IN DIESEM KAPITEL

Typische Fehleinschätzungen der Nutzerinnen

Fehler der Administratoren

Fake News der IT-Sicherheit

Kapitel 1
Irrtümer und häufige Fehler

Um die IT-Sicherheit ranken sich viele Mythen. Die Nutzerinnen der IT haben teilweise seltsame Vorstellungen, wie Informationstechnik (IT) und IT-Sicherheit funktioniert.

Es gibt Nutzerinnen, die unterschätzen das Risiko. Äußerungen im Bekannten- und Kollegenkreis, die Sie alle schon gehört haben, sind »Ich kann mit meinem Windows 7 ins Internet gehen, wenn ich immer nur kurz im Internet bin. Bei weniger als zehn Minuten kann nichts passieren.« »Solange ich nicht auf zwielichtigen Seiten surfe, kann ich mir keinen Virus einfangen.« »Eine E-Mail, in der sich ein Virus verbirgt, erkenne ich sofort.« »Ein Passwort zum Anmelden am Rechner benötige ich nur im Büro.« »Ich habe nichts zu verbergen.« »Wer interessiert sich schon für meine Daten?«

Andere Nutzerinnen überschätzen das Risiko. »Ich mache kein Online-Banking. Das ist viel zu gefährlich.« »Ich will kein Smartphone, da werde ich nur ausspioniert.« »Die Geheimdienste können mich dann komplett verfolgen.«

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt auf der Webseite für Verbraucherinnen und Verbraucher (`https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Sicherheitsirrtuemer/sicherheitsirrtuemer_node.html`) gängige IT-Sicherheitsirrtümer zusammen, die wir zu vier mal fünf häufigen Irrtümern ergänzt haben und im Folgenden in vier Kategorien vorstellen.

Internet-Sicherheit

Sie surfen wahrscheinlich auch regelmäßig im Internet und wollen sich dabei schützen. Einige Nutzerinnen haben seltsame Vorstellungen, wie man sich schützt und was die Schutzmechanismen leisten können.

✔ Eine Firewall schützt vor allen Angriffen aus dem Internet.

Eine Firewall schützt unsere Rechner erst einmal überhaupt nicht. Erst das Regelwerk der Firewall erzeugt den Schutz. Je nach Firewall gibt es im Lieferumfang unter Umständen ein Default-Regelwerk. Gerade im Privatbereich ist dieses jedoch nicht auf maximalen Schutz ausgelegt, sondern eher auf Vermeidung von Support-Anrufen. Eine Firewall als virtueller Pförtner lässt immer einigen Datenverkehr passieren, zum Beispiel E-Mail-Empfang und Web-Surfen, und damit kann auch Schadsoftware durch die Firewall gelangen. Für einen IT-Laien ist eine sichere Konfiguration einer Firewall nicht leistbar, da sie ein gutes technisches Verständnis der Internet-Protokolle voraussetzt.

✔ Wenn das Virenschutzprogramm aktuell ist, muss ich Updates für andere Software nicht sofort installieren. Ein kostenloses Virenschutzprogramm ist völlig ausreichend.

Virenschutzprogramme erkennen nicht alle Schadsoftware. Gerade aktuelle, neue Viren werden nicht sofort erkannt. Deswegen müssen wir trotz Virenscanner Softwareupdates immer unverzüglich einspielen. Windows 7 ist mittlerweile auch mit einem aktuellen Virenscanner unsicher. Kostenlose Virenschutzprogramme haben häufig eine geringere Funktionalität als die kostenpflichtigen Versionen und eine geringere Updatefrequenz, denn der Hersteller lebt vom Verkauf der Software. Die in der freien Version fehlende Funktionalität ist aber der innovative Teil des Virenscanners, den Sie gerne zum Schutz Ihres Rechners nutzen würden. In Unternehmen ist der Einsatz kostenloser Virenschutzprogramme aus lizenzrechtlichen Gründen nicht möglich, da die kostenlosen Varianten überwiegend nur für einen nicht-kommerziellen Einsatz lizenziert werden.

✔ Ein einziges langes und komplexes Passwort reicht für alle meine Internet-Dienste vollkommen aus.

