Inhaltsverzeichnis

1 Das zweite Jahresdrittel 2021

1.1 Vorfälle und Aussendungen

Insgesamt verlief das zweite Jahresdrittel 2021 sehr Microsoft-lastig: Neben den Nachwehen von ProxyLogon, wurde mit ProxyShell eine weitere Exploit-Chain für Microsoft Exchange Server bekannt, und PrintNightmare, eine Schwachstelle im Windows Printer Spooler entwickelte sich zu einer Fortsetzungsgeschichte, in der Patch um Patch das Problem nur unzureichend beheben konnte.

Außerdem wurden teilweise uralte, schwerwiegende Lücken in der Mailserversoftware `exim` entdeckt, eine RCE in VMware vCenter gefunden und Erpressungen via DDoS versucht.

1.1.1 ProxyLogon

Die im März mit einem Notfallpatch behobene Exploit-Chain für Microsoft Exchange Server, konnte auch im zweiten Jahresdrittel nicht vollständig ad-acta gelegt werden: Die initiale Patch-Disziplin war in diesem Fall extrem hoch, wie wir z.B. in diesem Post dargelegt haben, und Ende August 2021 waren laut unseren Informationen nur noch etwa 60 von rund 2500 uns bekannten Exchange Installationen anfällig für diese Schwachstellen. Das ist insgesamt sehr erfreulich, zumal davon ausgegangen werden kann, dass einige dieser Instanzen HoneyPots sind.

Der Verlauf der verwundbaren Installationen über das zweite Jahresdrittel in Österreich wird in Abbildung 1 dargestellt.

1.1.2 21 Nägel für `exim`

Nicht nur Microsofts E-Mail-Server wurde 2021 von IT-Security ResearcherInnen ein schlechtes Zeugnis ausgestellt: Die Firma Qualys warf einen genaueren Blick auf `exim` und fand dabei 21 Sicherheitslücken, von denen einige nicht nur potentiell die Übernahme des Servers ermöglichten, sondern bereits seit dem Beginn von `exims` Git-History im Jahr 2004 ausnutzbar waren. Details dazu finden Sie im Advisory von Qualys.

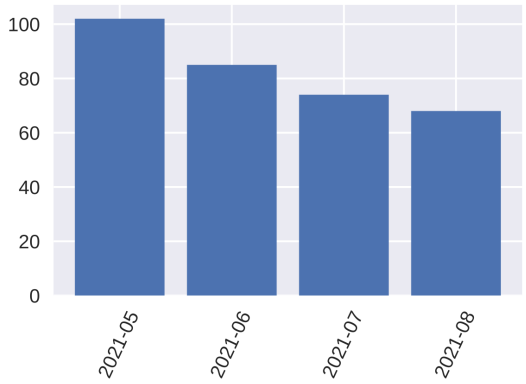

Abbildung 1: Für ProxyLogon verwundbare Exchange Server in AT

Wir veröffentlichten eine Warnung zu den Schwachstellen, führten allerdings in diesem Fall keine Scans nach potentiell Betroffenen durch, um diese direkt zu informieren. Dafür gab es zwei Gründe:

- Viele Linux-Distributionen passen den Versions-String von `exim` (und anderer Software) entsprechend ihrer eigenen Release-Zyklen an und verwenden nicht jenen von `exim` selbst. Entsprechend hätte ein einfacher Vergleich zwischen den zurückgelieferten Versions-Strings mit jenem, den `exim` für die gepatchte Version angab, zu zahlreichen False Positives geführt.
- Eine direkte Überprüfung der Lücken war aus unsere Sicht zu riskant, da hier Zugriff auf potentiell sensible Daten oder ein Systemabsturz die Folge hätten sein können.

1.1.3 VMware vCenter

Im Mai veröffentlichte VMware in VMSA-2021-0010 Workarounds und Updates zu CVE-2021-21985, einer Remote Code Execution Schwachstelle in VMware vCenter, die es AngreiferInnen ermöglichte, beliebige Befehle mit `root`-Rechten auf dem Server auszuführen. Die einzige Voraussetzung war Zugriff auf Port 443/TCP.

