Hacking Akademie

SICHER IM INTERNET

20 schlechte Online-Angewohnheiten,
die du besser sofort ablegst!

>>> Inhaltsverzeichnis

Einleitung { 02

01. (Dasselbe Passwort für alle Zugänge verwenden) ; 02

02. (Schwache Passwörter nutzen) ; 03

03. (Keine Zwei-Faktor-Authentifizierung einsetzen) ; 04

04. (Verwendung eines schwachen WLAN-Schlüssels) ; 05

05. (Updates ignorieren) ; 06

06. (Keinen Viren- und Malware-Schutz implementieren) ; 07

07. (Keine Backups anfertigen) ; 07

08. (Den Bildschirm nicht sperren) ; 08

09. (Davon ausgehen, dass dein System automatisch sicher ist) ; 08

10. (Auf unbekannte Links aus unsicheren Quellen klicken) ; 09

11. (Herunterladen von Anhängen ohne Prüfung) ; 09

12. (Herunterladen von dubiosen Dateien von unseriösen Webseiten) ; 10

13. (Ungeschütztes Notieren von Passwörtern im Klartext) ; 10

14. (Surfen auf HTTP-Seiten) ; 11

15. (Online-Banking über öffentliche Hotspots) ; 11

16. (Mit allen Lizenzbedingungen einverstanden sein) ; 12

17. (Zu viele Browsererweiterungen nutzen) ; 12

18. (Auf Virenwarnungs-Popups klicken) ; 13

19. (Daten unverschlüsselt in die Cloud hochladen) ; 13

20. (Sich zu sehr auf die technische Sicherheit verlassen) ; 14

}

>>> Einleitung

Im Internet lauern unzählige Gefahren. Es ist unmöglich, sie alle aufzuzählen: Hacker, Phisher, Scammer, Viren, Trojaner, Spyware wie Keylogger, uvm. Wenn wir uns davor schützen wollen, können wir nicht auf unseren Provider oder eine Firewall vertrauen. Wir müssen selbst aktiv werden. Wir selbst sind dafür verantwortlich, unsere Angriffsfläche bestmöglich zu reduzieren.

//

Und auch wenn es viele IT-Fachleute gibt, die eigentlich wissen, worauf sie achten müssen, gilt auch hier, dass der Schuster oft die schlechtesten Schuhe trägt. Oft ist es Faulheit oder Bequemlichkeit, die dazu führen, dass wir schlechte Angewohnheiten haben, wenn wir mit dem Internet interagieren. Insbesondere ein Argument ist dabei auch häufig zu hören: „Wer sollte Interesse daran haben, meinen Account zu hacken?“ Oder: „Ich habe eh nix zu verbergen!“ Aber das ist absolut der falsche Ansatz!

//

Zum einen müssen Hacker gar nicht speziell dich im Visier haben. Es reicht, dass du ein einfaches Ziel bist und zufällig am falschen Ort zur falschen Zeit bist. Andererseits sind viele Angriffe automatisiert und werden durch Trojaner und andere Malware völlig wahlfrei ausgeführt. Da kann es dich dann ganz genauso treffen, wie jeden anderen auch.

//

Vielleicht setzt du ja auch schon alle Tipps und Tricks in diesem Ratgeber um, aber andererseits findest du hier eventuell auch noch die eine oder andere Anregung, wie du mit wenig Aufwand und ein kleines bisschen Disziplin deine Sicherheit enorm erhöhen kannst. Also lass uns mal die größten Sünden betrachten, die Internet-Benutzer begehen und unsere eigenen Verhaltensweisen optimieren.

>>> 01. Dasselbe Passwort für alle Zugänge verwenden

Ha, erwischt! Ich habe genau gesehen, wie du gezuckt hast! Die meisten von uns nutzen ihr Lieblingspasswort auf diversen Plattformen und für diverse Anmeldungen. Das ist jedoch eine der schlechtesten Angewohnheiten überhaupt! Wenn ein Angreifer unser Passwort knacken kann, hat er damit automatisch Zugriff auf diverse andere unserer Online-Accounts.

