In diese Cyber-Fettnäpfchen sollten Internetnutzer 2021 nicht mehr tappen - Neues Jahr, neuer Start und neue Vorsätze? Was aus IT-Sicherheitssicht wichtig ist.

2020 wird zweifellos in die Geschichtsbücher eingehen, denn nur wenige Teile unseres Lebens sind so geblieben, wie wir sie vor Covid19 gewohnt waren. Und die Corona-Pandemie hat uns in vielen Bereichen die gesellschaftlichen und politischen Versäumnisse in puncto Digitalisierung und Cyber-Sicherheit schmerzhaft aufgezeigt. Aber: In kaum einem anderen Jahr hat die Digitalisierung im privaten und beruflichen Umfeld mehr an Fahrt aufgenommen als 2020. War Homeoffice als Arbeitsmodell in vielen Betrieben zuvor undenkbar, ist es jetzt gelebte Realität. Meetings finden dank Videokonferenzen klimaneutral statt und WhatsApp, Zoom und Co. haben unlängst auch die Wohnzimmer der Generation 70+ erobert. Dieser Digitalisierungsschub hat auch dazu beigetragen, dass das laufende Jahr für viele Onlinekriminelle sehr erfolgreich wurde. Daher hat ESET für Internetnutzer die wichtigsten "Don'ts" für 2021 zusammengefasst, damit Anwender im neuen Jahr nicht wieder in die gleichen Cyber-Fallen tappen.

Home-Digitalisierung: Vertrauen ist gut - Kontrolle ist besser!
Baumärkte hatten bereits während des ersten Lockdowns Umsatzrekorde zu vermelden. Deutschland wurde scheinbar über Nacht zu einem Land der Handwerker und Gartengestalter. Vielen nutzten die Zeit, um auch in den eigenen vier Wänden digital aufzurüsten und legten sich Smart Home Steuerungssysteme, vernetzte Haushalts- und Gartengeräte, Steckdosen per Sprachsteuerung oder Webcams zur Überwachung des eigenen Grundstücks zu. Das große Techie-Finale folgte dann am 24. Dezember mit Smart-TVs, Laptops, Tablets und Smartphones unterm Weihnachtsbaum.

Selbst ambitionierte Heim-Admins haben hier Schwierigkeiten, den Überblick und die Kontrolle über das Heimnetzwerk zu behalten. Dank Home-Office vermischen sich zudem private und berufliche Geräte im selben (W)LAN. Eine Schwachstelle im smarten Device, auf dem Privatrechner oder Router reicht dabei schnell aus, um nicht nur private Daten, sondern auch sensible Firmendaten zu gefährden.

Security-Tipp: Smarte Helfer

Anwender sollten sich zuerst einen Überblick verschaffen, welche Devices im eigenen Netzwerk eingebunden sind. Schnell und problemlos ist das mit einem Internet-Security-Paket zu bewerkstelligen, das über einen eingebauten Heimnetz-Scanner verfügt. Im nächsten Schritt sollten Anwender dann smarte und berufliche Geräte im Netzwerk separieren. Am einfachsten geht das mit Hilfe der Funktion Gast-WLAN, die bei allen Routern verfügbar ist. Die Geräte nutzen für den Onlinezugang weiterhin denselben Router, haben aber einen anderen IP-Adressbereich als das Heimnetz und sind hierdurch von ihm getrennt. So können Angreifer selbst über unsichere Smart-Home-Geräte keine Verbindung auf Netzwerkspeicher (z.B. Raid-Systeme), PC oder Notebooks im Heimnetzwerk aufbauen.

