Allianz

CYBER-NEWSLETTER

Aktuelle Entwicklungen

Sicherheitslücke in Apples E-Mail-App für iPhone und iPad

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt derzeit vor einer gefährlichen Sicherheitslücken bei Apples E-Mail-App für iPhone und iPad.

Durch die Schwachstellen ist es für Angreifer möglich, E-Mails zu lesen, zu ändern und zu löschen.

Apple wird voraussichtlich mit der iOS Version 13.4.5 ein Update zur Schließung der Sicherheitslücke zu Verfügung stellen.

Was können Sie tun?

1. Löschen Sie die E-Mail-App von Ihrem iPhone (löschen erst ab iOS12 möglich) bzw. iPad (erst ab iPadOS13 möglich) und nutzen Sie ein alternatives Programm.
2. Oder deaktivieren Sie die fortlaufende Synchronisation.

Kurzanleitung zur Deaktivierung der Synchronisation
(ab iOS bzw. iPad Version 13.x)

1. „Einstellungen“ → „Passwörter & Accounts“
2. E-Mail-Account auswählen → Button bei „Mail“ nach links (für jeden Account wiederholen)
3. Zurück zu „Passwörter & Accounts“ → „Datenabgleich“
4. Button bei „Push“ nach links
5. Auswahl bei „Abrufen“ auf „Manuell“.

IN DIESEM QUARTAL

BSI – Angepasste Empfehlungen für Passwörter

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seine Empfehlungen für Passwörter überarbeitet. So müssen z.B. Passwörter bei ausreichender Komplexität nicht mehr regelmäßig gewechselt werden, da dies eher dazu führte, dass schwache Passwörter genutzt wurden. Die ausführlichen Empfehlungen erhalten Sie über nebenstehenden QR-Code.

Corona – Infektionsgefahr im Internet

Die Hersteller von Schadsoftware nutzen das gesteigerte Informationsbedürfnis aufgrund von Corona massiv aus. Unter anderem kursieren gefälschte Corona-Apps und -Karten.

Mit Lockangeboten wie „CoronaVirus Discount! 10 % off ALL products!“ oder saftigen COVID-19-Rabattcodes werben Kriminelle in einschlägigen Untergrundforen derzeit für Angriffswerkzeuge, mit denen man sich Schadsoftware nach Maß schneidern kann. Ihre Geschäftsstrategie dürfte aufgehen. Seit Beginn der Pandemie setzen sie verstärkt auf Phishing-Kampagnen und Schadsoftware, welche das zunehmende Informationsbedürfnis ausnutzt.

Verseuchte Corona-Live-Karten

In einem russischsprachigen Forum wird u.a. ein „Corona Infection Kit“ angeboten. Potenzielle Opfer soll es mittels einer Kopie der COVID-19-Livekarte der Johns Hopkins University (JHU) anlocken – inklusive echter, automatisch aktualisierter Kartendaten. Das „Infection Kit“ kostet rund 200 US-Dollar.

Wer mit der Karte agiert, fängt sich eine Variante der Schadsoftware „AZORult“ ein, welche über den Diebstahl sensibler Informationen hinaus auch die Fähigkeit besitzen soll, weitere Schadsoftware nachzuladen.

Sieht aus wie das Original: AZORults bösartige Variante der COVID-19-Karte der JHU.
(Bild: https://blog.reasonsecurity.com/)

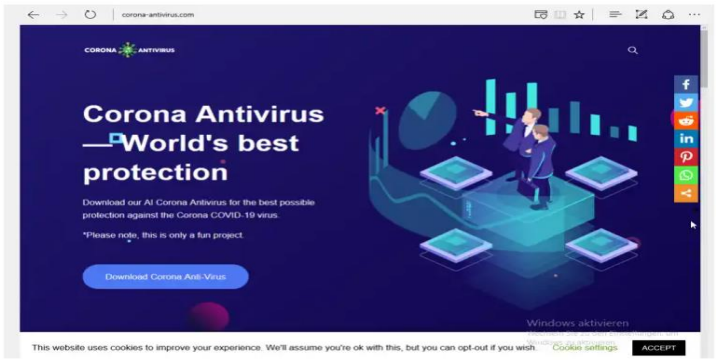
"Corona Antivirus":

Botnetz statt Social Distancing

Mit dem Werbeslogan „Corona Antivirus – World's best protection“ wird derzeit eine KI-basierte „Antivirensoftware“ angepriesen, die vor dem Coronavirus schützen soll.