Wir haben daraufhin via Shodan nach allen potentiell verwundbaren Installationen in Österreich gesucht und die Betroffenen informiert.

1.1.4 DDoS Erpressungen

Im Mai und Juni gingen bei uns zahlreiche Meldungen von Unternehmen ein, dass eine Gruppe Krimineller, die sich "Fancy Lazarus" nannte, DDoS-Angriffe gegen sie durchgeführt hatte und drohte, dass wesentlich stärkere Angriffe folgen würden, wenn die Unternehmen nicht eine Lösegeldforderung von einigen BitCoins zahlen würden.[1]

Da diese Gruppe nicht nur in Österreich aktiv war, tauschten wir uns mit einigen anderen CERTs/CSIRTs im europäischen Umfeld aus und hatten entsprechend einen guten Überblick

[1] Der Name der Gruppe dürfte ein Versuch sein, die Opfer einzuschüchtern, da er sich aus Teilen von "Fancy Bear" und "Lazarus" zusammensetzt, zwei APTs (Advanced Persistent Threats) von denen angenommen wird, dass sie staatlich finanziert sind; siehe https://attack.mitre.org/groups/G0032/ und https://attack.mitre.org/groups/G0007/. Eine tatsächliche Verbindung zu diesen Gruppen ist äußerst unwahrscheinlich.

zur Vorgehensweise von “Fancy Lazarus”: Während die Initialangriffe oft gegen die authoritativen Nameserver geführt wurden und die Services betroffener Firmen dadurch von außen unerreichbar schienen, waren die angedrohten Folgeangriffe auch nach Ablauf der Zahlungsfrist nirgends durchgeführt worden. Diese Erkenntnisse sowie Tipps, wie sich Unternehmen generell auf DDoS-Angriffe vorbereiten können, veröffentlichten wir in einer Warnung.

Uns ist nach wie vor kein Fall bekannt, in dem die Gruppe ihre Drohung wahr machte und tatsächlich stärkere Folgeangriffe durchführte.

1.1.5 PrintNightmare

Am 8. Juni veröffentlichte CERT/CC eine technisch detaillierte Beschreibung von CVE-2021-1675, einer Remote Code Execution Schwachstelle im Windows Print Spooler die im Zuge des Juni-Updates für Microsoft Windows behoben worden war.

Allerdings stellte sich schnell heraus, dass der Patch nicht ausreichend war und innerhalb kurzer Zeit tauchte Exploit-Code auf. Microsoft erklärte daraufhin, dass der Patch sehr wohl wirksam sei und es sich um eine neue, lediglich ähnliche Lücke handle, für die auch eine neue CVE (CVE-2021-34527) vergeben wurde. Diese erhielt dann auch explizit den Namen “PrintNightmare” und wurde offiziell in den Juli-Updates von Microsoft behoben, aber wiederum konnten Security-ResearcherInnen innerhalb kurzer Zeit zeigen, dass die Probleme nicht vollständig behoben waren.

Microsoft vergab wiederum neue CVE-Nummern für diese Lücken (CVE-2021-34481, CVE-2021-36936, und CVE-2021-36947), die am Microsoft Patchday im August behoben werden sollten. Security Researcher und Entwickler von `mimikatz`, Benjamin Delpy, zweifelte deren Wirksamkeit jedoch noch am Tag des Erscheinens der Patches an, da `mimikatz`’s Exploit nach wie vor funktionierte.

Als Reaktion veröffentlichte Microsoft einen Tag nach dem August Patchday mit CVE-2021-36958 eine weitere CVE-Nummer, für die lediglich ein Workaround zur Verfügung gestellt wurde, der schlicht darin besteht, den Print Spooler Service zu deaktivieren, was in vielen Unternehmen nicht möglich ist.

Wir verfassten dazu eine mehrmals aktualisierte Warnung und hoffen, dass wir uns von diesen Schwachstellen im September endgültig verabschieden dürfen.

