Avira

Avira Datenschutzbericht

Mehr Ordnung für Ihre digitale Welt

avira.com

August 2019

Einleitung

Wenn es um Online-Sicherheit geht, ist der Sommer keine Ferienzeit.

Ganz im Gegenteil: Bedrohungen und Risiken machen sprichwörtlich mobil, wenn sich die Menschen mit ihren Geräten auf Reisen begeben.

Unsere aktuellen Daten zur Jahresmitte zeigen, dass es überwiegend alte Bekannte in neuem Gewand und weniger die für Schlagzeilen sorgenden Zero-Day-Exploits sind, die den Großteil der vereitelten Angriffe ausmachen.

Dabei bietet die Reisezeit einen guten Anlass, um seine digitalen Gewohnheiten zu überdenken, mal wieder System und Apps zu aktualisieren, das Passwort-Management endlich in Ordnung zu bringen und ein VPN einzurichten, um sicherer im öffentlichen WLAN unterwegs zu sein und mehr Inhalte nutzen zu können.

Die Flucht aus der Wirklichkeit mag Teil eines idyllischen Sommerurlaubs sein, nicht jedoch, wenn man sich online bewegt. Vorsicht beim Surfen und der Eingabe personenbezogener Daten im Netz ist immer geboten – egal, zu welcher Jahreszeit.

Surfen Sie sicher!

Travis Witteveen,
CEO Avira

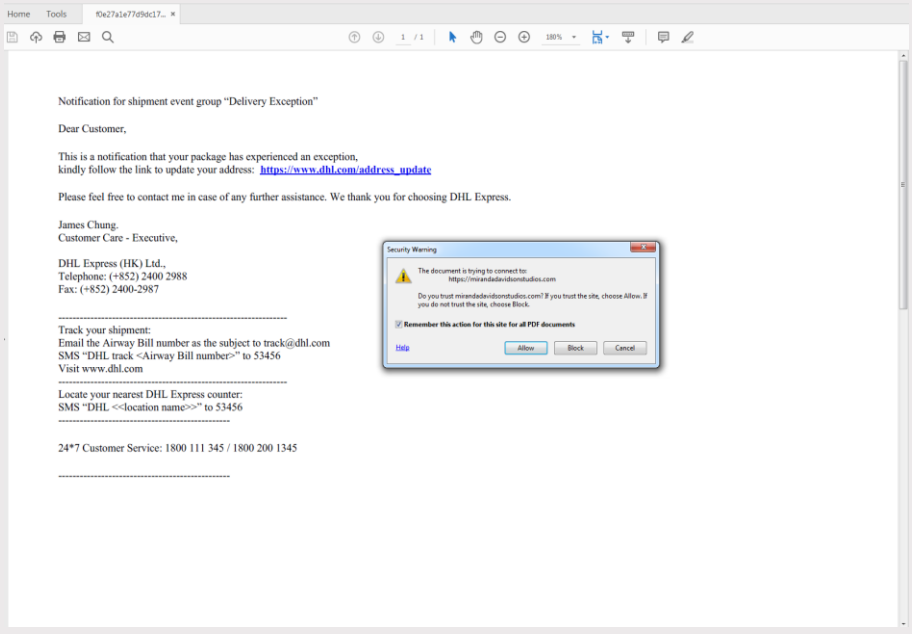
Bedrohungen zur Sommerzeit (1)

So wie die Hitzewellen rollen im Sommer auch die Bedrohungen auf uns zu und Kriminelle versuchen, in unsere Geräte einzudringen, um Profit aus unseren Daten zu schlagen. Wenn es um Mode, Urlaubsziele und Technologie geht, zieht es uns meist hin zum Neuen und Innovativen. Bei den Infektionsmethoden durch Malware ist es 2019 jedoch ein Mix aus Alt und Neu, der das Bild bestimmt.

Phishing-Angriffe (beliebt wie eh und je)

Phishing-E-Mails gehören immer noch zu den effektivsten Angriffsmethoden. Gerade in der Urlaubszeit, wenn man entspannt und arglos durch seine E-Mails klickt, wird man häufig Opfer dieser Attacken.