Es ist keine gute Idee, wenn wir für alle Dienste, die wir nutzen, immer dasselbe Passwort verwenden. Bei vielen Diensten wird als Nutzername eine E-Mail-Adresse verwendet. Werden der Nutzername und das zugehörige Passwort bei einem Dienst von Kriminellen gestohlen, ist es dann auch bei allen anderen Diensten kompromittiert, denn da funktioniert in diesem Fall dieselbe Kombination aus E-Mail-Adresse und Passwort! Und wenn Sie dann auch noch dasselbe Passwort bei Ihrem E-Mail-Anbieter nutzen, hat der Angreifer auch Zugriff auf all Ihre E-Mails. Anbieter wie »';– have i been pwnded« (`https://haveibeenpwned.com/`) zeigen, wie oft und in welchem Umfang dies geschieht. Nur wenn Sie für jeden (!) Dienst ein eigenes Passwort verwenden, können Sie im Falle des Falles den Schaden auf den Anbieter des kompromittierten Dienstes begrenzen.

✔ Ich surfe nur auf seriösen Webseiten, darum kann mir nichts passieren.

Auch das Webangebot eines vertrauenswürdigen Anbieters kann gehackt sein – dann wird über diese scheinbar ganz seriöse Webseite Schadsoftware verbreitet. Viele Anbieter finanzieren ihre Webangebote über Werbung. Die Werbeanzeigen werden dabei direkt von den Werbeanbietern geladen. Und auch diese können gehackt werden und mit der Werbung Schadsoftware verteilen. Auch Browser können Sicherheitslücken

haben, über welche sich Ihr Rechner hacken lässt. Letztendlich gibt es keine Garantie, dass eine Webseite dauerhaft frei von Schadsoftware bleibt, egal wie gut ihr Ruf ist.

✔ Die Nutzung eines Virtual Private Networks (VPN) erlaubt eine anonyme und sichere Internetnutzung.

Wenn Sie das VPN eines kommerziellen Anbieters verwenden, nutzen Sie das Internet mit einer IP-Adresse des Anbieters. Ihr Internet-Provider kann nicht mehr analysieren, welche Seiten Sie im Internet aufrufen. Dafür sieht jedoch der VPN-Anbieter alles, was Sie im Internet über das VPN so anstellen. Da dieser Dienst bezahlt wird, ist dem Anbieter in der Regel auch Ihre echte Identität bekannt. Damit erfolgt keine anonyme, sondern nur eine pseudonyme Nutzung des Internets. Es hängt vom Anbieter ab, ob er Ihre Identität auf Nachfrage von Dritten (zum Beispiel von Sicherheitsbehörden) offenlegt. Ein VPN stellt die Vertraulichkeit der Kommunikation in unsicheren Netzen, beispielsweise in einem öffentlichen WLAN, sicher. Es ist kein Anonymisierungsdienst.

Ein VPN verschlüsselt ausschließlich den Datenverkehr zwischen Ihrem PC und dem VPN-Server und schützt damit vor dem Abhören Ihrer Kommunikation in nicht-vertrauenswürdigen Netzen. Ein VPN schützt Sie nicht vor dem Download von Schadsoftware und nur eingeschränkt vor unberechtigten Zugriffen auf Ihren PC. In einem öffentlichen WLAN kann je nach Konfiguration Schutz vor Zugriffen durch andere gleichzeitige Nutzerinnen des WLANs möglich sein.

Mobile und Cloud-Sicherheit

Einige Nutzerinnen haben recht naive Vorstellungen, was ein Cloud-Dienstleister leisten kann, insbesondere, wenn der Kunde die Dienstleistung kostenlos in Anspruch nimmt. Auch beim sicheren Umgang mit Smartphones gibt es bei manchen Nutzerinnen einige Unklarheiten.

✔ Meine in der Cloud gespeicherten Daten sind vor einem Fremdzugriff sicher geschützt.

Schützen Sie auch den Zugriff auf Ihre Daten in der Cloud nur durch ein Passwort? Wird Ihr Passwort einem Dritten bekannt, so ist für den Dritten der Zugriff auf Ihre Daten möglich. Außerdem haben die Administratoren und möglicherweise andere Beschäftigte des Cloud-Anbieters Zugriff auf Ihre Daten. Dieser Zugriff ist den Beschäftigten zwar untersagt, aber er ist in der Regel nicht technisch unterbunden.

✔ Wenn ich meine Daten in der Cloud speichere, benötige ich kein Backup.

Gerade kostenloser Speicherplatz in der Cloud ist nicht immer mit umfangreichen automatischen Backups versehen. Schließlich kostet ein Backup Geld, was mit dem kostenlosen Angebot nicht verdient wird.

Auch Cloud-Anbieter haben schon Daten verloren oder mussten sogar danach ihr Geschäft aufgegeben. Und dann sind Ihre Daten, die Sie bei dem Cloud-Anbieter gespeichert haben, unter Umständen nicht mehr zugreifbar. Zwei Kopien der Daten,

auf Ihrem Rechner und in der Cloud sind zu wenig für ein verlässliches Backup. Ein Großbrand in einem Straßburger Rechenzentrum eines großen französischen Cloud-Anbieters im Frühjahr 2021 führte vielen Kunden vor Augen, dass die Daten, die in der Cloud gespeichert sind, verloren gehen können. Diese Erfahrung wollen Sie bestimmt nicht machen.