//

Auch wenn es zunächst unverhältnismäßig aufwändig erscheint: Erstelle dir für jeden Online-Zugang und jedes Login ein eigenes Passwort. Du kannst Passwörter in einem Passwort-Safe speichern und musst dir daher deine Passwörter nicht merken. Und ja, auch wenn die Verwendung eines Passwort-Safes etwas mehr Aufwand erfordert, ist es das absolut wert. Es erfordert etwas Disziplin, aber wenn du es erst einmal eingerichtet und dich daran gewöhnt hast, geht die Verwendung eines Passwort-Safes in Fleisch und Blut über.

//

Es gibt zahlreiche Passwort-Safes zum Gratis-Download oder gegen geringes Entgelt. Einige davon können im Browser integriert werden und stellen automatisch die richtigen Login-Daten bereit. Man könnte das hier beschriebene Fehlverhalten also auch mit „Keinen Passwort-Safe nutzen“ beschreiben.

>>> 02. Schwache Passwörter nutzen

Die häufigsten Passwörter sind **123456**, **quertz** bzw. **querty** oder 123456789. Hoffentlich lachst du jetzt schallend und schüttelst den Kopf. Dann bist du schon mal auf einem guten Weg. Wenn du dich jetzt irgendwie erwischt fühlst, solltest du ganz schnell handeln!

//

Nehmen wir an, dass du tatsächlich für jeden Zugang eigene Passwörter verwendest, die aber ähnlich schwach sind wie die obigen Beispiele. Dann kannst du davon ausgehen, dass deine Accounts schneller gehackt werden, als du „Hilfe, ich wurde gehackt!“ aussprechen kannst. Im Internet kursieren unzählige Listen mit vielen Millionen Passwörtern, die schon verwendet und geknackt wurden. Für ein Passwort-Cracking-Tool wie z.B. John the Ripper ist es ein Leichtes, dein schwaches Passwort mit Hilfe einer geeigneten Wortliste zu knacken.

//

Also: Denk dir starke Passwörter aus! Das sind Passwörter, die noch in keiner Wortliste im Internet oder Darknet auftauchen und die auch nicht so leicht durch eine Brute-Force-Attacke geknackt werden können. Ein solches Passwort sollte nach Möglichkeit 10 Zeichen oder länger sein und eine scheinbar zufällige Abfolge an Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen darstellen.

//

Scheinbar, weil du auch starke Passwörter z.B. aus Sätzen ableiten kannst. Nehmen wir den Satz „Ich weiß, was du letzten Sommer getan hast!“ Dann könnte dein Passwort z.B. lauten: **Iw,wdlSgh!**

//

Wenn wir das jetzt noch mit Ziffern und ggf. Sonderzeichen modifizieren, sieht das ggf. so aus:
lw,wd1$gh!
//
Das ist kein sooo schlechtes Passwort und es ist leicht herzuleiten, wenn man den Ausgangssatz kennt. Nun solltest du evtl. nicht unbedingt einen Filmtitel nutzen, den jeder kennt, aber wenn du dir einen eigenen Satz ausdenkst und daraus ein Passwort ableitest, hast du bald ein recht sicheres Passwort.
//
Allerdings gibt es noch einen besseren Weg! Verwende ein vollkommen zufälliges Passwort und nutze am besten gleich 20 oder 30 Zeichen! Ok, das kannst du dir dann ganz sicher nicht mehr merken. Aber wenn du einen Passwort-Manager nutzt (siehe Punkt 1), dann ist das alles kein Problem. Und das ist dann auch der Königsweg. Die meisten Passwort-Manager bringen einen eigenen Passwort-Generator mit. Damit kannst du dir ein sicheres Passwort erstellen.
//
Andernfalls gehst du einfach auf einen der vielen Online-Passwort-Generatoren, z.B. www.password-generator.eu, und erstellst dir ein sicheres Passwort. Verwende nach Möglichkeit Groß- und Kleinbuchstaben, Ziffern und die verfügbaren Sonderzeichen. Wenn du dir das Passwort ohnehin nicht merken musst, dann kannst du es auch gleich lang genug machen, dass selbst der stärkste NSA-Supercomputer in 1000 Jahren keine Chance hat, dein Passwort zu knacken. Also nutze 20 oder 30 Zeichen, das sollte reichen.