Wer diese Software nutzt, fängt sich eine Windows-spezifische Schadsoftware ein.

Sie integriert das infizierte System in ein Botnetz, um es unter anderem für DDoS-Attacken zu missbrauchen. Sie könnte vom Angreifer aber auch missbraucht werden, um aus der Ferne sensible Daten zu sammeln oder das Nachladen weiterer Schadsoftware zu veranlassen.



Nicht lustig: Eine angebliche Anti-Corona-Anwendung, die in Wirklichkeit Botnetze baut.
(Bild: Screenshot)

Was können Sie tun?

1. Folgen Sie keinen Links, welche Sie z.B. per E-Mail erhalten.
2. Laden Sie keine Dateien von nicht vertrauenswürdigen Seiten herunter.
3. Rufen Sie z.B. die Seiten der JHU oder des RKI nur direkt oder über Ihre Lesezeichen auf.

BSI – Angepasste Empfehlungen für Passwörter

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seine Empfehlungen für Passwörter überarbeitet. So müssen z.B. Passwörter bei ausreichender Komplexität nicht mehr regelmäßig gewechselt werden, da dies eher dazu führte, dass schwache Passwörter genutzt wurden. Die ausführlichen Empfehlungen erhalten Sie über nebenstehenden QR-Code.

Zoom – Videokonferenzlösung angreifbar

Medienberichten zufolge bieten Hacker in Untergrundforen zwei Zero-Day-Exploits für Clients der Videokonferenzsoftware Zoom an. Die Zoom-Clients unter macOS und Windows sollen über zwei bislang ungepatchte Sicherheitslücken angreifbar sein. Da derzeit weltweit Millionen Menschen Zoom nutzen, ist die Software ein lukratives Ziel.

Zero-Day-Lücken sind Schwachstellen, für die es noch kein Sicherheitsupdates gibt. Solche Lücken sind dementsprechend besonders gefährlich. Ohne einen Patch können Angreifer Software ungehindert attackieren. Der Exploit für den Windows-Client soll derzeit für 500.000 US-Dollar angeboten werden.

Angriffe durch Schadsoftware möglich

Nutzen Angreifer diese Zero-Day-Lücken erfolgreich aus, können sie Zoom-Konferenzen belauschen. Der Exploit für den Windows-Client soll es in Video-Konferenzen befindlichen Angreifern in Kombination mit einer anderen Schwachstelle erlauben, eigenen Code auf Computern auszuführen. Die Lücke im macOS-Client soll nicht zu Remote Code Execution führen und sich schwerer ausnutzen lassen. Gemäß Herstellerangaben wurden diese Schwachstellen in Zoom 5.0 behoben.

Zoom-Bombing und Datenweitergabe

In der jüngsten Vergangenheit sorgte Zoom für weitere Negativ-Schlagzeilen. So konnten sich Fremde leicht Zugang zu Videokonferenzen verschaffen und diese stören. Ebenso gab Zoom ohne das Wissen der Nutzer Daten an Facebook weiter und es wurden hunderttausende Nutzerdaten (inkl. Logindaten) im Darknet zum Kauf angeboten. Der Bundesdatenschutzbeauftragte rät bis zur Behebung der Probleme bzw. der Ausräumung der Bedenken generell von der Nutzung von Zoom ab.

Was können Sie tun?

1. Installieren Sie die aktuellste Version von Zoom bzw. alle verfügbaren Sicherheitsupdates.
2. Ändern Sie sofort das Passwort für Ihren Zoom-Account.
3. Aktivieren Sie, sofern möglich, die 2-Faktor-Autentifizierung als zusätzlichen Schutz.
4. Nutzen Sie eine andere Lösung für Videokonferenzen.

