2. November 2021 | Nationales Zentrum für Cybersicherheit NCSC

Halbjahresbericht 2021/I (Januar-Juni)

Informationssicherung

Lage in der Schweiz und International

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

1 Übersicht / Inhalt

1 Übersicht / Inhalt 2
Management Summary 4
2 Editorial 5
3 Fokus: Schwachstellen 7
3.1 Prominente Schwachstellen des ersten Halbjahres 2021 7
3.1.1 Microsoft Exchange: ProxyLogon 7
3.1.2 PulseSecure und SonicWall 9
3.1.3 Accellion 10
3.1.4 PrintNightmare 10
3.1.5 QNAP NAS 11
3.1.6 Dell-BIOSConnect Schwachstellen 12
3.1.7 Bad Alloc 13
3.2 Software-Management: Inventar und Update-Prozesse 13
3.3 Schwachstellenmanagement aus Sicht des NCSC 15
3.4 Bug Bounty-Programm der Bundesverwaltung 16
4 Ereignisse / Lage 16
4.1 Eingegangene Meldungen zu Cybervorfällen – Überblick 16
4.1.1 Meldungen zu Betrug 18
4.1.2 Meldungen zu Phishing 18
4.1.3 Meldungen zu Malware 19
4.2 Schadsoftware / Malware 19
4.2.1 Malware-Verbreitung 19
4.2.2 Dual-Use-Software «Cobalt Strike» 23
4.2.3 Ransomware 24
4.3 Angriffe auf Websites und -dienste 26
4.3.1 DDoS 26
4.3.2 Webseitenkompromittierungen 28
4.4 Industrielle Kontrollsysteme & OT 29
4.4.1 «RedEcho» infiltriert indische Stromversorgung 29
4.4.2 Manipulationsversuche bei Wasserversorgung in Florida 30
4.5 Datenabflüsse 31
4.5.1 SITA: Diebstahl von Passagierdaten 31
4.5.2 Angriffe auf Social Networks und Data Scraping 31

4.6 Spionage **33**
4.6.1 Nobelium: neue Kampagnen nach SolarWinds 33
4.6.2 «Hafnium» nutzt MS Exchange aus 33
4.7 Phishing und Social Engineering **34**
4.7.1 Phishing 34
4.7.2 Smishing 35
4.7.3 Social Engineering 35
4.8 Betrug: Aktuelle Varianten von Investitionsbetrug **36**

Management Summary

Der zweite Halbjahresbericht des Nationalen Zentrums für Cybersicherheit (NCSC) befasst sich mit den wichtigsten Cybervorfällen der ersten Jahreshälfte 2021 in der Schweiz und international. Das Schwerpunktthema widmet sich den Schwachstellen bei IT-Systemen, die für Cyberangriffe ausgenützt werden können.

Schwachstellen bei Hard- und Software sind willkommene Angriffsziele, wenn die lückenhaften Komponenten nicht zeitnah durch Patches aktualisiert werden. Die Sicherheitslücken auf den MS Exchange-Servern sowie «Sonic Wall», «PrintNightmare» oder «QNAP NAS» sind nur einige Beispiele, die im aktuellen Fokusthema beleuchtet werden.

Ausbau des Schwachstellen-Managements

Das NCSC baut das Schwachstellen-Management aus, so dass Sicherheitslücken auf einer Plattform koordiniert offengelegt werden können («Coordinated Vulnerability Disclosure»), aber auch um Entdeckenden von Sicherheitslücken die Möglichkeit zu geben, ihre Erkenntnisse anonym an eine staatliche Stelle zu melden. Zudem wird die Öffentlichkeit über die im Umlauf befindlichen kritischen Sicherheitslücken informiert und mit entsprechenden Sicherheitsmassnahmen unterstützt. Um Sicherheitslücken aufzuspüren, hat das NCSC im ersten Halbjahr 2021 die Testphase der Infrastruktur für das Covid-Zertifikat und das erste Pilot-Programm betreffend Bug Bounty in der Bundesverwaltung eng begleitet.

Häufigste Meldungen zu Betrug

Auch im ersten Halbjahr 2021 betrafen die meisten Meldungen an das NCSC verschiedenste Betrugsformen. Insbesondere CEO-Betrug, Fake-Support-Anrufe und Kleinanzeigenbetrug wurden sehr häufig gemeldet. Investitionsbetrüger locken aktuell mit enormen Gewinnversprechen bei Anlagen in Kryptowährungen. Insgesamt sind im Berichtszeitraum bei der Anlaufstelle des NCSC 10’234 Meldungen zu diversen Cybervorfällen eingegangen. Dies sind fast doppelt so viele wie im ersten Halbjahr 2020. Gründe für diese starke Zunahme sind einerseits die Einführung des neuen Meldeformulars des NCSC und dessen prominente Platzierung auf der Startseite. Andererseits ist die hohe Zahl auch auf mehrere grosse Angriffswellen mittels Fake-Sextortion oder Phishing zurückzuführen.

Anstieg von Meldungen zu Ransomware und Phishing

Die hohe Zahl an gemeldeten Vorfällen mit Verschlüsselungstrojanern, sogenannter Ransomware, ist ebenfalls auffällig. Die Zahl hat sich von 32 Fällen im ersten Halbjahr 2020 auf 94 Fälle in der aktuellen Berichtsperiode verdreifacht. Zurückzuführen ist dies vor allem auf die Ransomware «Qlocker», welche sich mehrheitlich gegen Private richtete und es auf Netzwerkspeicher der Marke «QNAP» abgesehen hatte.

Eine starke Zunahme verzeichnete das NCSC auch bei den Phishing-Meldungen. Wurden im ersten Semester 2020 über das Meldeformular noch 497 Hinweise zu Phishing gemeldet, waren es im Jahr 2021 in der gleichen Periode 2'439 Meldungen. Diese Zahl hat sich fast verfünffacht. Der Grund liegt vor allem am erhöhten Meldeeingang von E-Mails und SMS mit gefälschten Paketbenachrichtigungen, deren Versand in den letzten Monaten stark zugenommen hat.

2 Editorial

Partizipative Sicherheit – Gemeinsam erfolgreich für Cybersicherheit sorgen

Liebe Leserin, lieber Leser,

Die Cybersicherheit hat sich gewandelt. Noch vor Jahren war dies eine Spezialdisziplin in der IT, die sich hauptsächlich mit dem Schutz von Daten und Systemen beschäftigt hat. Die Unternehmen waren froh, dass es Mitarbeitende gab, die sich um diese Aspekte kümmerten. Aufgefallen sind sie meist nur dann, wenn eine Firewall die Funktion eines Systems behinderte. Es kam vor, dass bei solchen Vorfällen gleich die Firewall als Ganzes deaktiviert wurde, denn schliesslich stand sie nur im Weg und wirklich passiert war ja noch nie etwas.

