SWITCH Security Report zu aktuellen Trends im Bereich IT-Security und Privacy

Januar/Februar 2021

I. Dependency Confusion – Wenn Vertrauen zu gut ist, um gerechtfertigt zu sein

Man stelle sich folgendes Szenario vor: Auf frei zugänglichen Tischen in der Innenstadt kann jedermann Lebensmittel ablegen und jedermann kann sich von diesen Tischen bedienen. Auf einem der Tische liegt eine Schale frischer Lasagna al Forno. Niemand weiss, woher sie kommt oder was drin ist. Aber sie riecht fantastisch, sieht gut aus und wäre jetzt genau richtig, weil man Hunger hat. Würde man sie mitnehmen, in den eigenen Ofen stellen und ohne vorher zu prüfen, was in der Lasagna drinsteckt, in der Betriebskantine anbieten? Obwohl dort 30 top-ausgebildete und hochbezahlte Köchinnen arbeiten?

Klingt absurd, vielleicht geradezu aberwitzig? Ist es eigentlich auch. Dennoch passiert genau das tagtäglich in der IT-Welt. Mit dem Unterschied, dass die Tische hier "Open Source Repositories" heissen. Und auf ihnen statt Lasagna Software in allen erdenklichen Formen liegt. Und obwohl sie nicht immer wissen, woher der Code kommt, den sie – grob gesprochen – in ihre eigene Software einbinden und auf Servern, Endgeräten oder Netzen laufen lassen: alle greifen zu. Auch Tech-Giganten wie PayPal, Shopify, Netflix, Yelp, Tesla, Uber, Apple, Microsoft und andere. Sie

alle wurden "Opfer" des Sicherheitsforschers Alex Birsan, der u.a. im Rahmen von Bug-Bounty-Programmen 130.000 US-Dollar damit verdiente, dass er untersuchte, ob und wie Malware über sogenannte Dependencies aus Open Source Repositories in die Systeme der Auftraggeber gelangt. Birsan fand heraus, dass das "Ob?" gar keine Frage sei, sondern nur das "Wie?"

Der Sicherheitsforscher nutzte die Tatsache, dass sich in verschiedenen Programmiersprachen relativ einfach prüfen lässt, ob eine Dependency lokal oder im Internet bereitsteht. Da normalerweise die Dependency mit der höheren Versionsnummer, also der aktuelleren Version geladen wird, musste er lediglich die Namen der bislang verwendeten Dependencies kopieren, ihnen eine höhere Versionsnummer zuschreiben und konnte dann unter diesen Namen und Versionsnummern eigenen Code in öffentlich zugängliche Repositories hochladen. Der wurde dann auch gerne genommen und verschaffte ihm Zutritt zu den inneren Systemen der Tech-Firmen. Zum Auslesen der Daten aus den gehackten Systemen und zum Beleg dafür, wie tief er in die jeweiligen Systeme eindringen konnte, nutzte Birsan das DNS-Protokoll.

Die Firmen, die – darauf legt Birsan in seinem Bericht grossen Wert – alle vorab informiert waren, haben daraufhin ihre Routinen bei der Nutzung von Skripten aus Repositories so verändert, dass derlei Hacks künftig nicht mehr möglich sein sollen.

Nachzulesen unter:

https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
https://www.heise.de/news/Sicherheitsforscher-bricht-ueber-Open-Source-Repositories-bei-PayPal-Co-ein-5051635.html
https://www.bleepingcomputer.com/news/security/researcher-hacks-over-35-tech-firms-in-novel-supply-chain-attack/amp