9 Millionen EasyJet-Konten gehackt, Daten geleakt

Die Fluggesellschaft EasyJet ist Opfer eines Hackerangriffs geworden. Hierbei hatten die Angreifer Zugriff auf ca. 9 Millionen Kunden-Konten und auf die damit in Zusammenhang stehenden Daten (wie z.B. E-Mail-Adressen, Name, Adressen). Bei 2.208 Kunden-Konten konnten die Hacker zusätzlich auch Kreditkartendaten erbeuten. EasyJet selbst will alle betroffenen Kunden bis spätestens 26. Mai 2020 informieren.

Es ist zu erwarten, dass die betroffenen EasyJet-Kunden nun zeitnah Opfer von gezielten Phishing-Kampagnen werden.

Was können Sie tun?

1. Ändern Sie sofort die Zugangsdaten für Ihren EasyJet-Account und alle anderen Konten, bei denen sie das gleiche Passwort nutzen.
2. Nutzen Sie Passwortmanager zur Verwaltung Ihrer Passwort und nutzen Sie für jeden Dienst ein eigenes Passwort.
3. Seien Sie besonders achtsam bei E-Mails, welche vermeintlich von EasyJet oder EasyJet Holidays verschickt wurden. Hierbei könnte es sich um Phishing-Mails handeln.

BSI – Angepasste Empfehlungen für Passwörter

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seine Empfehlungen für Passwörter überarbeitet. So müssen z.B. Passwörter bei ausreichender Komplexität nicht mehr regelmäßig gewechselt werden, da dies eher dazu führte, dass schwache Passwörter genutzt wurden. Die ausführlichen Empfehlungen erhalten Sie über nebenstehenden QR-Code.

TOP 10 der Sicherheitslücken 2016 bis 2019

Offensichtlich patchen Administratoren vor allem Windows-Systeme nicht regelmäßig und zeitnah. Angreifer nutzen sehr häufig alte und bekannte aber ungepatchte Lücken, weil dafür meistens weniger Ressourcen nötig sind, als Angriffswerkzeuge für "brandneue" Sicherheitslücken zu entwickeln.

Dies geht aus einem Bericht der *Cybersecurity and Infrastructure Security Agency* (CISA), dem *Federal Bureau of Investigation* (FBI) sowie der US-Regierung hervor. Die Autoren zeigen auch die zehn am meisten ausgenutzten Sicherheitslücken im Zeitraum von 2016 bis 2019 auf.

Windows im Fadenkreuz

Angreifer haben es vor allem auf Sicherheitslücken in Microsofts Objekt Linking and Embedding (OLE) abgesehen. Damit kann beispielsweise eine Tabellenkalkulation in ein Textdokument eingebunden werden. Solche Lücken nutzen Angreifer aus, um Schadcode zu übertragen und auszuführen. Dem Bericht zufolge haben es vor allem staatliche Hacker aus China, Iran, Nordkorea und Russland auf solche OLE-Lücken abgesehen.

Weitere häufig genutzte Sicherheitslücken

- Apache Struts (CVE-2017-5638)
- Microsoft .NET Framework (CVE-2017-8759)
- Drupal (CVE-2018-7600)
- Microsoft Office (CVE-2017-11882, CVE-2017-0199, CVE-2012-0158)
- Microsoft SharePoint (CVE-2019-0604)
- Verschiedenen Windows- und Windows-Server-Versionen (CVE-2017-0143)
- Microsoft Word (CVE-2015-1641)
- Adobe Flash Player (CVE-2018-4878)

Was sind CVE-Nummern?

Common Vulnerabilities and Exposures (CVE – deutsch *Gemeinsame Schwachstellen und Verwundbarkeiten*) ist ein Industriestandard, dessen Ziel die Einführung einer einheitlichen Namenskonvention für Sicherheitslücken und anderen Schwachstellen in Computersystemen ist. Mehrfachbenennung gleicher Gefahren durch verschiedene Unternehmen und Institutionen werden um eine laufende Nummer (z. B. CVE-2006-3086) ergänzt, um eine eindeutige Identifizierung der Schwachstelle zu gewährleisten.