1.1.6 ProxyShell

Im Zuge der Blackhat 2021 USA hielt der Security-Researcher Orange Tsai einen Vortrag mit dem Titel “ProxyLogon is Just the Tip of the Iceberg” (die Folien dazu finden Sie auf der Webseite der Blackhat; ein Blogpost von Orange Tsai mit technischen Details erschien kurz darauf bei der Zero Day Initiative) in dem er generell die Angriffsmöglichkeiten auf Microsoft Exchange Server vorstellte und spezifisch eine neue Exploit-Chain präsentierte, über die AngreiferInnen über das Netzwerk beliebige Befehle als `NT Authority\SYSTEM` ausführen konnten, ohne über gültige Zugangsdaten zu verfügen. Diese “ProxyShell” genannte Kombination von Schwachstellen ist damit ebenso katastrophal wie ProxyLogon vom März 2021. Der einzige Unterschied bestand darin, dass ProxyShell zum Veröffentlichungszeitpunkt noch nicht aktiv ausgenutzt und die dazugehörigen Lücken bereits in den Exchange-Updates von April bzw. Mai 2021 behoben worden waren.

Kurz danach veröffentlichte der Sicherheitsforscher Kevin Beaumont ein `nmap` Script, mit dessen Hilfe verwundbare Server identifiziert werden konnten, es wurde aktiv nach verwundbaren Servern gescannt und bald darauf wurden auch erste Angriffe bekannt.

Wir haben daraufhin die Logik von Kevin Beaumonts `nmap` Script in Python implementiert und einen zusätzlichen Test über die Versionsnummer eingebaut, anschließend alle uns bekannten Exchange Server in Österreich überprüft und die Abuse-Kontakte aller potentiell verwundbaren Installation kontaktiert. Die ersten Ergebnisse haben wir auf unserer Webseite beschrieben. Im Laufe des Augusts haben wir einige weitere Scans und Aussendungen durchgeführt. Die Entwicklung der verwundbaren Server in Österreich, sieht dabei wie folgt aus:

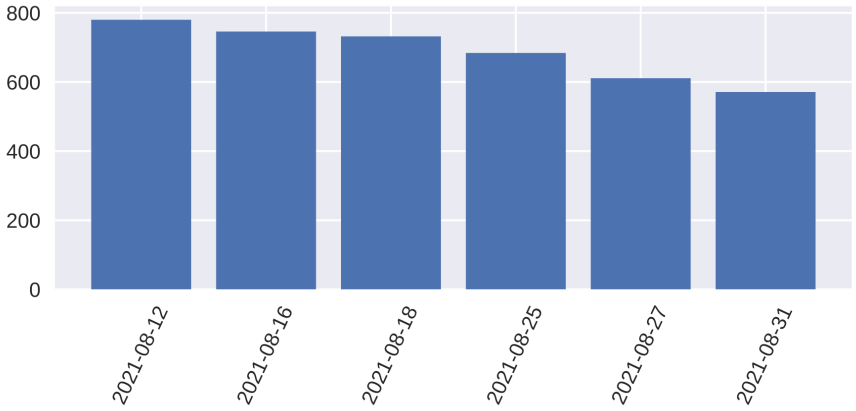

Abbildung 2: Für ProxyShell anfällige Exchange Server in AT

1.1.7 ProxyToken

Kurz vor Ende des zweiten Jahresdrittels wurde mit CVE-2021-33766 eine weitere schwere Schwachstelle in Microsoft Exchange Servern gefunden, die, der aktuellen Namenskonvention folgend, "ProxyToken" genannt wurde und in einer Veröffentlichung der Zero Day Initiative näher beschrieben wird. Es ist allerdings festzuhalten, dass es sich hierbei um eine einzelne Lücke handelt, nicht um eine ganze Exploit-Chain wie bei ProxyLogon und ProxyShell.

Obwohl ProxyToken zwar nicht zu einer Remote Code Execution als `NT Authority\SYSTEM` führt, sondern AngreiferInnen "nur" die Re-Konfiguration beliebiger Postfächern ohne Authentifizierung erlaubt, ist sie dennoch extrem gefährlich: Sie müssen lediglich wissen, dass ein Postfach existiert, um z.B. eine Weiterleitung zu einer E-Mail-Adresse unter ihrer Kontrolle einzurichten.

ProxyToken wurde im Zuge von Microsofts Patchday im Juli 2021 behoben,[2] öffentliche Exploits waren aber bald nach Erscheinen des oben erwähnten Posts von ZDI verfügbar.