Passwortfallen vermeiden und Durchblick behalten

In jedem zweiten Sicherheitsratgeber werden Anwender aufgefordert, komplexe Passwörter für jeden genutzten Online-Dienst zu verwenden. Eine lobenswerte Aufforderung, aber in der Praxis kaum realisierbar, denn kaum ein Anwender ist in der Lage, sich für jeden Dienst ein separates Passwort zu merken. Wie auch? Ohne Probleme müssten sich Anwender zehn oder mehr unterschiedliche komplexe Passwörter merken. In der Praxis gibt es daher entweder zu einfache Passwörter, die leicht zu knacken sind oder viele Passwort-Doubletten, d.h. zwei bis drei Passwörter werden für zehn oder mehr Dienste genutzt. Das erleichtert Cyberkriminellen ihre Arbeit, denn Passwortdiebe kommen so schnell auf einen Schlag mit nur einem erbeuteten Passwort an unterschiedliche Nutzerkonten, wie z.B. Social Media Accounts. Gelingt die Übernahme des E-Mail-Accounts, sind sie in der Lage, neue Passwörter für Online-Shops zu erstellen und anschließend auf Kosten der Opfer auf Shopping-Tour zu gehen.

Security-Tipp: Passwörter

PC-Nutzer sollten Passwortmanager verwenden, um für jeden Zweck ein anderes und vor allem sicheres Passwort zu erstellen und geschützt zu speichern. Achtung: Das Speichern im Browser ist keine sichere Alternative, da diese teilweise auf dem Endgerät unverschlüsselt vorliegen. Dadurch kann jeder Nutzer mit Zugang auf das Gerät die Dateien problemlos auslesen.
Ein Höchstmaß an Sicherheit bietet die Anmeldung mit Hilfe einer Zwei-Faktor-Authentifizierung. Hier wird zusätzlich zum Benutzernamen und Passwort ein individueller Einmalcode per SMS oder App an das Smartphone versendet oder die Anmeldung muss via APP bestätigt werden. Eine Vielzahl von Anbietern setzen seit längerem auf dieses sehr sichere Verfahren - Nutzer müssen es beim jeweiligen Dienst lediglich aktivieren. Zum Entsperren von Smartphones bieten sich

darüber hinaus biometrische Verfahren an, wie etwa der Fingerabdruck oder FaceID. Diese Methoden sind wesentlich schwerer zu knacken als eine simple Zahlenkombination oder Wischmuster.

Vier Basisregeln, die immer gelten:

* Setzen Sie eine Internet Security Software ein, die neben E-Mails und Webseiten auch Wechselmedien wie USB-Sticks, die Netzwerkschnittstellen und den Arbeitsspeicher auf Malware überprüft.

* Spielen Sie Updates des Betriebssystems, der installierten Software, Apps oder der Firmware automatisch ein. Bekannte Sicherheitslücken werden so geschlossen und sind nicht mehr durch Angreifer ausnutzbar. Sollte ein Automatismus fehlen: Regelmäßig auf Aktualisierungen prüfen und ebenfalls umgehend einspielen.

* Löschen Sie Mails unbekannten Ursprungs einfach - es handelt sich in der Regel immer um SPAM. Auch wenn ein vermeintlicher Lotto-Gewinn in Aussicht gestellt wird oder Schnäppchen locken: Klicken Sie auf keinen Fall auf Links oder öffnen Sie Dateianhänge, denn das kann zur Infektion Ihres Rechners mit Schadcode führen.

* Erstellen Sie regelmäßig Backups ihrer digitalen Schätze. Diese Backups sollten auf externen Festplatten erstellt werden, die nach Datensicherung vom Rechner umgehend zu trennen sind. Selbst wenn Ihr Rechner mit Ransomware infiziert und ihre Daten verschlüsselt wurden, hat der Schadcode keine Chance, auf das Backup-Medium zuzugreifen.

Und zu guter Letzt: Falls ein angeblicher Microsoft-Mitarbeiter bei Ihnen anruft, sollten Sie direkt einhängen. Denn es handelt sich immer um einen Kriminellen, der nur versucht Internetnutzer in die Falle zu locken und per Remote-Zugriff Schadcode auf den PC einzuspielen.