Abb. 1: Marcel Zumbühl, Konzern CISO Post und Co-Präsident ISSS

Diese Zeiten sind vorbei! Cybersecurity ist bei allen Unternehmen und Institutionen zu einem Mainstream-Risiko geworden, mit dem sich nebst dem Management auch der Verwaltungsrat beschäftigen muss. Sie ist zu einem Wirtschaftsfaktor in einer vernetzten digitalen Welt geworden. Kundinnen und Kunden fragen heute kritisch nach, ob sie einem digitalen Dienst vertrauen können und ob das jeweilige Unternehmen das Thema ernst nimmt. Und Cybersecurity ist nicht eine Disziplin in der nur Grossfirmen fit sein müssen. Gerade die kleineren und mittleren Unternehmen in unserem Land sind zur Zielscheibe von Kriminellen geworden, weil sie hier das schnelle Geld wittern und glauben, sie würden auf wenig Widerstand stossen. Die Betrügenden rechnen sich aus, dass sich Unternehmen vor negativer Presse fürchten und auch davor, in aller Öffentlichkeit bloss gestellt zu werden.

Zum Glück wendet sich auch in diesem Aspekt das Blatt. Wir lernen, dass erfolgreiche Sicherheitsattacken in erster Linie kriminelle Handlungen sind. Es interessiert nicht, ob man sich besser hätte schützen sollen, sondern dass die Schuldigen gefunden und angeklagt werden. Wir lernen, dass wir nicht die Opfer, sondern die Täterinnen und Täter ächten müssen. Zudem lernen wir, dass wir auch bei Erpressungsangriffen nicht aus Angst vor Reputationsschaden versuchen sollen, den Tätern Lösegeld zu zahlen. Nicht zuletzt, weil Unternehmen die Erpressungsgelder bezahlen, in 80% der Fälle nochmals zur Kasse gebeten werden, wie eine aktuelle Studie der Firma Cybereason zeigt.

Wir müssen lernen, uns in der Cybersecurity zu vernetzen. Das Schlagwort der Stunde heisst «Partizipative Sicherheit». Unternehmen lernen, dass Cybersecurity nicht von einer Nischenabteilung betrieben wird, sondern natürlicher Bestandteil von Applikations- und Systementwicklungen ist. In agilen DevSecOps-Entwicklungsmodellen spielen zum Beispiel Entwicklerinnen und Entwickler eine entscheidende Rolle. Bei der Schweizerischen Post treibt ein Team von engagierten «Security Champions» das Thema Sicherheit in allen entscheidenden Vorhaben voran.

Nicht nur die Communities im Innern des Unternehmens, sondern auch ausserhalb helfen, die Sicherheit voranzutreiben. Vertrauenszirkel und Austauschplattformen zwischen Sicherheitsexpertinnen und -experten unterschiedlicher Organisationen bestehen seit jeher und oft kommt es vor, dass Fachleute sich nicht nur in einer Austauschgruppe sondern in mehreren vernetzen. Gemeinsam entstehen hier Ideen und «Best Practices», Fachleute lernen voneinander und sind so den Angreifenden jeweils eine Nasenlänge voraus.

Die Zusammenarbeit mit ethischen Hackerinnen und Hackern ist ein relativ neues Phänomen und führt den Ansatz der Partizipativen Sicherheit auf ein höheres Level. Unternehmen laden Hackerinnen und Hacker ein, Onlinedienste auf Herz und Nieren zu testen und anzugreifen. Wer eine Lücke findet, wird belohnt. Die Post setzt diesen Ansatz der Partizipativen Sicherheit seit 2019 ein und das Programm ist weltweit zugänglich. Nicht nur Online-Dienste, wie die digitale Briefmarke «Webstamp» und die Post-App werden so auf einem hohen Sicherheitsniveau gehalten. Mittlerweile profitieren auch die digitalen Gesundheitssysteme und elektronische Abstimmungsservices von dieser neuen Technik der Fehlerfindung und -elimination. Uns ist klar, dass wir Fehler im Verbund mit internen und externen Expertinnen und Experten früh entdecken und beheben können. Keine Software ist ohne Fehler und wir setzen alles daran, die Fehler rechtzeitig zu kennen.

In diesem Verbund der Partizipativen Sicherheit leistet das Nationale Zentrum für Cybersicherheit (NCSC) der Schweiz unschätzbare Dienste. Die Fachleute des Bundes helfen, Unternehmen wie der Post, Bedrohungen rechtzeitig zu erkennen und abzuwenden und von anderen Instituten zu lernen. Die Berichte des NCSC gehören zur Pflichtlektüre aller Sicherheitsexpertinnen und -experten und ich danke dem NCSC an dieser Stelle für ihren grossartigen Einsatz im Sinne der Partizipativen Sicherheit der Schweiz.

Marcel Zumbühl, Konzern CISO Post und Co-Präsident ISSS

3 Fokus: Schwachstellen

3.1 Prominente Schwachstellen des ersten Halbjahres 2021

3.1.1 Microsoft Exchange: ProxyLogon

Die Sicherheitsfirma Volexity stellte Anfang Jahr Angriffe fest, die mehrere Schwachstellen in der Exchange-Server Software von Microsoft ausnutzten.[1] Dies bewog Microsoft zu einer ausserordentlichen Veröffentlichung von Sicherheitsupdates am 2. März 2021.[2] US-Sicherheitsbehörden warnten bereits am Folgetag vor laufenden Angriffen über diese Schwachstellen durch chinesische staatliche Akteure.[3]

Die betreffende Angriffskette besteht aus vier zuvor unbekannten Schwachstellen. Sowohl die kritische Schwachstelle, die am Anfang der Angriffskette steht, als auch die ganze Angriffskette wird mit dem Titel «ProxyLogon» bezeichnet.[4]

Die Angriffskette betraf Microsoft Exchange-Server 2013, 2016 und 2019 und erforderte eine Verbindung auf den für gesicherte HTTPS-Verbindungen zuständigen Port 443 des Exchange-Servers. Zu Beginn der Angriffskette steht die Ausnutzung einer Schwachstelle, die «Server-Side-Request-Forgery (SSRF)» ermöglicht: Sie erlaubt es Angreifenden, beliebige HTTP-Anfragen zu versenden und sich als Exchange-Server zu authentifizieren. Die Schwachstelle wurde als kritisch eingestuft, da sie die nachfolgende Ausnutzung der anderen Schwachstellen erst ermöglicht.[5] Der Schweregrad der weiteren drei Schwachstellen wurde als hoch eingestuft, denn sie erlauben das Ausführen von Code auf der Infrastruktur des Opfers sowie das Auslesen und Schreiben von Dateien.[6]

Die Ausnutzung dieser Angriffskette ermöglicht es Angreifenden, die Authentifizierung zu umgehen und sich als Administrator auszugeben. Somit ist es möglich, völlige Kontrolle über den Exchange-Server zu übernehmen und den E-Mail-Verkehr, Kalenderdaten, Kontaktangaben und Aufgaben auszulesen und zu manipulieren. Häufig fungieren Exchange-Server auch als Domänencontroller zur Authentifizierung von Computern und Benutzern im Netzwerk. Exchange-Server stellen deshalb ein hochwertiges Ziel für Angreifende dar.