II. Wasser hacken - keine neue Trendsportart, sondern ernsthafte Bedrohung

Während ein Malware-Skript aus einem Repository in Marc Elsbergs 2012 erschienenen Thriller "Blackout" zu einem – fiktionalen – europaweiten Stromausfall mit verheerenden Folgen führte, erlebte Florida am 5. Februar einen höchst realen Angriff auf eines seiner OT-Systeme: die Wasserversorgung der Stadt Olmar. Ein Hacker hatte sich Zugriff auf die Steuerung der Wasseraufbereitung verschafft und versucht, die Zumischung von Natriumhydroxid um den Faktor 111 zu erhöhen und damit das Trinkwasser für 15.000 Menschen zum tödlichen Cocktail zu machen. Die Manipulation wurde glücklicherweise rechtzeitig entdeckt, obwohl die Angreifer sich nicht-bestätigten Meldungen zufolge über eine Remote-Wartungssoftware ins System eingeschlichen hatten, die auch von vielen externen Vertragspartnern der Wasseraufbereitungsanlage genutzt wird.

Bei allem glimpflichen Ausgang zeigt der Vorfall, dass Angriffe auf kritische Infrastrukturen via OT- (Operational Technology, also Betriebstechnik), ICS- (Industrial Control Systems) und

SCADA- (Supervisory Control and Data Acquisition) Systeme immer mehr als ernst zu nehmende Bedrohungen erkannt und bekämpft werden müssen. SWITCH trägt dieser Entwicklung schon seit einigen Jahren mit dem Aufbau eines eigenen OT/ICS/SCADA-Security-Bereichs Rechnung.

Nachzulesen unter:

https://www.welivesecurity.com/2021/02/09/hacker-attempts-poison-florida-city-water-supply
https://www.faz.net/aktuell/gesellschaft/kriminalitaet/florida-hacker-manipulieren-wasser-in-aufbereitungsanlage-17188261.html
https://www.computerworld.ch/security/hacking/hacker-brunnenvergifter-2630786.html
https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html?utm_source=twCNN&utm_term=link&utm_medium=social&utm_content=2021-02-09T02%3A55%3A27
https://www.databreachtoday.com/5-critical-questions-raised-by-water-treatment-facility-hack-a-15955

III. Emotet: Der König ist tot – Es lebe hoffentlich so schnell kein neuer!

2019 bezeichnete der Präsident des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), Arne Schönbohm, Emotet als "König der Schadsoftware". Mitte Januar 2021 beendeten Europol und die Cyberspezialeinheiten acht europäischer Länder diese Regentschaft, indem sie in einer konzertierten zweijährigen Aktion die Infrastruktur des weltweit gefürchteten Malware-Netzwerks unter ihre Kontrolle bringen konnten.

Emotet trat 2014 erstmals als Bankentrojaner in unliebsame Erscheinung, mutierte aber im Lauf der Zeit zum lizenzpflichtigen Türöffner für andere Cyberkriminelle und avancierte so zum Lieblingstool des organisierten Verbrechens. Mit dem simplen Trick, mittels gefälschter Word-Dokumente, wie z.B. Rechnungen, Lieferankündigungen oder Covid19-Förderanträge, Computer mit Malware zu kompromittieren, installierten die Emotet-Hacker einen gut getarnten, immer wieder nutzbaren Zugang zu Systemen und Netzwerken, den sie an andere Kriminelle weiterverkauften, die dann ihre eigenen Würmer, Erpressungstrojaner oder Daten-Grabber installieren und entsprechend nutzen konnten. Welchen massiven Impact Emotet hatte, lässt sich nicht zuletzt auch daran ablesen, dass wir seit der Ausgabe 1/2019 in insgesamt fünf Security Reports immer wieder berichtet, Sicherheitsmassnahmen vorgeschlagen und für erhöhte Awareness geworben hatten für die Gefahren, die z.B. vom Malware-Trio Emotet - Trickbot - Ryuk ausgegangen waren.

Nun scheint die Emotet-Gefahr fürs erste gebannt zu sein, doch ist für alle, die sich ernsthaft mit Cybersecurity beschäftigen, aktuell zwar eine grosse und wichtige Schlacht geschlagen und gewonnen. Der Krieg indes wird weitergehen. Zumal – und das ist enorm wichtig zu wissen – nur die Emotet-Infrastruktur zerschlagen ist. Alle anderen nachgeladenen Malware-Programme, wie Erpressungsmalware und andere, sind nach wie vor aktiv und brandgefährlich.

