rechtlicher Beratung (max. 1 h pro Kalenderjahr) – telefonisch, schriftlich oder persönlich."

Für berufliche Zwecke (z. B. für eine Arztordination) bietet sich darüber hinaus der Abschluss einer gewerblichen Cyber-Versicherung an, die eine etwaige Betriebsunterbrechung durch einen Cyber Angriff abfedern kann.