Die Angriffskette wurde ab ihrem Bekanntwerden im März nicht nur von weiteren staatlichen Cyberakteuren ausgenutzt, sondern auch zunehmend von Kriminellen missbraucht, unter anderem zur Verbreitung von Ransomware.[7] Verschiedentlich platzierten Akteure auch bloss eine Webshell und damit eine Hintertür auf verwundbaren Systemen, um auch nach allfälligen

---

1 Vgl. Operation Exchange Marauder (volexity.com) und ProxyLogon (proxylogon.com)

2 On-Premises Exchange Server Vulnerabilities Resource Center (microsoft.com)

3 Mitigate Microsoft Exchange Server Vulnerabilities (cisa.gov); siehe auch unten Kap. 4.6.2.

4 ProxyLogon (proxylogon.com)

5 NVD - CVE-2021-26855 (nist.gov)

6 Mehr Informationen zu den zwei Post-authentification-file-write Schwachstellen und der Deserialisierungs-Schwachstelle finden Sie unter NVD - CVE-2021-26857 (nist.gov), NVD - CVE-2021-26858 (nist.gov) und NVD - CVE-2021-27065 (nist.gov)

7 Z. B. die auch als DoejoCrypt bekannte DearCry (fraunhofer.de) und BlackKingdom (fraunhofer.de)

Updates noch Zugriff zu haben und später Angriffe ausführen zu können. Dies machte für Systembetreiberinnen neben den Updates auch die Analyse von Logs und forensische Untersuchungen nötig, um solche Webshells zu finden und zu entfernen. Das US-Justizministerium autorisierte sogar behördliche Eingriffe bei Opfern zur Bekämpfung dieser Angriffe.[8] In der Schweiz wurden Anfang März hunderte von ungepatchten Servern festgestellt, welche für solche Angriffe verwundbar waren. Das NCSC informierte die betroffenen Unternehmen und empfahl dringend, die Systeme zu aktualisieren und auf Kompromittierung zu prüfen.[9]

Empfehlungen:

Zum besseren Schutz von Exchange-Server-Infrastrukturen empfiehlt das NCSC generell die Implementierung folgender Sicherheitsvorkehrungen:

- Exchange-Server dürfen nicht direkt aus dem Internet erreichbar sein. Schalten Sie entweder eine WAF (Web Application Firewall) vor oder setzen Sie einen SMTP-Filtering-Proxy vor den Exchange-Server.
- Erstellen Sie einen Prozess zur notfallmässigen Einspielung von Sicherheitsupdates und stellen Sie sicher, dass Updates innerhalb weniger Stunden eingespielt werden können. Dies gilt in erster Linie für alle Systeme, die direkt vom Internet aus erreichbar sind.
- Stellen Sie durch ein Life Cycle Management sicher, dass Sie nur Versionen verwenden, die vom Hersteller (vorliegend Microsoft) mit Sicherheitsupdates versorgt werden.
- Überwachen Sie alle Exchange-Server Logfiles genau, sammeln Sie diese in einem SIEM (Security Information and Event Management) und durchsuchen Sie diese nach unüblichen Mustern.
- Richten Sie auf allen Systemen eine Zwei-Faktoren-Authentisierung für sämtliche Nutzer ein.
- Verwenden Sie ein dediziertes Management Framework für den Zugriff auf Exchange-Server mit hohen Privilegien.
- Zeichnen Sie alle Active Directory-Logs zentral auf und analysieren Sie diese regelmässig.
- Erhöhen Sie die Sichtbarkeit Ihrer Endpunkte durch Einsatz eines EDR-Tools (Endpoint Detection and Response).

Weitere Informationen und Empfehlungen finden Sie auf unseren Websites:

Exchange Vulnerability 2021 (govcert.admin.ch)

Schwachstelle bei Exchange-Servern (ncsc.admin.ch)

Microsoft schliesst weitere Lücken in Exchange-Servern (ncsc.admin.ch)

---

8 Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities (justice.gov)

9 Exchange Vulnerability 2021 (govcert.admin.ch); Schwachstelle bei Exchange-Servern (ncsc.admin.ch); Microsoft schliesst weitere Lücken in Exchange-Servern (ncsc.admin.ch).

3.1.2 PulseSecure und SonicWall

Am 20. April 2021 wurden kritische Verwundbarkeiten in zwei Produkten für Fernzugriffe bekannt, welche die Herstellerinnen PulseSecure und SonicWall betrafen. Das NCSC hat über die Bedrohungen öffentlich informiert und Empfehlungen herausgegeben.[10]

PulseSecure: Der Sicherheitsdienstleister FireEye berichtete über fortschrittliche Angriffe, bei welchen eine bisher unbekannte Schwachstelle in einem Produkt von PulseSecure ausgenutzt wurde und gab an, dass zwölf verschiedene Malware-Typen über diesen Weg verbreitet wurden.[11] Die betreffende Schwachstelle erlaubt einer nicht authentifizierten Person aus der Distanz die Ausführung von beliebigem Code via dem SSL-VPN-Produkt «PulseSecure Connect». Während zuerst nur ein Workaround zur Absicherung existierte, publizierte PulseSecure am 3. Mai dann den Patch für die betreffende Schwachstelle sowie für drei weitere Sicherheitslücken.[12] Forscher fanden allerdings heraus, dass der Patch die Lücken nicht vollständig schloss.[13] PulseSecure stellte am 16. Juni ein Tool bereit, um Installationen der Software auf ihre Integrität zu überprüfen.[14]

SonicWall: Auch im Produkt «SonicWall Email Security» von SonicWall wurden eine Reihe von Schwachstellen bekannt, deren gemeinsame Ausnutzung administrativen Zugriff und das Ausführen von Code auf dem Zielsystem erlaubte.[15] FireEye berichtete, dass die Schwachstellen zwecks Kompromittierung von Unternehmensnetzwerken ausgenutzt wurden.[16] SonicWall stellte am 20. April 2021 Patches bereit.[17]

Schlussfolgerung / Empfehlungen:

Schwachstellen in Produkten, die Fernzugriffe ermöglichen, bieten aufgrund ihrer Funktionalität sehr grosses Missbrauchspotenzial.

Für alle Logins sollte eine Zwei-Faktor-Authentisierung eingerichtet werden. Einfache Logins mit lediglich einem Faktor (Benutzername-Passwort-Kombination) bieten zu wenig Schutz und sollten technisch unterbunden werden.

Produkte für Fernzugriffe müssen so konfiguriert werden, dass sowohl erfolgreiche wie auch fehlgeschlagene Zugriffsversuche aufgezeichnet werden (Logging). Fernzugriffe müssen zudem überwacht werden, damit ungewöhnliche Aktivitäten auffallen und bei Missbrauch in nützlicher Frist angemessene Gegenmassnahmen ergriffen werden können.