Hier ein Beispiel für einen äußerst raffinierten Phishing-Versuch, der von unseren Systemen erkannt wurde. Es handelt sich scheinbar um eine Lieferbenachrichtigung von DHL, professionell verfasst. Im Gegensatz zu herkömmlichen Phishing-E-Mails scheint die URL im Dokument auf die Website von DHL zu verweisen. Tatsächlich handelt es sich jedoch um eine böswillige Website (siehe Abbildung), die mit der Absicht erstellt wurde, den Nutzern nach dem Klicken auf den Link sensible Informationen zu entlocken.



Bedrohungen zur Sommerzeit (2)

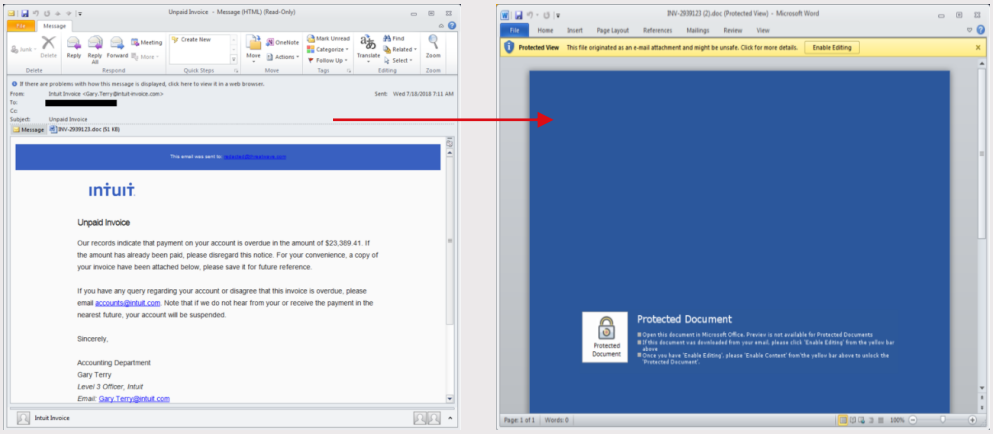
EXP/CVE-2010-2568 (altbekannt, aber noch immer effektiv)

Alte Windows-Sicherheitslücken bieten immer noch viel Angriffsfläche. Bei diesem Beispiel lässt die Windows-Shell das Ausführen von beliebigem Code über eine zu diesem Zweck erstellte LNK- oder PIF-Verknüpfungsdatei zu. Wenn in Windows die standardmäßige automatische Wiedergabe aktiviert ist, reicht schon das Anzeigen einer Vorschau dieser Datei aus, um den böswilligen Code auszulösen. Die Übertragung erfolgt häufig durch USB-Sticks.

Trickbot (Weiterentwicklung in neuem Gewand)

Vor Kurzem sorgte Trickbot, ein Banking-Trojaner, für Furore. In ihrer neuesten Form infizierte die Malware über 250 Mio. E-Mails. Die neue, unter dem Namen „TrickBooster“ bekannte Version ist mit einem gültigen Zertifikat signiert, äußerst funktionsreich und raffiniert:

- Speicherbasiertes Powershell-Spam-Mail-Bot-Modul
- Browser-Grabber-Modul zur Cookie- und Datenextraktion
- WebInjects für häufig genutzte Websites zum Diebstahl von Zugangsdaten
- Laterale Ausbreitung über berüchtigtes EternalBlue-Exploit
- Diebstahl von Zugangsdaten aus installierten Programmen, z. B. Wallets, Outlook, Nutzung des infizierten Computers als E-Mail-Spam-Knoten
- In hohem Maße verschlüsselt und verschleiert
- Durchgehende Aktualisierung via C&C-Server (hauptsächlich auf infizierten Routern ausgeführt)



Sicherheitstipps:

Sicherheitstipps:

- Nutzen Sie immer aktuelle Antiviren-Software.
- Aktualisieren Sie Windows und installierte Programme, ersetzen Sie veraltete Software-Versionen durch neue.
- Schließen Sie keine USB-Datenträger unbekannter Herkunft an, da diese infiziert sein könnten.
- Öffnen Sie keine Dokumente/Links aus E-Mails mit unbekanntem Absender/Spam-E-Mails. Geben Sie bei Aufruf unbekannter Links oder Quellen keine persönlichen Zugangsdaten ein und laden Sie keine Dateianhänge solcher E-Mails herunter.
- Nutzen Sie immer eine aktuelle Browser-Version.
- Ändern Sie häufig Ihre Zugangsdaten.