Nachzulesen unter:

https://www.tagesschau.de/wirtschaft/emotet-bka-101.html
https://www.golem.de/news/europol-ermittler-legen-koenig-der-schadsoftware-lahm-2101-153723.html
https://www.swisscybersecurity.net/cybersecurity/2021-01-28/europol-legt-banking-trojaner-emotet-lahm
https://www.heise.de/news/Emotet-Strafverfolger-zerschlagen-Malware-Infrastruktur-5038233.html
https://www.nzz.ch/technologie/die-ermittler-machen-fortschritte-im-kampf-gegen-cyberkriminelle-doch-das-alleine-reicht-nicht-ld.1599047?reduced=true
https://www.heise.de/news/Emotet-Was-passiert-mit-den-Opfern-5039808.html

IV. Totgesagte leben länger: Wie Phishing-Mailer mit dem guten alten Morse-Alphabet modernste Sicherheitsfilter austricksen

Dass man Emotet trotz Zerschlagung noch nicht abschreiben sollte, mag ein anderes aktuelles Beispiel zeigen: Anfang Februar berichtete Bleepingcomputer.com darüber, dass Hacker einen neuen Weg gefunden hätten, Sicherheitsfilter in Mailprogrammen des 21. Jahrhunderts mit einem beinahe 200-jährigen Zeichensystem zu umgehen. Sie nutzen das Morsealphabet. 1837 hatte Samuel Morse zusammen mit Alfred Vail das nach ihm benannte Zeichenset entwickelt, das Buchstaben als Abfolge von Punkten und Strichen bzw. kurzen und langen Signalen aller Art (Lichter, Töne, elektrische Impulse) codiert.

2021 verschicken Cyberkriminelle im ersten Schritt eine E-Mail, der eine als wichtig deklarierte vorgebliche Excel-Datei angehängt ist. Diese ist in Wahrheit aber ein HTML-Dokument mit einem Javascript, in dem die Buchstaben durch die entsprechenden Morsezeichen ersetzt wurden, so dass das Script von Sicherheitsfiltern nicht als bösartig erkannt wird.

Wird das Dokument geöffnet, wandelt sich der Morsecode automatisch in eine hexadezimale Zeichenfolge um, die zur Anzeige einer gefakten Login-Seite für Office 365 führt. Kommen die Nutzer der Aufforderung nach, ihre Zugangsdaten einzugeben, werden Benutzername und Kennwort direkt zu den Cyberkriminellen geschickt. Angaben von Bleepingcomputer zufolge gelang es den Hackern bisher, Zugangsdaten von mindestens elf Unternehmen abzufischen.

Erkennbar ist der maliziöse Anhang daran, dass er in einer doppelten Dateierweiterung der folgenden Form endet: ".xlsx.html". Sie zeigt sich, wenn in den Einstellungen des Betriebssystems (betroffen sind offenbar aktuell nur Windows-Systeme) die Anzeige von Dateinamenerweiterungen aktiviert ist. Ist sie das nicht, ist Vorsicht geboten, wenn dennoch ein Mailanhang mit der Dateinamenerweiterung ".xlsx" angezeigt wird.

Nachzulesen unter:

https://www.com-magazin.de/news/hacker/hacker-nutzen-morsecode-verbreitung-malware-2631419.html
https://www.bleepingcomputer.com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/
https://www.reddit.com/r/cybersecurity/comments/le2q3v/first_time_ive_seen_this_a_malware_attachement_in

Dieser SWITCH Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.

Der SWITCH Security Report greift aktuelle Themen aus dem Bereich der Cybersecurity auf und wendet sich an interessierte Internetnutzerinnen und -nutzer, um sie für die aktuellen Gefahren zu sensibilisieren. Eine Haftung für die Richtigkeit kann trotz sorgfältiger Prüfung nicht übernommen werden.