---

10 Kritische zero-day Verwundbarkeiten in Pulse Secure und SonicWall Produkten (ncsc.admin.ch)
11 Check Your Pulse (mandiant.com); Re-Checking Your Pulse (mandiant.com).
12 Pulse Security Advisory: SA44784 - 2021-04 (pulsesecure.net)
13 Technical Advisory: Pulse Connect Secure (nccgroup.com)
14 Pulse Secure Article: KB44755 - Pulse Connect Secure (PCS) Integrity Assurance (pulsesecure.net)
15 Kritische zero-day Verwundbarkeiten in Pulse Secure und SonicWall Produkten (ncsc.admin.ch)
16 Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise (mandiant.com)
17 Security Notice: SonicWall Email Security Zero-Day Vulnerabilities (sonicwall.com)

3.1.3 Accellion

Die Filesharing-Software «Accellion File Transfer Appliance (FTA)» stand kurz vor dem «End of Life», als sie im Dezember 2020 von Akteuren im Umfeld der Ransomware «Clop» angegriffen wurde.[18] Über verschiedene Schwachstellen gelangten die Angreifenden an Daten von bis zu 320 Kundinnen und Kunden von Accellion[19] und drohten mit der Veröffentlichung im Dark Web, sollte kein Lösegeld bezahlt werden. Zu den Opfern in mehreren Ländern gehörten grosse Institutionen wie die Reserve Bank Neuseelands oder die Washington-State Finanzkontrolle. Auch sechs Monate nach dem Vorfall werden noch regelmässig Opfer bekannt; ein unschönes Ende der Karriere eines Produktes.[20] Die Mitteilung von Accellion über die Schwachstellen und entsprechenden Patches haben die Kundinnen und Kunden offenbar zu spät erreicht.[21]

Schlussfolgerung / Empfehlung:

Eingesetzte Software muss jederzeit aktuell gehalten werden. Dies gilt für anbietende wie auch für anwendende Unternehmen. Wenn bei einem Produkt absehbar ist, dass es vom Hersteller nicht mehr unterhalten werden wird, sollte umgehend der Ablösungsprozess lanciert werden, damit die Nachfolgelösung weder zu spät kommt, noch unter Zeitdruck organisiert und implementiert werden muss. Der Einsatz von Software nach ihrem «End of Life» respektive «End of Support» stellt für Unternehmen und Private ein hohes Sicherheitsrisiko dar.

3.1.4 PrintNightmare

Am 8. Juni 2021 veröffentlichte Microsoft ein Sicherheitsupdate, um die Sicherheitslücke «PrintNightmare» in der Drucker-Warteschlange (dem sog. «Print Spooler») zu schliessen.[22] Kurz danach wurden weitere Verwundbarkeiten bekannt, die ebenfalls den Druckspooler betrafen.[23] Die gefundenen Schwachstellen konnten von Angreifenden insbesondere auch für laterale Bewegungen in Netzwerken verwendet werden, was sich auch Ransomware-Gruppen zunutze gemacht haben.[24]. Bis Microsoft zur Behebung ausserordentliche Sicherheitsupdates publizieren konnte, wurde als Massnahme das Deaktivieren des Druckspoolers auf Systemen empfohlen, mit welchen nicht gedruckt werden müsse. Dazu gehören typischerweise Domänencontroller wie auch viele Server-Systeme.[25]

---

18 Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion (mandiant.com)
19 Accellion FTA Attack Customer FAQs (accellion.com)
20 Accellion Announces End of Life (EOL) for its Legacy FTA Product (accellion.com)
21 Vulnérabilité Accellion FTA : les notifications en question (lemagit.fr)
22 CVE-2021-1675 – Sicherheitsanfälligkeit im Windows-Druckerspooler (microsoft.com)
23 CVE-2021-34527 – Sicherheitsanfälligkeit im Windows-Druckerspooler (microsoft.com)
24 Ransomware: Now attackers are exploiting Windows PrintNightmare vulnerabilities (zdnet.com)
25 CVE-2021-1675: Incomplete Patch and Leaked RCE Exploit (sans.edu)

Das NCSC hat die Bevölkerung über die Bedrohung informiert und Empfehlungen herausgegeben.[26]

Schlussfolgerung / Empfehlung:

Um die Angriffsfläche zu reduzieren, sollten Standarddienste auf Systemen, die diese nicht benötigen, grundsätzlich deaktiviert werden. Dies sollte im Rahmen von Prozessen zur Härtung von Systemen bei deren Installation vorgesehen werden.

3.1.5 QNAP NAS

Nutzerinnen und Nutzer von Netzwerkspeichern, Network Attached Storage (NAS), der taiwanesischen Firma QNAP waren ab April 2021 Ziel von Angriffen mit der Ransomware «Qlocker».[27] Die Angreifenden nutzten dafür eine kritische Schwachstelle[28] aus, für welche QNAP am 16. April 2021 ein Update bereitgestellt hat. Zahlreiche Nutzerinnen und Nutzer haben dieses Update jedoch verspätet oder gar nicht installiert. Dem NCSC wurden mehrere Schweizer Opfer gemeldet, vor allem Privatpersonen und KMUs.

Das NCSC hat die Bevölkerung über die Bedrohung informiert und Empfehlungen herausgegeben.[29]

Schlussfolgerung / Empfehlungen:

Netzwerkspeicher werden in Heimnetzwerken häufig direkt an den Router angeschlossen und sind deshalb je nach Konfiguration exponiert.[30]

Ein NAS sollte nie direkt vom Internet her erreichbar sein. Sowohl in Unternehmen als auch im Heimbereich gilt es, dies zu vermeiden und stattdessen via ein VPN mit einer Zwei-Faktor-Authentisierung auf diese Ressourcen zuzugreifen.

Keinesfalls darf das Management Interface gegen das Internet hin exponiert werden.

Daten und Backups, die auf NAS gespeichert sind, müssen ebenfalls (zusätzlich offline) gesichert werden.

---

26 Kritische Schwachstelle in Drucker-Spoolern von Microsoft-Systemen (ncsc.admin.ch); Patches verfügbar - Kritische Schwachstelle in Drucker-Spoolern von Microsoft-Systemen (ncsc.admin.ch).

27 Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices (bleepingcomputer.com); Qnap sichert NAS spät gegen Qlocker-Attacken ab (heise.de).