>>> 03. Keine Zwei-Faktor-Authentifizierung einsetzen

Wir bleiben noch bei der Authentifizierung, weil sie einfach ein so elementares Konzept in der Internet-Sicherheit darstellt. Während eine Username-Passwort-Kombination in vielen Fällen relativ einfach zu knacken ist, erhöht die Zwei-Faktor-Authentifizierung den Schutz der Anmeldeprozedur um ein Vielfaches und macht es Angreifern enorm schwer bis unmöglich, einen Account zu knacken.
//
Immer mehr Anbieter bieten diese Zwei-Faktor-Authentifizierung an, die auch mit 2FA abgekürzt wird. Und du solltest sie unbedingt nutzen! Ja, es ist etwas aufwändiger, sich anzumelden. Aber dafür minimieren sich deine Sorgen, dass dein Account gehackt werden könnte.
//
Was bedeutet Zwei-Faktor-Authentifizierung? Nun, grundsätzlich gibt es drei Formen, wie wir nachweisen können, wer wir sind:

1. Durch etwas, was wir wissen (Passwort, PIN)
2. Durch etwas, das wir haben (Ausweis, Zutrittskarte, Schlüssel)
3. Durch etwas, das wir sind (biometrische Erkennung wie Iris, Retina, Gesicht, Fingerabdruck)

//

Bei der 2FA werden zwei dieser Alternativen kombiniert. Wenn wir uns also mit einem Benutzernamen und dem Passwort an einer Internet-Plattform anmelden (das ist etwas, das wir wissen) und dann noch einen PIN eingeben müssen, den wir über SMS auf unser Smartphone erhalten (das ist etwas, das wir haben), dann wäre das ein Beispiel für eine 2FA.

//

Selbst wenn der Angreifer Zugang zu unseren Login-Daten hat, benötigt er zusätzlich die Angaben in der SMS, die an unser Handy geschickt wurden. Das ist sehr schwer zu realisieren. Daher ist diese Form der zusätzlichen Sicherheit insbesondere dann zu empfehlen, wenn es sich um sicherheitskritische Zugänge, wie Online-Banking oder Ähnliches handelt.

>>> 04. Verwendung eines schwachen WLAN-Schlüssels

Und weil es so schön ist, bleiben wir noch einmal kurz bei den Passwörtern. Ein Fehler, der leider auch immer wieder gemacht wird, ist die Verwendung eines schwachen WLAN-Schlüssels. Hier sollten auch besser gleich mindestens 20 zufällige Zeichen genutzt werden, um den Zugang zu schützen. Denk dran: WLAN ist eine Funktechnologie, die in alle Richtungen strahlt. Wenn ein Angreifer im Nebenraum, in der Nebenwohnung oder auch nur im Nebenhaus oder auf dem Parkplatz neben dem Haus steht, kann er alle übertragenen Daten mitlesen.

//

Durch sogenannte Replay-Angriffe kann ein Angreifer bestimmte Datenpakete immer wieder an den Access Point schicken, um somit genügend Pakete zu sammeln, die ihm unter Umständen das Knacken des Passwortes ermöglichen. Je komplexer und zufälliger das Passwort, desto unwahrscheinlicher wird ihm das gelingen. Daher lass es bitte nicht darauf ankommen und mach dir die Mühe, ein wirklich langes und komplexes Passwort für deinen WLAN-Zugang festzulegen.

>>> 05. Updates ignorieren

Ja, das mit den Passwörtern ist wirklich eine große Sache, daher haben wir die ersten 4 Punkte diesem Thema gewidmet. Aber natürlich gibt es auch diverse andere schlechte Angewohnheiten, die IT-Anwender pflegen, um möglichst bequem durchs Leben zu kommen. Eine der übelsten ist das Ignorieren von Updates.