Status quo

Im aktuellen Jahr haben es Hacker bisher vor allem auf eine Lücke (CVE-2019-19781) im Citrix Application Delivery Controller (ADC) abgesehen. Sicherheitspatches sind seit Ende Januar 2020 verfügbar und sollten dringend installiert werden.

Auch die Schwachstellen in der VPN-Lösung von Pulse Secure steht dieses Jahr bisher hoch im Kurs. Updates stehen ebenfalls seit Anfang Januar 2020 zum Download bereit und sollten ebenfalls dringend installiert werden.

Was können Sie tun?

1. Halten Sie die Virensignaturen auf Ihren Systemen immer aktuell.
2. Installieren Sie zeitnah die von den Herstellern zur Verfügung gestellten Sicherheitsupdates.
3. Überprüfen Sie Ihre Systeme regelmäßig auf Schwachstellen.

BSI – Angepasste Empfehlungen für Passwörter

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seine Empfehlungen für Passwörter überarbeitet. So müssen z.B. Passwörter bei ausreichender Komplexität nicht mehr regelmäßig gewechselt werden, da dies eher dazu führte, dass schwache Passwörter genutzt wurden. Die ausführlichen Empfehlungen erhalten Sie über nebenstehenden QR-Code.

Thunderspy: Notebooks in 5 Minuten gehackt

Forscher der Eindhoven University of Technology haben einen neuen Weg gefunden, um Sicherheitslücken in Thunderbolt-Anschlüssen auszunutzen und so vollständigen Zugriff auf PCs zu erhalten.

Die Angriff funktioniert ausschließlich mit physischem Zugriff auf ein Gerät mit Thunderbolt 3 Schnittstellen, erlaubt dann aber das Auslesen sämtlicher Daten und die Installation beliebiger Software.

Thunderbolt ist eine Schnittstelle, welche an vielen aktuellen Notebooks vorhanden ist. Diese sieht aus wie eine USB-C-Schnittstelle und wird beispielsweise dafür genutzt, ein Laptop mit einer Docking-Station zu verbinden.

Thunderbolt-3-Schnittstelle

Eine „Thunderspy"-Attacke lässt sich mit gängigen Hardware-Tools in unter 5 Minuten durchführen. Der Angreifer muss dazu physischen Zugriff auf das Notebook haben und die Unterseite aufschrauben, um an den Thunderbolt-Controller zu gelangen. Über entsprechende Hardware-Tools kann er sich mit den Firmware-Speicherchips verbinden und eine eigene modifizierte Firmware aufspielen.

Danach kann der Angreifer sein eigenes Notebook über Thunderbolt verbinden, Code ausführen und so die Passwortsperre umgehen. Eine verschlüsselte Festplatte schützt in einem solchen Fall nicht.

Noch einfacher wird der Angriff, wenn der Angreifer Zugriff auf Thunderbolt-Peripherie (wie zum Beispiel eine Dockingstation) erhält, die das Opfer mindestens einmal an seinem Notebook angeschlossen hat. Diese ist mittels hinterlegtem Code als vertrauenswürdig eingestuft, so dass es noch einfacher ist, auf andere Thunderbolt-Geräte zu kopieren.

„Thunderspy" lässt sich wegen der Komplexität nur gezielt auf einem individuellem Notebook ausführen. Es geht hier um das so genannte „Evil Maid"-Szenario, bei dem ein Computer mit wichtigen Informationen heimlich manipuliert oder gestohlen wird, um beispielsweise an Daten zu gelangen oder um eine Backdoor zu installieren.

Was können Sie tun?

1. Deaktivieren Sie sämtliche Thunderbolt-Anschlüsse.
2. Lassen Sie ihr Notebook nicht unbeaufsichtigt.
3. Stellen Sie sicher, dass keine fremde Person Zugriff auf Thunderbolt-Geräte hat, welche Sie verwenden.

BSI – Angepasste Empfehlungen für Passwörter

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seine Empfehlungen für Passwörter überarbeitet. So müssen z.B. Passwörter bei ausreichender Komplexität nicht mehr regelmäßig gewechselt werden, da dies eher dazu führte, dass schwache Passwörter genutzt wurden. Die ausführlichen Empfehlungen erhalten Sie über nebenstehenden QR-Code.