28 NVD – CVE-2020-36195 (nist.gov); SQL Injection Vulnerability – Security Advisory (qnap.com).

29 Die Woche 16 im Rückblick (ncsc.admin.ch); Die Woche 17 im Rückblick (ncsc.admin.ch).

30 The reason why you shouldn't connect QNAP NAS directly to the Internet without any protection (qnap.com)

3.1.6 Dell-BIOSConnect Schwachstellen

Am 24. Juni 2021 publizierten Forschende der Sicherheitsfirma Eclypsium mehrere Schwachstellen im Programm «SupportAssist» von Dell.[31] Diese Software ist auf den meisten Windows-Geräten von Dell vorinstalliert und ermöglicht unter anderem ein Update der Firmware oder die Wiederherstellung wichtiger Funktionen im Falle eines Festplattenfehlers oder einer Beschädigung. Das Problem soll 129 Modelle und damit über 30 Mio. Geräte betreffen. Die Verwundbarkeiten würden es Angreifenden ermöglichen, den Boot-Prozess des Geräts zu kontrollieren und damit das Betriebssystem sowie die Sicherheitskontrollen auf höherer Ebene zu unterlaufen. Jedoch müssten die Angreifenden dazu zuerst das Netzwerk, in welchem der Computer steht, kompromittiert und zudem ein vertrauenswürdiges Zertifikat erworben haben. Schliesslich wären sie auch noch darauf angewiesen, dass eine Nutzerin oder ein Nutzer vor Ort das Update oder die Wiederherstellung aktiv einleitet.[32]

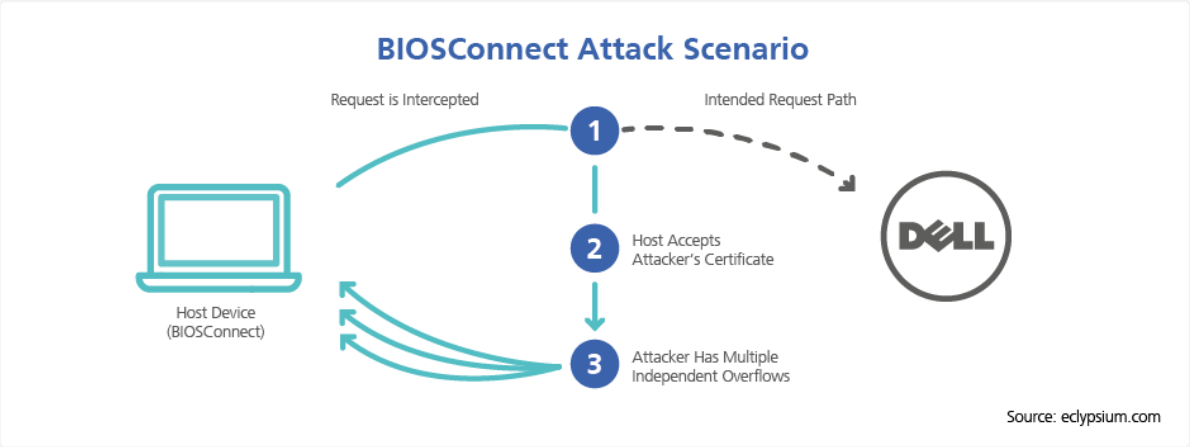


Abb. 2: Die Verbindung zum Server von Dell wird abgefangen.

Schlussfolgerung:

Diese Schwachstellen wurden wohl nicht breit ausgenutzt, weil der Angriff von vielen Bedingungen abhängt. Bemerkenswert an Verwundbarkeiten auf dieser Ebene ist, dass jegliche Sicherheitsmassnahmen auf dem Endgerät ausgehebelt werden können, da diese erst nach dem Aufstarten aktiviert werden. In kompromittierten Firmennetzwerken können solche Schwachstellen jedoch dazu führen, dass eine Vielzahl von Endgeräten infiziert werden.

---

31 Eclypsium Discovers Multiple Vulnerabilities in Dell BIOSConnect (eclypsium.com)

32 DSA-2021-106: Sicherheitsupdate der Dell Client-Plattform aufgrund mehrere Schwachstellen in den Funktionen BIOSConnect und HTTPS Boot als Teil des Dell Client-BIOS (dell.com)

3.1.7 Bad Alloc

Sicherheitsforschende des Teams Section 52 von Microsoft haben mehrere Verwundbarkeiten entdeckt, die mit Speicherzuweisungen zusammenhängen.[33] Da es sich dabei jeweils um fehlerhafte Zuweisungen (engl. «bad allocation») von Speicherplatz handelt, wurde diese Serie von Verwundbarkeiten «BadAlloc» genannt. Durch die Provokation von Pufferüberläufen könnten Angreifende bösartigen Code auf dem Zielgerät ausführen oder das Gerät zum Absturz bringen. Als Ursache wurde mangelnde Validierung von Input eruiert.

Microsoft hat in Zusammenarbeit mit dem amerikanischen Heimatschutzministerium DHS die verschiedenen Hersteller von verwundbaren Geräten informiert, damit diese die Schwachstellen beheben und Updates zur Verfügung stellen können.[34] Da es sich bei den betroffenen Systemen jedoch unter anderem um Echtzeit-Betriebssysteme in industriellen Anlagen und (zertifizierte) medizinische Geräte handelt, ist deren Absicherung nicht trivial. Wenn diese Systeme nach empfohlener Praxis von Umsystemen sauber getrennt sind, dürfte einer Ausnützung der Schwachstellen durch Angreifende vorgebeugt sein.

Schlussfolgerung:

Bereits bei der Programmierung ist auf die Implementierung von Sicherheitsmassnahmen zu achten («security by design»). Ansonsten entsteht ein enormer Aufwand bei der Ausbesserung, wenn eine solche überhaupt möglich ist.

3.2 Software-Management: Inventar und Update-Prozesse

Cyberangriffe können nicht nur über Schwachstellen sondern auch über Software-Lieferketten, sogenannte Software Supply-Chains, stattfinden. Bei diesen Angriffsszenarien greift die Täterschaft in den Herstellungs- oder Update-Prozess von Software ein, wodurch dann kompromittierte Software über reguläre Wege verteilt wird. Meistens ist nach Bekanntwerden eines solchen Angriffs die kompromittierte Software leicht festzustellen, doch ist dies nicht immer der Fall. Während der weltweiten Reaktion auf die Kompromittierung von SolarWinds[35] mussten die Unternehmen überprüfen, welche Version sie verwendeten und ob sie betroffen waren. Verschiedentlich wurde die Software jedoch von Originalgeräteherstellern (OEM) eingebaut, und die Endkunden waren sich nicht bewusst, dass die Software in dem bei ihnen eingesetzten Produkt enthalten war.

Diese Komplexität ist auch in folgendem Fall ersichtlich: Am 15. April 2021 informierte das Unternehmen Codecov, Herstellerin eines Software-Audit-Tools, seine Kundschaft über eine Sicherheitsverletzung bezüglich ihrem Produkt «Bash-Uploader».[36] Das entsprechende Script wird von Tausenden von Kundinnen und Kunden verwendet und ist auch in verschiedenen

---

33 "BadAlloc" – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in industrial, medical, and enterprise networks (microsoft.com)

34 ICS Advisory (ICSA-21-119-04) – Multiple RTOS (cisa.gov)

35 Vgl. NCSC HJB 2020-2, Kap. 4.7.2.

36 Bash Uploader Security Update (codecov.io)

Programmen integriert, weshalb es schwierig zu erkennen ist, wer tatsächlich von diesem Vorfall betroffen ist.