„Grund zur Besorgnis liefern nicht nur aktuelle Zero-Day-Bedrohungen. Viele Menschen empfinden es mitunter als lästig, sich um ihre Sicherheit im digitalen Raum zu kümmern, und vernachlässigen daher grundlegende Sicherheitsvorkehrungen.“

Alexander Vukcevic,
Director Protection Labs & QA

Updates sind Pflicht

Auf dem neuesten Stand bleiben

Veraltete Software birgt Sicherheitslücken, die für Angriffe auf alle Systeme ausgenutzt werden – von einzelnen Geräten bis zu Unternehmensnetzwerken.

Vor allem ungepatchte Software öffnet Tür und Tor für Hacker, die sich nicht nur Zugang zu Ihrem Gerät und Ihren persönlichen Daten verschaffen möchten, sondern ebenfalls in die Geräte Ihrer Freunde und Bekannten eindringen wollen, mit denen Sie vernetzt sind.

Einem aktuellen Bericht von Avira zufolge **wurden in den letzten Monaten einige der umfassendsten und wichtigsten Patches/Updates zur Behebung von Sicherheitslücken für Google Chrome, Java 8 und das Adobe Flash Player-Plug-in 32 veröffentlicht. Darüber hinaus sind gefälschte Update-Aufforderungen für Adobe Flash Player eine bekannte Strategie zur Verbreitung von Malware.**

Immer auf dem aktuellen Stand zu bleiben ist kein leichtes Unterfangen. Vielen Nutzern gelingt es nicht, die richtigen Updates für die vielen verschiedenen Apps auf ihren Geräten ausfindig zu machen und aufzuspielen. Darum machen sie es einfach nicht. Die Unsicherheit, ob es sich um ein echtes oder gefälschtes Update handelt, hat zur verstärkten Nutzung von Programmen zur automatisierten Software-Aktualisierung geführt, die Suche und das Anwenden von Patches übernehmen.

Leistung zählt

Elektronische Geräte und Koffer können einiges gemeinsam haben, vor allem: In den Ecken sammelt sich gern das ein oder andere, das Funktion und Leistung beeinträchtigt.

Darum ist Sauberkeit für eine positive digitale Erfahrung Pflicht. Löschen Sie also nicht benötigte vertrauliche Dateien dauerhaft, um Platz für neue zu schaffen.