//

Updates sind Korrekturen und Verbesserungen einer Software. Jede Software ist verbesserungswürdig. Die eine mehr, die andere weniger. Manchmal handelt es sich um Fehler, im Fachjargon Bugs genannt, die nur unter bestimmten Bedingungen auftreten und ansonsten keine Rolle spielen. Manchmal sind es auch einfach nur Verbesserungen der Funktionen einer Software. Darauf kann man vielleicht verzichten. So weit ist es nachvollziehbar, dass ein Benutzer nicht sofort aktiv wird, wenn er erfährt, dass es ein Update für seine Software gibt.

//

Nicht selten jedoch werden mit Updates auch Sicherheitslücken geschlossen. Und hier wird es essenziell! Ständig werden Schwachstellen entdeckt und oft auch recht schnell gepatcht – ein anderer Ausdruck für das Einspielen eines Updates, das daher auch als Patch bezeichnet wird. Nur nützt der beste Patch nichts, wenn er nicht zur Anwendung kommt.

//

Bitte führe dir vor Augen, dass die meisten erfolgreichen Angriffe nicht über so genannte Zero-Day-Exploits geschehen. Das bezeichnet das Ausnutzen von Schwachstellen, die noch nicht bekannt sind oder für die der Hersteller einer Software noch keinen Patch zur Verfügung gestellt hat. Stattdessen erfolgen die meisten Angriffe auf bekannte Schwachstellen erfolgen, und zwar auf Systeme, die nicht auf dem aktuellen Stand sind, bei denen also Updates fehlen.

//

Die wichtigste Aufgabe, die du in Bezug auf die Pflege deiner IT-Systeme hast, ist, sie auf dem aktuellen Softwarestand zu halten. Das erfordert ein gutes Patch-Management. Während ein normaler User sicher problemlos fast alle Updates einspielen kann, müssen die Patches in einem Unternehmen oft erst gut getestet werden, um Probleme in der eigenen Umgebung zu erkennen. Denn das ist die Kehrseite der Medaille: Updates können auch Probleme erzeugen, wo vorher keine waren. Das ist zwar selten, kommt aber vor.

//

Aber auch wenn es heißt: Never touch a running system! solltest du deine Software möglichst auf dem aktuellen Stand halten, um bekannte Schwachstellen auszumerzen. Das gilt insbesondere für Programme, die direkt mit dem Internet oder im Netzwerk interagieren, also Browser, E-Mail-Clients, Serverdienste, etc.

>>> 06. Keinen Viren- und Malware-Schutz implementieren

Glücklicherweise ist mittlerweile auf jedem Windows-System mit dem Windows Defender eine sehr brauchbare Virenschutzlösung implementiert. Sie erkennt auch andere Malware, wie z.B. Trojaner oder potentielle Schadsoftware. Generell ist es wichtig, sich gegen alle Arten von Malware zu schützen. Daher sollte vertrauenswürdige Schutzsoftware installiert werden, die auch gegen andere Angriffe aus dem Internet schützt.

//

Die meisten externen Virenschutzprogramme können mehr als der Windows Defender. Sie können neben dem Defender installiert werden und bilden so eine zweite Sicherheitsschicht. Neben dem Schutz vor klassischer Malware bringen sie oft auch zusätzliche Features wie VPN-Dienste, Passwort-Manager, Cloud-Backup, Kindersicherung, Webcam-Schutz, Anti-Tracking, Anti-Phishing, etc.

//

Mit einer guten Internet-Security-Suite lässt sich der Schutz des eigenen Computers erheblich verbessern. Welches Produkt für dich am besten passt, kannst du durch die zahlreichen Vergleichstests im Internet schnell selbst herausfinden.

>>> 07. Keine Backups anfertigen

Niemand denkt groß an Backups, bis sie gebraucht werden. Sei es ein gestohlenes Gerät, ein infiziertes System oder eine Fehlfunktion einer wichtigen Komponente. Plötzlich wird das Backup zur wichtigsten Sache auf der Welt.

//

Ein Backup ist die Lebensversicherung für deine Daten! Sollte eine Festplatte ausfallen, dein Laptop, Tablet oder Smartphone gestohlen werden oder eine Ransomware deine Daten verschlüsseln, kannst du kalt lächelnd dein System neu aufsetzen und die Daten aus einem Backup wiederherstellen.