Eine angemessene Reaktion bei einem Vorfall setzt voraus, dass System- und Netzwerkbetreibende ein aktuelles Inventar führen. Das gilt nicht nur für Hardware, sondern auch für die in ihren Umgebungen vorhandenen Software und ihre Abhängigkeiten. Die Pflege eines solchen Inventars ist anspruchsvoll, muss laufend erfolgen und benötigt entsprechende Ressourcen.

Angesichts der zunehmenden Komplexität von Hard- und Software sowie der fortschreitenden Digitalisierung der Gesellschaft stellen nicht zuletzt Software-Abhängigkeiten eine grosse Herausforderung für die Sicherheit von Unternehmen dar. In den letzten Jahren hat die «US National Telecommunications and Information Administration (NTIA)» mit Partnern an der Entwicklung einer «Software Bill of Materials (SBOM)» gearbeitet.[37] Ähnlich wie bei Lebensmitteln, bei denen die Zutaten zur Herstellung des Endprodukts deklariert werden müssen, würde die SBOM vorschreiben, dass bei digitalen Produkten anzugeben ist, welche Komponenten zur Herstellung des Endprodukts verwendet wurden. Am 12. Mai 2021 veröffentlichte die US-Regierung die Cybersicherheitsverordnung «Executive Order on Improving the Nation's Cybersecurity»,[38] in der die SBOM im Kapitel über die Verbesserung der Sicherheit der Software-Lieferkette ausdrücklich erwähnt wird.

Die Erhöhung der Transparenz digitaler Produkte bietet eine Möglichkeit, den Überblick über die eingesetzten Produkte und ihre Abhängigkeiten zu behalten. Die zunehmende Komplexität und Informationsfülle in diesem Bereich erfordert jedoch auch ein gewisses Mass an Automatisierung bei der Pflege des Softwareinventars und der Verarbeitung von Sicherheitshinweisen («Security Advisory»), die sich auf die Elemente des Inventars beziehen.

Derzeit werden Sicherheitshinweise auf unterschiedliche Weise und in verschiedenen Formaten veröffentlicht: Einige Hersteller veröffentlichen sie auf ihren Websites, bei anderen muss man sich in ihr Portal einloggen, wieder andere verschicken sie als pdf-Datei, und die Struktur der Hinweise hängt von den individuellen Präferenzen jeder Organisation ab.

OASIS Open, ein gemeinnütziges Gremium für Open-Source-Standards, hat betreffend Automatisierung eine Diskussion über ein neues Format, das «Common Security Advisory Framework (CSAF 2.0)», angestossen. Dieses soll es ermöglichen, die erforderlichen Security Advisories standardisiert und maschinenlesbar zu erstellen. Das Ziel ist die Etablierung eines Standards für die automatisierte Verarbeitung von Sicherheitshinweisen.[39]

---

37 SOFTWARE BILL OF MATERIALS | National Telecommunications and Information Administration (ntia.gov)

38 Executive Order on Improving the Nation's Cybersecurity (whitehouse.gov)

39 Common Security Advisory Framework (CSAF) Website (csaf.io, oasis-open.github.io, oasis-open.org); BSI - Common Security Advisory Framework (CSAF) (bsi.bund.de).

Schlussfolgerung:

Die Führung und laufende Aktualisierung eines Inventars aller Hard- und Software-Komponenten ist ein wesentlicher Aspekt für die Sicherung einer IT-Infrastruktur. Idealerweise hat man zudem einen Überblick über alle Software-Abhängigkeiten. Die Einführung von SBOM würde diesen Überblick bieten, jedoch auch die Komplexität der zu pflegenden Datenbanken erhöhen. Nicht zuletzt deshalb wäre ein Mittel zur automatisierten Erfassung und Verarbeitung von Sicherheitshinweisen für die im Netz vorhandenen Elemente von Vorteil. Ein möglicher Weg dazu könnte das von OASIS Open entwickelte «CSAF 2.0» sein.

3.3 Schwachstellenmanagement aus Sicht des NCSC

Sicherheitslücken in der IT stehen immer mehr im Fokus der Öffentlichkeit. Die jüngsten Angriffe auf SolarWinds-Produkte,[40] die Sicherheitslücken in Microsoft Exchange[41] wie auch diejenigen im Druckprozess von Microsoft Windows[42] zeigen, wie solche Lücken inzwischen von staatlichen und nichtstaatlichen Akteuren genutzt werden. Bis vor einigen Jahren erfolgten solche Angriffe fast nur durch Staaten mit bedeutenden offensiven Cyberfähigkeiten, aber heute werden Sicherheitslücken zunehmend von Kriminellen genutzt. Durch das Aufkommen von leicht zugänglichen und nutzbaren kriminellen Diensten («Crimeware-as-a-Service») und die riesige Menge an im Umlauf befindlicher Software sind Sicherheitslücken in nur wenigen Jahren zum Albtraum von IT-Sicherheitsverantwortlichen weltweit geworden. Das NCSC hat eine Abteilung eingerichtet, die sich mit Sicherheitslücken befasst. Die Ziele sind vielfältig: Information, Sensibilisierung und Unterstützung der Öffentlichkeit (Privatpersonen, Unternehmen, staatliche Stellen) über die im Umlauf befindlichen kritischen Sicherheitslücken und die entsprechenden Sicherheitsmassnahmen; Bereitstellung einer Bug Bounty-Plattform für staatliche Stellen, um mögliche Sicherheitslücken in staatlichen Computernetzen zu ermitteln; Eröffnung einer Plattform für die koordinierte Offenlegung von Sicherheitslücken («Coordinated Vulnerability Disclosure»), um Entdeckerinnen und Entdeckern von Sicherheitslücken die Möglichkeit zu geben, ihre Erkenntnisse anonym an eine staatliche Stelle zu melden.[43] Dies sind nur einige der Ziele, die sich das NCSC mit der neuen Abteilung gesetzt hat und von denen einige bereits erreicht worden sind. Da Sicherheitsprobleme im Zusammenhang mit Software- und Hardware-Schwachstellen in naher Zukunft zunehmen werden, wird die Arbeit des NCSC im Bereich der Prävention, Erkennung und Behebung von Problemen in diesem Bereich immer wichtiger werden.

---

[40] Vgl. NCSC HJB 2020-2, Kap. 4.7.2 und unten Kap. 4.6.1.

[41] Siehe hiervor Kap. 3.1.1 und unten Kap. 4.6.2.

[42] Siehe hiervor Kap. 3.1.4.