Ein Backup basiert auf der Idee, das Sie mehrere Kopien einer Datei so speichern, dass eine Beschädigung oder Zerstörung einer Datei die Kopie dieser Datei in der Cloud nicht betrifft. Da die gängigen Cloud-Speicher die lokale Kopie der Datei auf Ihrem PC mit der Cloud-Kopie automatisch synchronisieren, führt die Beschädigung Ihrer lokalen Kopie automatisch auch zur Beschädigung der Cloud-Kopie, wenn der Cloud-Dienst keine Versionierung der Dateien unterstützt.

✔ Das Surfen in öffentlichen WLANs kostet mich kein Geld und ist zusätzlich auch noch sicher.

Öffentliche WLANs sind in der Regel unverschlüsselt. Auch wenn nach § 202b StGB das »Abfangen von Daten (…) aus einer nichtöffentlichen Datenübermittlung« verboten ist und bestraft wird, ist dies wegen der fehlenden Verschlüsselung technisch problemlos möglich. Der Rechner, mit dem Sie in dem öffentlichen WLAN eingebucht sind, kann auch recht leicht angegriffen werden, da Ihr Rechner im WLAN von den Rechnern der anderen Nutzerinnen in dem WLAN einfach zu erreichen ist. Die meisten WLAN-Anbieter verhindern dies nicht. Der Schutz einer dedizierten Firewall, wie Sie ihn an Ihrem Arbeitsplatz im Unternehmens-LAN oder in Ihrem Heimnetz haben, fehlt. Sie sind allein auf die Schutzwirkung Ihrer Desktop-Firewall angewiesen. Haben Sie die dafür richtig konfiguriert? Wenn nicht, ist Ihr Rechner im WLAN allen anderen Rechnern im gleichen WLAN weitgehend schutzlos ausgeliefert.

✔ Wenn ich mir ein neues Smartphone zulege, habe ich immer auch ein sicheres Gerät.

Nicht jedes aktuell verkaufte Smartphone wird mit der aktuellsten Version des Betriebssystems ausgeliefert. Die Sicherheit Ihres neuen Smartphones hängt aber wesentlich von der Aktualität der Software (Betriebssystem und Anwendungen) ab. Gerade bei günstigen Geräten ist es häufig nicht möglich, die Software zu aktualisieren, da der Hersteller nie ein Update ausliefert. Der Hersteller hat hier zulasten des Kunden am falschen Ende gespart.

✔ Ich habe alle automatischen Updates und Aktualisierungen des Betriebssystems und meiner Apps aktiviert, daher brauche ich mich um keine Schwachstellen und Sicherheitslücken zu kümmern.

Zum einen müssen Sie regelmäßig kontrollieren, ob das Einspielen der Updates auch funktioniert hat, zum anderen sind alle Geräte irgendwann End-of-Life (das heißt, sie werden vom Hersteller nicht mehr mit Aktualisierungen unterstützt) und werden dann eben nicht mehr aktualisiert. Vom Bekanntwerden einer Sicherheitslücke bis zur Verfügbarkeit des Updates, das die Sicherheitslücke behebt, für Ihr Gerät kann es im Extremfall ein paar Wochen dauern. So lange müssen Sie sich mit einem provisorischen Workaround schützen, der in der Regel manuell einzurichten ist.

Endgerätesicherheit

Die Rechner der Nutzerinnen werden mittlerweile flächendeckend von Kriminellen angegriffen. Dadurch wird ein Grundrauschen erzeugt, in dem zielgerichtete Angriffe kaum noch auffallen. Manche Einschätzung der damit verbundenen Gefahren ist deutlich durch Unkenntnis geprägt.

- ✔ Wenn ich mir doch mal einen Virus oder eine andere Schadsoftware auf dem Computer einfange, bemerke ich dies sofort.

  Die Erfahrung in Unternehmen zeigt, dass ein Befall mit einer Schadsoftware nicht sofort bemerkt wird. Destruktive Schadsoftware, wie zum Beispiel ein Verschlüsselungstrojaner, wird dabei noch am schnellsten festgestellt. Bei ausgefeilter Spionagesoftware dauert es dagegen im Mittel etliche Monate, bis die Infektion im Unternehmen bemerkt wird – manchmal nur durch Zufall. Und auch dann wird der Befall häufig erst nach Hinweisen Dritter gefunden. Wenn aber die IT-Profis die Infektion durch eine Schadsoftware nicht sofort bemerken, wie sollen IT-Laien oder normale Verbraucher das dann schaffen?