//

Eine gute Backup-Strategie beinhaltet regelmäßige Backups der wichtigen Daten. Nach Möglichkeit sollten diese Daten nicht auf demselben Gerät gespeichert werden, von dem sie stammen. Stattdessen bieten sich externe Speicher, wie NAS, SAN oder Cloud-Speicherlösungen an. Wer seine Daten außerhalb seines Einflussbereichs speichert, also z.B. in der Cloud, sollte die Backups verschlüsseln. Auch wenn wir unserem Cloud-Provider vertrauen, können wir nicht wissen, wer auf die dort gespeicherten Daten Zugriff hat.

>>> 08. Den Bildschirm nicht sperren

Egal ob Smartphone, Tablet, Laptop oder Arbeitsplatz-PC: Jedes Gerät bietet die Möglichkeit, den Bildschirm zu sperren. Viele lassen diesen wichtigen Schutzmechanismus jedoch außen vor, weil es unbequem ist, sich jedes Mal authentifizieren zu müssen, wenn man wieder mit dem Gerät arbeiten möchte.

//

Aber der Sicherheitsgewinn ist diese kleine Mühe wert! Ansonsten kann jeder auf dein Gerät zugreifen und private Nachrichten und E-Mails lesen, wenn du das betreffende Gerät gerade nicht im Blickfeld hast. Wenn ein Smartphone gestohlen wurde oder verloren gegangen ist, hat der "Finder" unbeschränkten Zugriff auf deine Daten, also Bilder, Videos, E-Mails, etc.

//

Also: Falls noch nicht gesehen, richte auf allen deinen Geräten eine Bildschirmsperre ein und sorge dafür, dass sich jeder Benutzer, der das System nutzen möchte, authentifizieren muss. Dabei sind Passwörter oder PINs weniger sicher als biometrische Methoden, wie z.B. Gesichtserkennung.

//

>>> 09. Davon ausgehen, dass dein System automatisch sicher ist

Windows und Android sind mit Abstand die größten Ziele von Angriffen aller Art. Doch auch Linux und iOS sind Betriebssysteme, die angreifbar sind. Nur, weil es wesentlich weniger Angriffe auf diese Systeme gibt, sind sie nicht automatisch sicherer.

//

Stattdessen solltest du sicher stellen, dass alle Einstellungen deines Systems – egal ob Smartphone, Tablet, PC oder Server – auf Sicherheit optimiert sind. Das Stichwort hier lautet: Hardening. Ein System zu "härten" bedeutet, dass es möglichst wenig Angriffsfläche bietet. Das geht durch Reduzieren von Diensten und Anwendungen auf das benötigte Maß und Konfigurieren aller Einstellungen auf möglichst sichere Optionen. Grundsätzlich gilt: Alles, was nicht benötigt wird, sollte deaktiviert oder deinstalliert werden.

//

>>> 10. Auf unbekannte Links aus unsicheren Quellen klicken

Es ist fast schon unheimlich, wie einfach es ist, intelligente Menschen dazu zu bringen, auf bestimmte Links zu klicken, die dann auf manipulierte Webseiten führen oder direkt eine Malware-Datei herunterladen. Diese Links können direkt in Webseiten integriert sein (z.B. über unauffällige Werbebanner) oder aber auch via E-Mail ins Postfach flattern.

//

Jeder von uns kennt Phishing-Mails. Aber wer kann von sich behaupten, dass er noch nie auf einen dubiosen Link geklickt hätte? Manchmal ist das dann schon alles, was die Angreifer brauchen: Der Link öffnet eine manipulierte Webseite und via Drive-By-Download wird Malware auf dem System installiert.

//

Aber auch die üblichen Phishing-Mails sind mittlerweile teilweise so täuschend echt gemacht, dass man schon genau hinschauen muss, um Fehler und Ungereimtheiten zu finden. Wichtig ist: Augen aufhalten und genau schauen, was hinter einem Link steckt. Links aus unsicheren Quellen solltest du besser nicht anklicken, außer, du hast ein Sandboxing-System und möchtest sehen, was hinter den Kulissen passiert.