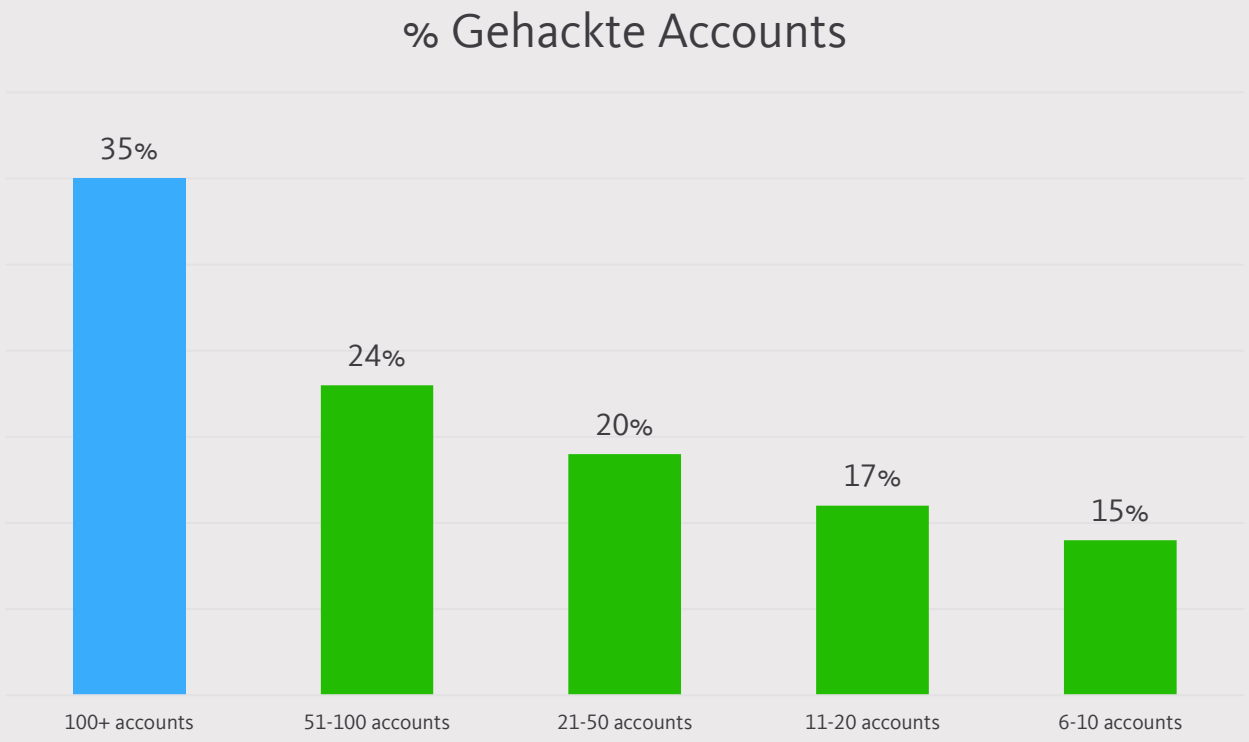
Der zwischen Januar und Ende Mai freigegebene Speicherplatz für Windows-Nutzer beläuft sich insgesamt auf 651.714.335 MB. Die Schätzungen für Android-Nutzer belaufen sich auf 321.118.640 MB für den Zeitraum Februar bis Mai.

Die morgendliche Zeitersparnis, von der die Nutzer aufgrund des schnelleren Systemstarts profitieren, ist hierbei nicht berücksichtigt.

Pack den Passwort-Manager ein

Sommer, Sonne, Datenpanne. Datenerhebungen zur Häufigkeit von Kontohacks und Datenpannen zeigen eines ganz deutlich: Je mehr Konten ein Nutzer besitzt, desto höher die Chance, dass eines davon gehackt wird. Hauptgrund hierfür ist das menschliche Gedächtnis und der Hang zum „Passwort-Recycling“. **Die Wahrscheinlichkeit, Opfer eines Hacks zu werden, beläuft sich bei Besitzern von 1–5 Konten auf 14 % – bei mehr als 30 Konten sogar auf 21 %.**

Den meisten Menschen fällt es schwer, sichere Passwörter im Gedächtnis zu behalten, die länger als acht Zeichen sind und Buchstaben in Klein-/Großschreibung sowie Zahlen und Symbole umfassen. Also verzichtet man auf die Mühe und verwendet einfach immer dasselbe Passwort – oder eine einfache Variante davon – für alle Konten. Die Schwierigkeiten beginnen, wenn ein Konto gehackt wird. Dann breitet sich das Problem nämlich auf alle Konten aus.



*von Avira zwischen dem 1. Januar 2019 und 31. Mai 2019 gesammelte Daten

Kontensicherheit

Derzeit besteht der Trend, Passwörter gehackter Konten weiterzugeben. Diesem Trend stehen die Nutzer schutzlos gegenüber. Man kann es sich jedoch einfacher machen, seine Konten wieder zu schützen. Viele der aktuellen Hacks zielen auf Unternehmen ab, die es versäumt haben, ihre Cloud-Datenspeicher-Konten sicher einzurichten. Wenn der Zugriff nicht durch sichere Passwörter geschützt wird und die Verschlüsselung von Daten ausbleibt, ist Ärger vorprogrammiert.

In diesem Fall besteht die Möglichkeit, auf www.haveibeenpwned.com zu prüfen, ob man gehackt wurde oder das Passwort seinen Weg auf eine Darkweb-Liste gefunden hat. Sofern man einen Passwort-Manager verwendet, hat man auch die Möglichkeit, sich bei einer Datenpanne benachrichtigen zu lassen. Außerdem lassen sich mit einem Passwort-Manager sichere und individuelle Passwörter für alle Konten erstellen und speichern.