- ✔ Ich habe nichts zu verbergen und meine Daten sind völlig uninteressant, also bin ich doch kein lohnendes Ziel für Angreifer. Deshalb benötige ich auch keinen Schutz.

  Sie haben bestimmt, wie jeder andere auch, auf Ihrem Rechner wichtige vertrauliche Daten. Die Zugangsdaten zu Ihrem Bankkonto, Ihre Verträge, Ihre Steuererklärungen, Kommunikation mit Ihren Ärzten und so weiter. Das sind Daten, die Sie sicher ungern in der Öffentlichkeit sehen würden. Und damit bieten diese Daten zumindest die Basis für eine Erpressung, sei es durch eine Verschlüsselung Ihrer Daten (Ransomware) oder durch die Drohung, Ihre Daten zu veröffentlichen.

- ✔ Ich habe alle Zugriffsmöglichkeiten auf meinen Computer umkonfiguriert, die findet niemand mehr.

  Das Prinzip heißt »Security by Obscurity« und ist leider überhaupt nicht sicher. Warum legen Sie Ihren Haustürschlüssel nicht unter die Fußmatte? Weil jemand den Schlüssel dort finden könnte, ist die typische Antwort. Niemand kommt auch auf die Idee, dass Sie Ihre Girocard-PIN als Telefonnummer im Adressbuch stehen haben, oder? Egal wie Sie Dienste umkonfigurieren, also Ihren Webserver, den Remotedesktop-Zugriff und andere Dienste, wenn Sie die Dienste aus dem Internet erreichbar machen, findet ein Angreifer die Dienste auch. Insbesondere, wenn Sie für die Umkonfiguration eine gängige Anleitung aus dem Internet benutzt haben, können Sie davon ausgehen, dass Angreifer diese mindestens so gut kennen wie Sie. Wenn Sie den Dienst aber wirklich gut abgesichert haben, dann müssen Sie ihn nicht verstecken.

- ✔ Wenn ich alle Daten von meinem Gerät lösche und dann auich noch den Papierkorb leere, dann kann niemand mehr auf meine Daten zugreifen.

  Aus Geschwindigkeitsgründen wird, wenn Sie eine Datei löschen, oft nur der Verzeichniseintrag der Datei entfernt, woraufhin die Datei Ihnen nicht mehr angezeigt

wird. Der Inhalt der Datei wird beim Löschen dagegen nicht verändert. Diese Dateireste auf dem Datenträger werden erst im Laufe der Zeit, wenn der Speicherplatz für andere Dateien benötigt wird, überschrieben. Mit einfachen Softwarewerkzeugen (sogenannte Unerase-Programme) lässt sich die Datei, solange sie nicht überschrieben wurde, wiederherstellen. Daten auf einer klassischen Festplatte müssen Sie komplett mit anderen Daten überschreiben, Daten auf einem Solid State Drive (SSD) müssen Sie mit speziellen Befehlen löschen oder Sie müssen den Datenträger physisch zerstören, damit die Daten wirklich gelöscht sind.

✔ Never touch a running system.

Wenn Ihr sorgfältig konfiguriertes IT-System einmal stabil läuft, möchten Sie es möglichst nicht mehr ändern. Das Risiko, dass es nach der Änderung nicht mehr läuft, erscheint Ihnen zu hoch. Dabei ist es zwingend erforderlich, dass Sie sicherheitsrelevante Updates installieren. Gegebenenfalls überlegen Sie auf Basis der Updatebeschreibung und der Beschreibung der Sicherheitslücken sorgfältig, ob die zugrundeliegende Bedrohung bei Ihrem System gegeben ist. Wenn die Sicherheitslücke zum Beispiel den Bluetooth-Funk betrifft, Sie aber Bluetooth deaktiviert haben, können Sie das Update überspringen. Sie dürfen dann aber, wenn Sie Bluetooth doch aktivieren, nicht vergessen, das Update eben doch zu installieren!

E-Mail-Sicherheit

Auf Grund des fehlenden technischen Verständnisses schätzen viele Nutzerinnen die Risiken bei der E-Mail-Nutzung völlig falsch ein.

✔ Wenn ich den Anhang einer E-Mail nicht öffne, sondern nur den Mailtext lese, kann mir nichts passieren.