>>> 11. Herunterladen von Anhängen ohne Prüfung

Eng verwandt mit dem vorigen Punkt ist das Herunterladen von Anhängen aus E-Mails. Unternehmen erhalten z.B. regelmäßig gefakte Initiativbewerbungen mit professionell geschriebenen Anschreiben von scheinbar sehr qualifizierten Mitarbeitern und – natürlich – einem CV (Lebenslauf) im Anhang als PDF. Einmal draufgeklickt, wird eine Schwachstelle im PDF-Reader ausgenutzt und Malware auf das System gebracht.

//

Ein unbedachter Klick und schon ist alles vorbei. Die Ransomware aktiviert sich nach einiger Zeit und verschlüsselt die Daten auf der Festplatte – oder etwas anderes, in der Regel sehr unschönes passiert. Egal: In jedem Fall sollte Malware keine Chance erhalten, sich auf deinem System zu etablieren. Also: Lade Anhänge nur herunter, wenn du sie selbst angefordert und die Quelle geprüft hast. Achtung: Bei ausgefeilten Phishing-Mails kann der Text sehr individuell auf das Opfer zugeschnitten sein. Man spricht hier von Spear Phishing. Dabei werden täuschend echt scheinende Mails von scheinbar bekannten Absendern mit persönlicher Ansprache des Opfers verschickt. Hier ist es teilweise sehr schwer den Fake zu erkennen. Bleib also immer wachsam und skeptisch.

>>> 12. Herunterladen von dubiosen Dateien von unseriösen Webseiten

Ergänzend zu den vorigen beiden Punkten müssen wir natürlich auch noch eine ganz schlechte Angewohnheit vieler Internet-User ansprechen: Das Herunterladen von dubiosen Dateien von unseriösen Webseiten. Klar, es ist verlockend, den neuesten Kinofilm oder das neueste Game gecrackt herunterzuladen und ohne etwas dafür bezahlen zu wollen. Auch die neueste Version einer beliebten Software wird häufig auf solchen Seiten angeboten – natürlich gecrackt.

//

Aber das ist auch der beste Weg, sich Malware einzufangen. Sei also sehr vorsichtig bei derartigen Angeboten und lass am besten die Finger davon! Ist ohnehin nicht legal …

>>> 13. Ungeschütztes Notieren von Passwörtern im Klartext

Du hast bestimmt schon mal Filme gesehen, in denen ein Angreifer das Passwort seines Opfers knacken wollte. Er sitzt also nun vor dem Computer der Zielperson und was macht er zuerst? Er schaut unter die Tastatur und tastet den Monitor ab. Warum? Weil da nicht selten Klebezettel zu finden sind, auf denen das Passwort steht.

//

Man kann eigentlich gar nicht so dumm denken, wie manche Leute handeln. Diese Technik des „Passwort-Merkens“ist weit verbreitet! Es ist nichts dagegen einzuwenden, dass du deine Passwörter notierst – aber bitte in einem Passwort-Safe, der durch ein Master-Passwort und am besten Zwei-Faktor-Authentifizierung geschützt ist und der Inhalt natürlich verschlüsselt abgelegt wird. Ansonsten solltest du dir zumindest das Master-Passwort merken und nicht irgendwo im Klartext auf dem Desktop in einer Textdatei speichern. Klingt das für dich selbstverständlich? Gut! Dann bist du vielen schon einen Schritt voraus!

//

Aber weißt du, was der häufigste Satz von Opfern ist: „Sonst passe ich eigentlich immer auf …“ Also bleib konsequent und erlaube dir keine Ausnahmen bei der Sicherung deine Passwörter.

>>> 14. Surfen auf HTTP-Seiten

Klingt das komisch für dich? Gemeint sind hier Seiten, die nicht durch HTTPS geschützt sind, also Webseiten, mit denen du im Klartext interagierst. Hier kann die Kommunikation abgehört werden und jeder kann mitlesen. Du solltest also immer darauf achten, dass ein geschlossenes Schloss-Symbol in der Browser-Adresszeile vorhanden ist.