Auf Passwörter lässt sich auch in Zukunft nicht verzichten

Die Einrichtung des World Wide Web Consortium (W3C) zur Umsetzung des neuen Webstandards „**WebAuthn**“ ließ die Hoffnung keimen, dass Passwörter schon bald der Vergangenheit angehören würden. Allerdings wird der neue Standard wohl vorerst ein zweitrangiger Faktor bei der Authentifizierung bleiben.

Aktuell besteht die größte Herausforderung darin, dass WebAuthn auf Geräteverknüpfung basiert und daher nicht nur die Registrierung für die einzelnen Dienste, sondern auch für die einzelnen Geräte erfordern würde.

„Man stelle sich den organisatorischen Aufwand vor: Es müsste immer verfolgt und erfasst werden, welche Dienste bei welchen Authentifizierungsgeräten registriert sind. Neben diesen konzeptionellen Herausforderungen ist es so, dass **mit WebAuthn keine Daten verschlüsselt werden können**“, erklärt Tom Gaiser, Leiter der Identity Protection Unit bei Avira. „Am besten verwendet man hierfür ein Passwort, das ausschließlich der Eigentümer der Daten kennt – wie das Master-Passwort bei einem Passwort-Manager.“

Anonym und sicher surfen

Ein VPN (Virtual Private Network) stellt eine sichere, verschlüsselte Verbindung zwischen zwei physikalisch getrennten Geräten her. Das ist gegenüber dem Versenden unverschlüsselter HTTP-Datenpakete ein enormer Fortschritt. Oft wird HTTP mit einer für jeden lesbaren Postkarte und ein VPN mit einem Einschreiben verglichen, bei dem Sender und Empfänger unterschreiben müssen.

VPN-Nutzung ist jahreszeitenabhängig
Unsere aktuellen Untersuchungen zeigen, dass VPN-Nutzung jahreszeitenabhängig ist. Während der Sommermonate steigt die Anzahl der Nutzer spürbar. Gleichzeitig sehen wir, dass die Nutzer im Sommer häufiger über das Smartphone auf das VPN zugreifen. Bei unserer in Amerika durchgeführten Erhebung gaben **51 % der Teilnehmer an, ein VPN auf dem Smartphone zu nutzen – beinah gleichauf mit den 56 %, die via Laptop auf das VPN zugreifen.**

Auch die typische Verwendung korrelierte mit den Sommermonaten: **66 % gaben an, ein VPN zur Erhöhung der Verbindungssicherheit bei Online-Banking und zur Kommunikation über öffentliche WLAN-Netzwerke zu nutzen. 65 % verwenden ein VPN zur Umgehung von Geo-IP-Einschränkungen, um außerhalb der USA Website-Inhalte aufzurufen oder zu streamen.**

*Quelle: Avira Online Survey (Multiple-Choice-Fragestellung) mit 2519 Teilnehmern im Alter zwischen 20 und 65 Jahren (USA – Januar–Februar 2019)


Avira
Protecting people
in the connected world
avira.com

Das geheime Leben des Fernsehers

Der Fernseher ist häufig das erste IoT-Gerät im Haushalt. Aber nur wenige wissen, was vor ihren Augen in diesen Geräten alles vor sich geht.

Smart-TVs begannen vor einigen Monaten zunehmend in das Licht von Datenschützern zu rücken, als Hacker über 72.000 Smart-TVs Botschaften sendeten, die den YouTube-Kanal „PewDiePie“ bewarben. Smart-TVs haben sich als einfache Ziele erwiesen, zu denen selbst unerfahrene Hacker Remote-Verbindungen herstellen können. Die ungebetenen Fernsehgäste waren in der Lage, den Kanal zu wechseln, die Lautstärke zu ändern und bizarre oder relativ harmlose Inhalte wiederzugeben (wie etwa die Aufforderung, PewDiePie zu abonnieren).