1.2 Projekte und Vorträge

1.2.1 MeliCERTes 2 (SMART-2018-2014)

Nachdem die Anforderungen an die Single-Sign-On Lösung für das CSIRTs Network (CNW) fertig ausdefiniert waren, wurde eine Studie erstellt, wie gut diverse Open Source Lösungen diese er-

[2] Um diesen Umstand gibt es etwas Verwirrung, denn Microsofts Advisory zu CVE-2021-33766 schreibt, dass bereits die Updates im April das Problem behoben hatten, allerdings darauf vergessen wurde, die CVE-Nummer dort anzuführen. Entsprechend dürften auch Exchange Server mit Patchstand April 2021 gegen die Lücke abgesichert sein, wir konnten dies aber nicht testen.

füllen können. Dabei wurden die Dokumentationen, der Status (Projektaktivität, Verfügbarkeit von kommerziellem Support, etc.) sowie der Security Track Record miteinbezogen.

Von den Top Drei (WSO2, Keycloak, Gluu) wurden anschließend Testinstallationen durchgeführt, um die Anbindung der relevanten Applikationen zu testen. Dabei hat sich herausgestellt, dass die Integration von SharePoint am problematischsten ist: Die On-Premise Version unterstützt nur WS-Fed (Web Services Federation), und wird ADFS (Active Directory Federation Services) als Integrationslayer eingesetzt, zeigt sich, dass auch dort die Unterstützung für SAML (Security Assertion Markup Language) und OIDC (OpenID Connect), zwei weit verbreiteten Standards auf diesem Gebiet, mangelhaft und veraltet ist. Dieser Umstand spiegelt deutlich Microsofts Strategie wider, KundInnen zur Nutzung der Cloud-Services zu drängen, während die Unterstützung aktueller, offener Standards in den On-Premise Varianten keine Priorität hat. Das CSIRTs Network kann sich diesen Vendor Lock-in auf Dauer nicht leisten.

Im Sommer wurde dann ausgiebig an den Verfügbarkeitserwartungen des CSIRTs Network bzgl. der von der ENISA betriebenen Systemen gearbeitet. Dazu gab es eine Umfrage im CNW, welche Ausfallszeiten für welche Services akzeptabel sind. Eingeteilt in Bürozeiten/außerhalb, Kern- und Zusatzservices und Normalbetrieb versus Krisenmodus des CNW ergab das in Summe acht Werte für die angestrebten Wiederanlaufzeiten. Während die CSIRTs solche Verfügbarkeitsanforderungen gewohnt sind (die auch von der NIS Direktive abgeleitet werden), hatte die ENISA bis zum EU Cyber Security Act von 2019 keine operativen Aufgaben und daher auch keinen Bedarf für einen hochverfügbaren IT Betrieb. Inzwischen kamen mit dem neuen Mandat operative Aufgaben dazu und es wurde klar, dass die Rolle des Sekretariats für das CSIRTs Network und das Cyber Crisis Liaison Organisation Network (CyCLONe) sich nicht nur auf die Organisation von Meetings beschränkt, sondern auch den Betrieb von IT Infrastruktur erfordert. Das MeliCERTes 2 Konsortium hilft der ENISA bei der Umstellung auf diese neuen Anforderungen.

Davon unabhängig wurden auch wieder Workshops und Trainings zu IntelMQ für die Mitglieder des CNW abgehalten.

1.2.2 “Enhancing Cybersecurity in Austria” (2018-AT-IA-0111)

Da dieses Projekt mit Ende August 2021 auslief, war die Arbeit im zweiten Jahresdrittel auf den Projektabschluss und die dabei abzugebenden Berichte fokussiert.

Trainings und Konferenzen Wie auch im Vorjahr wurden die FIRST Conference und das dazugehörige Capture The Flag (CTF) Event 2021 online abgehalten. Thomas Pribitzer, Dimitri Robl und Sebastian Waldbauer von CERT.at nahmen als Team am CTF teil und belegten am Ende den 9. Platz von 42. Teams. Dazu gibt es auch ein längeres Writeup auf Englisch.