//

Es gibt noch vereinzelte Webpräsenzen, die nicht durch HTTPS geschützt sind. Solange es sich um simple, vielleicht statische Seiten handelt, ist das auch kein großes Problem. Solltest du aber irgendwelche persönlichen oder sensiblen Daten übermitteln müssen, dann bitte auf keinen Fall via Klartext-HTTP, sondern immer SSL/TLS-geschützt via HTTPS.

//

Ein Weg, um trotzdem geschützt zu sein, ist die Verwendung eines VPN-Dienstleisters. Über das VPN sind deine Daten zumindest bis zum Gateway des Anbieters geschützt. Das ist zwar nicht perfekt, aber besser als nichts.

>>> 15. Online-Banking über öffentliche Hotspots

WLAN ist mittlerweile an vielen öffentlichen Plätzen verfügbar. Allerdings sind da auch viele andere Menschen und evtl. auch Hacker unterwegs, die die Verbindung deines mobilen Gerätes zum Hotspot-Access-Point knacken könnten und damit in der Lage wären, all deine Daten mitzulesen und vielleicht sogar zu manipulieren.

//

Mit Evil Twins werden Fake-Access-Points bereitgestellt, die unbedarfte WLAN-User anlocken, so dass die gesamte Kommunikation über den AP des Angreifers geht. Generell kannst du bei öffentlichen WLAN-Hotspots nicht davon ausgehen, dass die Netze gut genug geschützt sind. Also vermeide es, in solchen öffentlichen Umgebungen sensible Daten auszutauschen. In erster Linie betrifft das das Online-Banking, aber natürlich nicht ausschließlich.

//

Um hier eine bessere Sicherheit zu erhalten, bietet sich erneut der Einsatz von VPNs an. Sie bieten eine durchgängig gesicherte Verbindung zwischen deinem mobilen System und dem VPN-Dienstleister. Damit wird unsere „erste Meile“ der Anbindung an das Internet gut geschützt.

>>> 16. Mit allen Lizenzbedingungen einverstanden sein

Sei mal ehrlich: Liest du dir die ellenlangen Lizenzbedingungen und allgemeinen Geschäftsbedingungen einer heruntergeladenen Software durch, bevor du sie installierst? Nein? Dann bist du in der guten Gesellschaft der allermeisten von uns. Aber vielleicht solltest du damit anfangen. Es ist nämlich erstaunlich, wie dreist manche Anbieter von Software sind.

//

Wenn du nicht aufpasst, erlaubst du ihnen das Ausspähen deiner Daten und die Weitergabe sensibler Informationen. Aber das ist noch nicht alles: Unter Umständen gibst du sogar dein Einverständnis, dass die Software Malware installiert, dich belauscht und vieles mehr. Also solltest du es dir zur Angewohnheit machen, die Lizenzbedingungen zu lesen und ggf. abzuwägen, ob der Vorteil der Nutzung der betreffenden Software die Nachteile der Lizenzvereinbarung aufwiegt.

//

>>> 17. Zu viele Browsererweiterungen nutzen

Für viele gängige Browser gibt es zahllose Addons, also Erweiterungen. Oft sind wir versucht, diverse Addons zu installieren, weil sie Zusatznutzen versprechen. Aber: Brauchen wir die wirklich alle? Tatsächlich überwiegen nämlich oft die Nachteile, wenn man zu viele Browser-Extensions nutzt. Wie beim vorigen Thema über die Software-Lizenzbedingungen ist es auch bei den Browsererweiterungen so, dass es viele schwarze Schafe gibt. Da werden dann ganz merkwürdige Spyware-Funktionen eingebaut und die Erweiterung sammelt diverse Daten über dich. Oder noch schlimmer: Es wird Malware installiert, die z.B. Man-in-the-Middle-Angriffe ermöglicht – in diesem Zusammenhang auch als Man-in-the-Browser bezeichnet.

//

Also: Sei vorsichtig und wähle deine Browsererweiterungen weise! Nicht alles was angeboten wird, muss man auch unbedingt haben und manchmal ist weniger mehr.