[43] Melden einer Schwachstelle (Coordinated vulnerability disclosure, CVD) (ncsc.admin.ch)

3.4 Bug Bounty-Programm der Bundesverwaltung

Ein wichtiger Pfeiler im Schwachstellenmanagement bieten sogenannt Bug Bounty-Programme. Dabei werden ethische Hackerinnen und Hacker dazu aufgerufen, Schwachstellen in den IT-Systemen einer Organisation aufzuspüren. Für jede gefundene und bestätigte Schwachstelle (Bug) erhält die erfolgreiche Hackerin oder der erfolgreiche Hacker eine Belohnung (Bounty), abgestuft nach Schweregrad der gefundenen Schwachstelle.

Vom 10. bis 21. Mai 2021 hat das NCSC in Zusammenarbeit mit der Bug Bounty Switzerland GmbH, dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und den Parlamentsdiensten (PD) ein Bug Bounty-Pilotprojekt durchgeführt. Insgesamt nahmen 15 durch den Bund beauftragte ethische Hackerinnen und Hacker an diesem Pilotprojekt teil. Diese fanden insgesamt zehn Sicherheitslücken. Das Projekt verlief sehr erfolgreich und die gewonnenen Erkenntnisse sollen in die Durchführung weiterer Bug Bounty-Programme in der Bundesverwaltung einfliessen.[44]

Das Pilotprojekt hat gezeigt, dass mittels Bug Bounty-Programmen Schwachstellen in IT-Systemen und Anwendungen effizient identifiziert und behoben werden können. Der «Return on Investment» wurde als hoch identifiziert. Ein Bug Bounty-Programm für die Bundesverwaltung, betrieben durch das NCSC, leistet einen wichtigen Beitrag zur Reduktion des Cyberrisikos des Bundes.

4 Ereignisse / Lage

4.1 Eingegangene Meldungen zu Cybervorfällen – Überblick

Im ersten Halbjahr 2021 sind bei der Anlaufstelle des NCSC insgesamt 10’234 Meldungen eingegangen. Dies sind fast doppelt so viele wie im ersten Halbjahr 2020. Gründe für diese starke Zunahme sind auf der einen Seite die Einführung des neuen Meldeformulars[45] und dessen prominente Platzierung auf der Startseite. Auf der anderen Seite ist die hohe Zahl aber auch auf mehrere grosse Fake-Sextortion-[46] und Phishing-Wellen zurückzuführen. Dies zeigt sich vor allem an den hohen Meldezahlen rund um die Woche 5 und Woche 16.

---

44 Erfolgreiches Bug Bounty-Pilotprojekt in der Bundesverwaltung (ncsc.admin.ch)

45 NCSC Meldeformular (ncsc.admin.ch)

46 Informationen zu Fake Sextortion (ncsc.admin.ch); s. a. Stop Sextortion (stop-sextortion.ch).

Abb. 3: Anzahl Meldungen pro Woche beim NCSC vom August 2020 bis Juli 2021, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

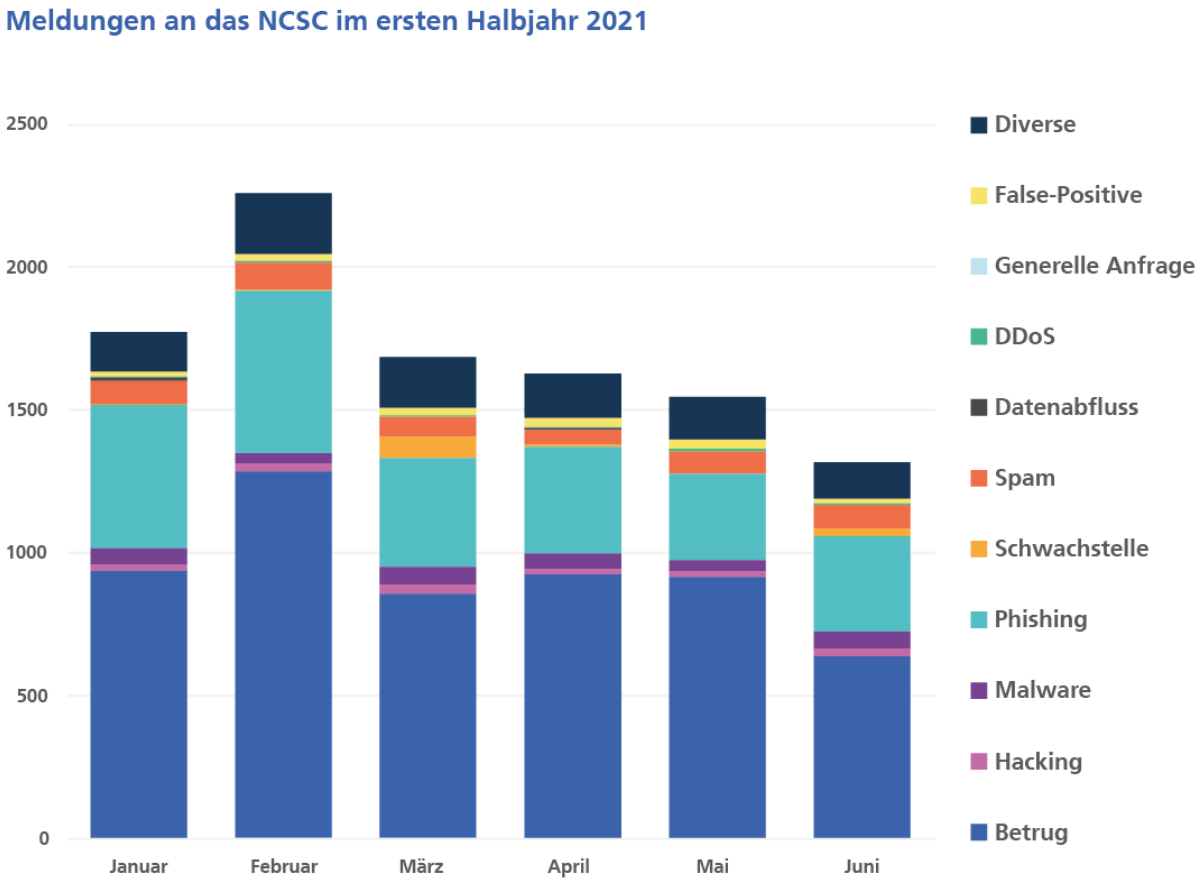


Abb. 4: Meldungen an das NCSC im ersten Halbjahr 2021 nach Kategorien, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

4.1.1 Meldungen zu Betrug

In der Hauptkategorie «Betrug», welche mit 5'526 Meldungen über die Hälfte der Meldungen ausmacht, wurde Fake-Sextortion im ersten Halbjahr 2021 mit 1'351 Meldungen am häufigsten gemeldet und verdrängte dabei Meldungen zu Vorschussbetrug mit 1'284 Hinweisen auf Platz zwei. Vorschussbetrug[47] war in den beiden Semestern zuvor noch das am häufigsten gemeldete Phänomen.