Im Juli besuchte Thomas Pribitzer SANS SEC402: Cybersecurity Writing: Hack the Reader als on-demand online Kurs. Im August absolvierte Dimitri Robl das Windows Host Security Training des InfoSec Institutes und Thomas Pribitzer schloss deren CompTIA Network+ Learning Path ab.

Auch wenn es weiterhin COVID-19-bedingt kaum möglich war, physische Konferenzen zu besuchen, so konnten wir im Rahmen dieses CEF-Projekts am 63. TF-CSIRT Meeting im Mai und am 14. CSIRTs Network Meeting im Juni jeweils virtuell teilnehmen.

Außerdem organisierte und leitete Otmar Lendl im Juni einen Hackaton zum Thema RTIR-Statistiken für die Mitglieder des CSIRTs Network.

Tooling Am 2. Juli wurde mit IntelMQ 3.0.0 eine rundum überarbeitete Version von IntelMQ veröffentlicht und damit auch ein wesentlicher Milestone für das Projekt erreicht. Einen Über-

blick zu den Änderungen und Umbauten finden Sie auf unserem Blog.

Neben IntelMQ 3.0 wurde zeitgleich die erste stabile Version von ”Tuency”, unserem neuen “Constituency-Portal”, veröffentlicht. Das Portal ist ein Kontaktmanagementtool mit Self-Service Funktionen und verwendet als Authentifizerungslösung Keycloak. Dadurch können die dort hinterlegten Zugangsdaten auch bei anderen, zukünftigen Diensten verwendet werden. Das Portal verbessert und erweitert außerdem die Adressierung unserer täglichen E-Mailbenachrichtigungen an NetzbetreiberInnen über Probleme in deren Netzen, die wir via IntelMQ ausschicken. Eine genauere Beschreibung der Funktionen finden Sie in unserem Blogpost dazu. Der Source-Code von Tuency ist öffentlich auf GitLab einsehbar. Vor der Veröffentlichung wurde ein Pentest durch Externe durchgeführt, der kleine Verbesserungsmöglichkeiten fand, insgesamt aber das sichere Design und die robuste Ausführung des Projekts bestätigte.

Außerdem haben wir im zweiten Jahresdrittel umgesetzt, dass unsere öffentlichen Datenfeeds via IntelMQ in unser SIEM eingespeist werden. Entsprechend ist es jetzt möglich, dessen Logs mit den Feeds zu korrelieren und effizienter auf Probleme zu reagieren.

Ebenfalls abschließen konnten wir die Integration der MeliCERTes Plattform, unter anderem durch die Installation von Cerebrate. Diese Software ermöglicht allen Mitgliedern des CSIRTs Network, eine gemeinsame Authentifizierungslösung zu betreiben. Für die erfolgreiche Umsetzung war es notwendig, im IT Betrieb technische Grundlagen und Kompetenzen zu schaffen und auszubauen.

Als finalen “Test” für die Integration von MeliCERTes führten wir gemeinsam mit CERT.ee den ersten erfolgreichen Inter-Operability Test zwischen zwei MeliCERTes Installationen durch.

1.2.3 Vorträge

- Im April moderierte Wolfgang Rosenkranz die Vorstellung der Ergebnisse der letzten Cyber Security Studie des Kuratorium Sicheres Österreich (KSÖ).
- Im Mai präsentierte Sebastian Wagner IntelMQ 3.0 und die damit einhergehenden Veränderungen am 63. TF-CSIRT Meeting.
- Im gleichen Monat hielt Birger Schacht einen interaktiven Workshop zu IntelMQ im Rahmen des MeliCERTes 2 Projekts.
- Im Juni hielt Dimitri Robl an der Universität Wien einen Gastvortrag im Zuge der Lehrveranstaltung “Network Security”.
- Im August sprach Dimitri Robl vor dem Fachausschuss für Informationstechnologie des Städtebunds über die aktuelle Lage in der IT-Sicherheit, welche Bedrohungen 2021 besonders wichtig waren und welche wohl oder übel noch länger relevant bleiben werden. Außerdem wurde besprochen, wie die Zusammenarbeit zwischen GovCERT Austria und dem Städtebund intensiviert werdenn könnte.