Smart-TVs beunruhigen Datenschützer ebenfalls, weil sie personenbezogene Nutzerdaten sammeln und weitergeben. Dass Laptops und Smartphones Nutzerdaten sammeln, ist bekannt, aber auch **Fernsehgeräte mit Internetverbindung sammeln enorme Datenmengen**: Fernsehgewohnheiten, Programmauswahl und diverse weitere Information werden an die Gerätehersteller und ihre Werbepartner gesendet – oft ohne Wissen der Gerätenutzer.

Sicherheitstipps für den Sommer (1)

Der Sommer ist eine besondere Zeit: Wir freuen uns darauf, bekannte Gesichter wiederzusehen und ferne Länder zu entdecken – all das planen wir selbst Monate im Voraus. Dabei begleitet uns moderne Technologie, die in Form von Laptops, Smartphones und Tablets ihren Weg in unser Reisgepäck findet. Hier einige grundlegende Tipps für einen sorgenfreien Urlaub:

Bleiben Sie geschützt

- Antivirus: Installieren Sie eine renommierte, unabhängig getestete Sicherheitslösung auf Ihrem Gerät, die Sie vor neuen – und bekannten – Bedrohungen schützt.

- Updates: Gehen Sie kein Risiko ein und installieren Sie alle aktuellen Updates auf ihrem Gerät. Das geht am einfachsten mit einem Software Updater. Auf diese Weise brauchen Sie sich selbst nicht mehr um die richtigen Updates für Ihre vielen Apps zu kümmern.

Gönnen Sie sich eine Denkpause

- Password Manager: Mit einem Passwort-Manager gehört Passwort-Recycling der Vergangenheit an und Sie brauchen selbst keine sicheren und individuellen Passwörter mehr für all Ihre Online-Konten im Gedächtnis zu behalten. So müssen Sie sich lediglich ein sicheres Passwort merken und können das Erstellen, Speichern und Synchronisieren sicherer Passwörter für alle Ihre Geräte der Anwendung überlassen.

Stilsicher – überall

- Ein virtuelles privates Netzwerk begleitet Sie auf all Ihren Geräten – nicht nur zuhause auf dem Desktop. Mit einem VPN bewegen Sie sich sicher in unsicheren öffentlichen Netzwerken und können Ihre eigene GEO-IP auswählen. So können Sie auf Inhalte zugreifen, egal, wo Sie gerade sind. Ohne VPN private Daten in einem öffentlichen WLAN übermitteln? Vergessen Sie das lieber ganz schnell.

Sicherheitstipps für den Sommer (2)

Gehen Sie nicht ins Phishing-Netz

- Phishing: Irreführende E-Mails oder Websites, die speziell nach dem Vorbild echter Quellen erstellt wurden, sind ein großes Geschäft. Cyberkriminelle nutzen sie, um Ransomware zu verbreiten, politische Parteien zu unterwandern und nichtsahnenden Personen Passwörter und Zugangsdaten zu entlocken.

- Vorsicht beim Klicken: Prüfen Sie E-Mails und Websites sorgfältig. Ist die Adresse des Senders korrekt? Sind die Links mit HTTPS verschlüsselt? Was sagt Ihr Bauchgefühl? Auch über Links aus zwielichtigen E-Mails kann man sich schnell mit Ransomware anstecken.

- Vorsicht bei der Dateneingabe: Geben Sie keine Daten über Links und Anhänge ein, die Ihnen per E-Mail gesendet wurden.

Legen Sie Ihre Smart-Geräte an die Leine

- Vergewissern Sie sich, welche Daten Ihre Smart-Geräte sammeln und senden. Mithilfe kostenloser Apps bringen Sie in Erfahrung, wer sich in Ihrem Heimnetzwerk angemeldet hat, mit wem kommuniziert wird und ob die Kommunikation sicher ist.

Behalten Sie eine gesunde Skepsis: **Der wichtigste Faktor Ihrer Sicherheitslösung sind Sie**. Antivirenprogramme filtern einen Großteil der Schadsoftware. Update-Programme und Passwort-Manager erleichtern das Leben und sorgen für mehr Sicherheit. Aber vergessen Sie dabei nicht Ihre Rolle. Eine gesunde Skepsis ist wichtig – auch im Urlaub. Ihre digitale Gesundheit wird es Ihnen danken.


Avira
Protecting people
in the connected world
avira.com

Avira

avira.com