Da E-Mail-Programme Ihnen ein Vorschaufenster zum Betrachten der E-Mail bieten und viele E-Mails, damit sie schöner aussehen, als HTML-Mails verschickt werden, können Sie auch durch das Anschauen einer E-Mail bereits eine Schadsoftware starten. Insbesondere Glückwunsch- und Weihnachtskarten und dergleichen sind da ein besonderes Risiko, da sie mit viel Aufwand (und entsprechend viel ausführbarem Code in der E-Mail) daherkommen.

✔ Auf eine Spam-Mail kann ich gefahrlos antworten, ich auch den Link zum Löschen aus dem Verteiler nutzen.

Durch die Antwort auf solch eine E-Mail oder einen Klick auf den Link darin unterstützen Sie den Spammer. Er erhält die Bestätigung, dass Ihre E-Mail-Adresse aktiv genutzt wird, und damit steigt der Wert Ihrer E-Mail-Adresse für ihn. Nur seriöse Verteilerlisten erlauben es Ihnen als Abonnenten der Mailing-Liste, sich auszutragen. Gerade das Anklicken eines Links in einer nicht-vertrauenswürdigen E-Mail stellt immer ein hohes Risiko für Sie dar, da Sie nie wissen, ob dadurch nicht ein schädliches Programm auf ihrem Endgerät gestartet wird.

- ✔ Eine E-Mail wurde immer von der Adresse versandt, die mir im Absender-Feld angezeigt wird.

  Die Ihnen von Ihrem Mail-Programm angezeigte E-Mail-Adresse des Absenders hat technisch nichts mit dem tatsächlichen Absender zu tun. Sie kann mehr oder weniger frei gewählt werden. Der tatsächliche Absender steht zwar häufig auch in der E-Mail (genauer im E-Mail-Header), dieser E-Mail-Header wird Ihnen aber von Ihrem Mail-Programm standardmäßig nicht angezeigt. Und auch wenn es etwas aufwendiger ist, lassen sich auch Einträge im E-Mail-Header manipulieren.

  Das gilt übrigens auch für das An-Feld in der E-Mail. Der tatsächliche Empfänger und der angezeigte Empfänger sind zwei verschiedene Adressen. Das kennen Sie von E-Mails, bei denen Sie die Mail per Blind Carbon Copy (BCC, so viel wie »unsichtbare Kopie«) erhalten. Sie bekommen die E-Mail, aber weder im An-Feld noch im cc-Feld steht ihre E-Mail-Adresse.

- ✔ Phishing-Mails erkenne ich auf den erstten Blick.

  Schlecht gemachte Phishing-E-Mails erkennen Sie leicht, wenn Sie wissen, woran Sie diese erkennen können. Wirklich gute Phishing-E-Mails sind jedoch auch für erfahrene IT-Sicherheitsexperten allein durch normales Öffnen und Betrachten sehr schwer zu erkennen. Zum Glück sind diese selten, da sie aufwendig zu erstellen sind. Für nicht so erfahrene Nutzerinnen sind allerdings auch durchschnittliche Phishing-E-Mails im beruflichen Alltagsstress nicht immer direkt zu erkennen.

- ✔ Eine E-Mail ist beim Transport vor unbefugten Zugriffen geschützt.

  Der Vergleich der Vertraulichkeit einer E-Mail mit einer Postkarte ist Ihnen sicher bekannt. Aktuell können Sie nur dann sicher sein, dass eine E-Mail »unterwegs« geschützt ist, wenn Sie sie mit einem geeigneten Verfahren (S/MIME oder OpenPGP) verschlüsseln. Häufig, aber leider nicht immer, wird der Transport einer E-Mail von Mail-Server zu Mail-Server durch eine solche Verschlüsselung geschützt. Ob eine solche Transportverschlüsselung genutzt wird, entscheiden aber die Betreiber der Mail-Server und nicht Sie als Absender oder Empfänger der E-Mail.

  Die Transportverschlüsselung schützt nur vor dem Abhören der Übertragung zwischen den Mail-Servern durch Dritte. Eine unverschlüsselte E-Mail ist für den Betreiber eines Mail-Servers grundsätzlich zugänglich. Der Zugriff ist rechtlich nur eng beschränkt zulässig, aber rein technisch eben durchaus möglich.

Sie haben jetzt schon einige Begriffe und Konzepte der IT-Sicherheit kennengelernt. Begriffe wie Backup, Cloud, LAN, Schadsoftware oder Verschlüsselung haben Sie im normalen IT-Leben wohl auch schon einmal gehört. Speziellere Begriffe wie S/MIME, OpenPGP oder Transportverschlüsselung sind dagegen vielleicht völlig neu für Sie. Beim weiteren Studium des Buches werden Sie diese Begriffe im Detail kennenlernen und die Konzepte dahinter verstehen.