Kapitel 12 – Geräte absichern

Das Thema Internetsicherheit lässt sich in vier Bereiche unterteilen: Schutz der Geräte und des Heimnetzwerks, Passwörter, Browser, Surfen in Wifi-Netzwerken.
Für jede dieser Kategorien werden wir uns ansehen, was alles getan werden sollte, um ein Mindestmaß an Sicherheit zu erreichen, bis das System und alle über das Web und das Netzwerk übertragenen Daten vollständig geschützt sind.

1) Sicherheit von Computer, Tablet oder Mobiltelefon

Ist ein Antivirenprogramm installiert? Aktualisiert sich das Antivirenprogramm automatisch jeden Tag?
Wenn Sie noch kein Antivirenprogramm installiert haben oder wenn Sie ein abgelaufenes Programm haben, das sich nicht mehr aktualisiert, sollten Sie etwas unternehmen. Deinstallieren Sie Ihr aktuelles Antivirenprogramm und laden Sie eines der empfohlenen kostenlosen Antivirenprogramme herunter. Um ein Antivirenprogramm so zu beurteilen, dass es für jeden verständlich ist, müssen wir mindestens 6 Parameter berücksichtigen, bevor wir eine Entscheidung treffen. Ein gutes Antivirenprogramm

- darf den PC nicht zu sehr verlangsamen und muss wenig RAM-Speicher benötigen
- muss Viren stoppen, bevor sie aktiv werden können (residentes aktives Scannen)
- darf nicht zu viele falsch-positive Ergebnisse liefern und Bedrohungen erkennen, wo keine sind
- darf für die On-Demand-Überprüfung oder die regelmäßige automatische Überprüfung nicht zu lange brauchen
- muss sich automatisch aktualisieren, damit es neue Infektionen sofort stoppen und den Zugriff auf wichtige Teile des Systems verhindern kann
- muss in der Lage sein, unentdeckte Malware (0-Day-Bedrohungen) zu blockieren und die Bedrohung nur durch das verdächtige Verhalten bestimmter Komponenten zu erkennen

Neben diesen Parametern, die alle sehr wichtig sind, wenn es um Antivirenprogramme geht, müssen wir auch die Benutzerfreundlichkeit, die Benutzeroberfläche, eventuelle Probleme mit der Benutzerfreundlichkeit und das Vorhandensein von Bugs, Fehlern und Inkompatibilitäten berücksichtigen.

- Ist eine Firewall installiert?

Wenn Sie Windows 7 (oder höher) haben und zu Hause über einen Router im Internet surfen, benötigen Sie kein Firewall-Programm. Falls Sie doch eine möchten, können Sie eine kostenlose Firewall herunterladen, um Ihr Netzwerk zu schützen und Eindringlinge abzuwehren.

- Ist Windows (oder Mac) auf dem neuesten Stand und wird es automatisch und regelmäßig aktualisiert?

Viele Menschen vernachlässigen oder vergessen, Windows mit den Patches zu aktualisieren, die Microsoft jede Woche verteilt. Bei diesen Updates handelt es sich immer um Sicherheits-Patches, die die neuesten Lücken schließen, die es böswilligen Benutzern ermöglichen, von außen in PCs einzudringen und die Kontrolle zu übernehmen.
Überprüfen Sie, ob der Windows Update-Dienst in der Systemsteuerung aktiv ist.
Auch Mac-Benutzer sollten Sicherheitsupdates nicht unterschätzen.

- Haben Sie einen Backup-Plan für Ihre Daten, Dokumente und Fotos erstellt?

Um sicherzustellen, dass die Dateien, die Sie auf Ihrem Computer erstellen und speichern, nicht verloren gehen, sollten Sie eine automatische Sicherung einplanen, damit Sie ein doppeltes Backup haben.

Wenn Sie nicht allzu viele Daten zu sichern haben, kann es viel einfacher und schneller sein, ein Online-Backup über Cloud-Speicherdienste wie Dropbox oder Skydrive zu erstellen.

- Halten Sie die auf Ihrem Computer installierten Programme auf dem neuesten Stand?

Wie bei Windows werden auch für Programme häufig Sicherheitsupdates herausgegeben.
Für diejenigen, die dies wünschen, gibt es Möglichkeiten, die auf Ihrem Computer installierten Programme und Software automatisch zu aktualisieren.

- Achten Sie beim Herunterladen von Programmen darauf, dass Sie bei der Installation nicht auch andere "empfohlene" Software mitinstallieren?

Leider kommen viele kostenlose Programme mit Sponsoren, so genannter "Crapware", in Form von unerwünschten Programmen, die sich automatisch installieren.

2) Browser-Sicherheit

Die Tatsache, dass Ihr Computer, Tablet oder Mobiltelefon gegen Viren und externe Eindringlinge geschützt ist, garantiert nicht, dass das Surfen immer sicher und privat ist. Vielen Menschen mag die Privatsphäre egal sein, aber Sicherheit ist dennoch von größter Bedeutung.
Welchen Browser Sie auch immer verwenden, er sollte auf die neueste Version aktualisiert sein und automatische Updates aktiviert haben. Zu den Browsern, die auf dem neuesten Stand sind und über automatische Updates verfügen, gehören sicherlich Chrome, Firefox, Opera und Microsoft Edge.

- Wenn Sie sich mit einem Passwort bei einer Website anmelden, überprüfen Sie dann immer, ob die Adresse mit https beginnt?

HTPPS ist das verschlüsselte Verbindungsprotokoll und unterscheidet sich vom normalen http dadurch, dass alle Daten, die mit https übertragen werden, verschlüsselt werden. Das bedeutet, dass das, was in https geschrieben wird, für niemanden lesbar ist, auch nicht für die Betreiber der betreffenden Website.