//

>>> 18. Auf Virenwarnungs-Popups klicken

Es kommt immer wieder vor, dass auf einer unseriösen Webseite plötzlich ein Popup auftaucht, dass dir vermeldet, diverse schlimme Viren und andere Malware entdeckt zu haben. Glücklicherweise ist die Lösung auch gleich mit angegeben: Einfach auf den Download-Button klicken und die heruntergeladene Software bereinigt dein ach so verseuchtes System. Nun, spätestens nach der Installation dieser Fake-Antiviren-Software ist dein System tatsächlich mit allerlei Malware verseucht!

//

Mit anderen Worten: Lass dir keine Angst machen! Kein seriöser Anbieter von Antimalware-Software wird dein System ungefragt scannen und dich dann zur Installation von Software auffordern. Eine andere Situation liegt natürlich vor, wenn dein installiertes AV-Programm Alarm schlägt! In diesem Fall solltest du das auf keinen Fall ignorieren und genau schauen, was dort gefunden wurde.

//

>>> 19. Daten unverschlüsselt in die Cloud hochladen

Cloud-Speicher ist mittlerweile fester Bestandteil in vielen Umgebungen. Festspeicher, den man nicht mit sich herumschleppen muss und der überall verfügbar ist – topp! Leider hat das auch seine Schattenseiten: Du hast nämlich nicht mehr exklusiven Zugriff auf deine Daten. Auch wenn seriöse Cloud-Speicher-Provider sicher viel für den Schutz der Daten ihrer Kunden tun werden, kannst du nicht wissen, was dort hinter den Kulissen passiert. Vielleicht schaut sich ein Mitarbeiter des Cloud-Providers mit genügend Privilegien deine privaten Daten an. Vielleicht werden die Daten Geheimdiensten oder anderen Institutionen zur Verfügung gestellt. Vielleicht ist die Vertraulichkeit auch durch eine Drittpartei gefährdet.

//

Da du keine Kontrolle über den Zugriff auf deine Daten in der Cloud hast, solltest du zumindest die sensiblen Daten verschlüsselt speichern. Dazu gibt es zahlreiche Tools, wie z.B. VeraCrypt, etc. Mit einer guten Verschlüsselung mit Hilfe eines starken Passwortes machst du es neugierigen Zeitgenossen schwierig, an deine Daten zu gelangen.

//

>>> 20. Sich zu sehr auf die technische Sicherheit verlassen

Firewalls, Antiviren-Software, Browser-Schutz, VPN-Software, etc. sind alles wichtige Elemente, um deine Computersysteme so sicher wie möglich zu machen. Dennoch solltest du ihn nicht blind vertrauen und dabei den Kopf ausschalten. Es gibt Angriffsformen, die auch die beste Schutz-Software nicht abfangen können. Zero-Day-Exploits sind beispielsweise Angriffe auf Schwachstellen, die noch nicht gefixt wurden.

Eine andere Art von Schwachstelle kann ebenfalls kaum durch Sicherheitseinstellungen oder Security-Software geschützt werden. Es handelt sich um die größte Schwachstelle in Computersystemen, nämlich dem User. Unser Computersystem ist immer nur so gut, wie wir es bedienen.

Eine Angriffstechnik, die genau auf die Schwachstelle „Mensch“ abzielt, ist das Social Engineering. Dabei werden psychologische Mechanismen ausgenutzt, die das Opfer dazu bringen, z.B. seine Kreditkartendaten oder Zugangsdaten preiszugeben. Phishing-Mails sind eine allseits bekannte Variante des Social Engineerings. Dazu gehört aber auch das sogenannte Vishing, ein Kunstwort aus Voice und Phishing, bei dem der Angreifer sein Opfer anruft und dazu bringt, sensible Daten offenzulegen.

Also: Sei dir nicht zu sicher und vertraue in erster Linie auf deinen gesunden Menschenverstand, wenn du im Internet unterwegs bist und mit deinen Computersystemen arbeitest – gleich welcher Art. Der beste Schutz vor einem erfolgreichen Angriff ist die eigene Skepsis und das bewusste, vorsichtige Handeln.

>>> Werde auch Du ein Ethical Hacker und Penetration Tester

Klicke hier!

Hacking Akademie