- Können Sie gefährliche Websites erkennen, bei denen Sie vorsichtig sein müssen, wo Sie klicken?

Wenn Sie immer noch nicht in der Lage sind, eine gute von einer schlechten Website mit bloßem Auge zu unterscheiden, und Sie immer paranoid oder schlecht gelaunt sind, wenn es um andere Websites als die beliebtesten geht, dann können Sie einige Erweiterungen wie WOT installieren, um das Klicken auf gefährliche Links und verdächtige Websites zu vermeiden.

- Loggen Sie sich immer aus, wenn Sie eine Website von einem Computer aus aufrufen, der nicht nur von Ihnen benutzt wird?

Denken Sie immer daran, sich von allen Konten abzumelden, die Sie auf einem öffentlichen oder gemeinsam mit anderen Personen, einschließlich Familienmitgliedern, genutzten Computer verwenden.

- Kennen Sie die Grundlagen von Online-Betrug und Betrug?

Zu wissen, was Phishing, Malware und andere Gefahren im Internet sind, ist wichtig, um sich vor ihnen zu schützen.

- Schützen Sie Ihren Browser vor Online-Tracking?

Wie bereits erklärt, bedeutet die Verhinderung des Online-Trackings durch Websites, dass Sie die Sammlung von Daten blockieren. Dies ist über bestimmte Erweiterungen möglich, die Sie in Ihrem Browser installieren können.
Die höchste Stufe des Schutzes und der Privatsphäre im Internet ist das anonyme Surfen. Völlig anonymes Surfen ist nicht für jeden sinnvoll und kann nicht in jeder Situation durchgeführt werden. Es kann nützlich sein, wenn Sie etwas Illegales tun (oder Gutes wie das Herunterladen von Torrents), wenn Sie Ihren geografischen Standort nicht preisgeben wollen oder wenn Sie Ihre IP-Adresse verschleiern wollen, um auf gesperrte Websites zuzugreifen.

Obwohl Sie auf verschiedene Weise anonym im Internet surfen können, ist die Online-Privatsphäre nur mit dem TOR-Browser gewährleistet.

3) Sicherheit der online verwendeten Passwörter

- Verwenden Sie komplexe Passwörter?

Einer der häufigsten Fehler, den Internetnutzer machen, ist die Verwendung von einfachen Passwörtern oder von Passwörtern, die sich auf Fakten oder Ereignisse aus ihrem persönlichen Leben beziehen. Sie sollten immer Passwörter wählen, die nicht entdeckt werden können, und vor allem ein starkes Passwort für alle Websites erstellen, ohne dass jemand die Chance hat, es zu erraten (verwenden Sie niemals Ihr Geburtsdatum, Ihre Lieblingsmannschaft oder den Namen Ihrer Frau oder Ihres Hundes).

- Verwenden Sie für jede Website ein anderes Kennwort?

Sie sollten niemals dieselbe E-Mail- und Passwortkombination für mehrere Dienste verwenden, denn wenn es einem Hacker gelingt, in dieses Konto einzudringen, kann er damit problemlos in jedes andere persönliche Konto eindringen.
Verwenden Sie ein Programm zur Erstellung und Verwaltung von Passwörtern für Webkonten (Passwort-Manager).
Wo es möglich ist (Dropbox, Google, Gmail und Facebook), können Sie eine Zwei-Faktor-Authentifizierung verwenden.
Für zusätzlichen Schutz sollten Sie die App-Berechtigungen auf Facebook und Twitter überprüfen.

4) Network security

- Ist Ihr WiFi-Netzwerk zu Hause mit einem WPA2-Schlüssel geschützt?

Wenn nicht, oder wenn Sie keine Ahnung haben, was WPA2 ist, sollten Sie wissen, dass WPA für Wi-Fi Protected Access steht und dass Wi-Fi Protected Access II (WPA2) und Wi-Fi Protected Access III (WPA3) drei Sicherheitsprotokolle und Zertifizierungsprogramme sind, die von der Wi-Fi Alliance zum Schutz drahtloser Computernetzwerke entwickelt wurden.

- Ist Ihnen bewusst, dass alles, was Sie tun, wenn Sie sich mit einem offenen Wi-Fi-Netzwerk verbinden, von außerhalb Ihres Computers sichtbar ist?

Das Einzige, was die Passwortsicherheit im Internet in einem öffentlichen Wi-Fi-Netzwerk schützt, ist das in der ersten Frage unter Punkt zwei erwähnte HTTPS-Protokoll.

- Haben Sie die gemeinsamen Ordner auf Ihrem Computer überprüft?

Wie sich gezeigt hat, ist es sehr einfach, sich in Computer zu hacken und die gemeinsamen Ordner anderer Computer einzusehen. Sehr oft ist die Operation erfolgreich, weil man vergisst, die Freigabe von Ordnern oder der gesamten Festplatte auf dem Computer auszuschließen.
Sicherheit ist für jeden wichtig, vom erfahrenen Techniker bis zum Computer-Analphabeten. Es liegt an Ihnen, welche Vorsichtsmaßnahmen Sie treffen, aber bedenken Sie, dass die Online-Sicherheit heute genauso wichtig (wenn nicht sogar wichtiger) ist wie die Sicherheit Ihres eigenen Zuhauses.

Dieses Projekt wird aus Mitteln der Europäischen Union kofinanziert. Die Verantwortung für den Inhalt dieses Dokuments tragen allein die Projektpartner; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.