Weitere häufig gemeldete Betrugsarten sind CEO Betrug[48] (239), Fake Support Anrufe[49] (370) und Kleinanzeigenbetrug[50] (307). Beim Kleinanzeigenbetrug wurde neben den klassischen Varianten, bei denen nichtexistierende Waren verkauft werden oder Waren nach der Bezahlung nicht geliefert werden, vor allem die Variante beobachtet, bei der man unter irgendeinem Vorwand trotz eines Verkaufes noch Geld an die Käuferin oder den Käufer, respektive an eine Drittfirma überweisen soll, die dann beispielsweise den Transport organisieren soll. Es gibt auch die Variante, dass die Zahlung über Paypal abgewickelt werden soll. Anschliessend kommt ein betrügerisches E-Mail mit gefälschtem Paypal-Absender, dass Gebühren zu bezahlen sind, bevor die Transaktion durchgeführt werden kann.

Investitionsbetrug[51] gehört zu den Delikten mit typischerweise hohen Schadensummen. Insgesamt wurden dem NCSC 252 Fälle gemeldet, wobei es in 38 Fällen auch zu einem finanziellen Verlust gekommen ist. Beispiele zu aktuellen Vorgehensweisen finden Sie unten in Kapitel 4.8.

4.1.2 Meldungen zu Phishing

Eine starke Zunahme verzeichnete das NCSC auch bei den Phishing-Meldungen an die Anlaufstelle.[52] Wurden im ersten Semester 2020 über das Meldeformular noch 497 Hinweise zu Phishing gemeldet, waren es in der gleichen Periode im Jahr 2021 2'439.[53] Diese Zahl hat sich fast verfünffacht. Der Grund liegt vor allem am erhöhten Meldeeingang von E-Mails und SMS mit gefälschten Paketbenachrichtigungen, deren Versand in den letzten Monaten stark zugenommen hat.[54] In diesen Fällen wird jeweils vorgegeben, dass ein Paket nicht zugestellt werden konnte und deshalb eine kleine Gebühr für einen weiteren Zustellversuch entrichtet werden muss. Zu diesem Zweck muss das Opfer einen Link anklicken und anschliessend seine Kreditkartendaten angeben. In der Regel wird kurz darauf ein grosser Betrag direkt von der Kreditkarte abgezogen. In einer ähnlichen Variante, welche 479 Mal gemeldet wurde, werden nicht die Kreditkartendaten, sondern Zollgebühren verlangt, welche dann mit Paysafe-Karten

---

47 Informationen zu Vorschussbetrug (ncsc.admin.ch)

48 Informationen zu CEO-Betrug (ncsc.admin.ch)

49 Informationen zu Fake-Support (ncsc.admin.ch)

50 Informationen zu Kleinanzeigenbetrug (ncsc.admin.ch); Kleinanzeigenbetrug - Fake Gebühr (ncsc.admin.ch).

51 Informationen zu Investmentbetrug (ncsc.admin.ch); siehe auch unten Kap. 4.8.

52 Informationen zu Phishing (ncsc.admin.ch)

53 Die Zahl bezieht sich auf Hinweise zu Phishing-E-Mails, die über das NCSC-Meldeformular eingegangen sind. Diese werden analysiert und die betrügerischen Links dann an das vom NCSC betriebene Portal antiphishing.ch weitergeleitet. Die Zahlen von antiphishing.ch (siehe unten Kap. 4.7.1) beinhalten deshalb die Zahlen des NCSC-Meldeformulars.

54 Siehe Die Woche 11 im Rückblick (ncsc.admin.ch), Die Woche 23 im Rückblick (ncsc.admin.ch) und Kap. 4.7.2.

bezahlt werden sollen. Die vermeintliche Absenderin solcher E-Mails ist meist die Eidgenössische Zollverwaltung (EZV). Die Nummern der Paysafe-Karten, welche es der Täterschaft ermöglicht, das Geld abzuheben, sollen dann an eine E-Mail-Adresse gesendet werden. Das perfide dabei ist, dass die betrügerische E-Mail-Adresse hinter der offiziellen Adresse der Zollverwaltung versteckt ist und erst sichtbar wird, wenn man darauf klickt. Da diese E-Mails und SMS vielfach mit getätigten Online-Bestellungen zusammenfallen, wird häufig vermutet, dass es bei der Zollverwaltung oder bei der Post ein Datenleck geben müsse. Bis heute sind aber weder bei der Post noch bei der Zollverwaltung Datenlecks gefunden worden. Der Grund des zeitlichen Zusammenfalls solcher E-Mails hat vielmehr mit statistischen Effekten zu tun. Gerade in Zeiten von Covid-19 haben Online-Bestellungen einen wahren Boom erlebt. Dies haben auch die Kriminellen gemerkt und intensivierten seit dem Ausbruch der Pandemie den Versand von betrügerischen Paketankündigungs-E-Mails und -SMS. Es ist deshalb gar nicht so unwahrscheinlich, dass eine wirklich getätigte Bestellung und eine betrügerische Nachricht zeitlich zusammenfallen.

4.1.3 Meldungen zu Malware

Die hohe Zahl an gemeldeten Vorfällen mit Verschlüsselungstrojanern, sogenannter Ransomware, im ersten Halbjahr 2021 ist ebenfalls auffällig. Die Zahl hat sich von 32 Fällen im ersten Halbjahr 2020 auf 94 Fälle in der aktuellen Berichtsperiode verdreifacht. Zurückzuführen ist dies vor allem auf die Ransomware «Qlocker», welche sich vor allem gegen Private richtete und es auf Netzwerkspeicher der Marke QNAP abgesehen hatte (s. a. oben, Kapitel 3.1.5). Mit 39 Fällen war «Qlocker» mit Abstand die meistgemeldete Ransomware. Viele Personen haben auch E-Mails mit bösartigen Anhängen oder verdächtigen Links erkannt und gemeldet (siehe dazu das nachfolgende Kapitel).

4.2 Schadsoftware / Malware

4.2.1 Malware-Verbreitung

Der meistgenutzte Weg zur Verbreitung von Schadsoftware ist nach wie vor E-Mail. Malware kann direkt an E-Mails angehängt sein, durch das Öffnen einer angehängten Datei heruntergeladen und installiert werden oder sich auf einer im Mail verlinkten Website befinden, auf welcher eine schädliche Datei heruntergeladen werden soll oder worauf eine Drive-by Infektion[55] platziert ist. Empfänger werden typischerweise mit Social Engineering-Methoden[56] dazu gebracht, Aktionen auszuführen, die schliesslich in der Installation von Schadsoftware münden.

Die Infektion eines Computers oder Netzwerks läuft typischerweise in mehreren Phasen ab. Zu Beginn geht es den Angreifenden darum, eine erste Infektion zu erreichen. Die initiale Malware wird oft über grossangelegte Malspam-Kampagnen breit gestreut, so etwa «AgentTesla», «Lokibot» und «FormBook» im vergangenen Halbjahr in der Schweiz. Solche Malware dient typischerweise als Türöffner und kann häufig Informationen über das infizierte System

[55] Siehe dazu unten Kap. 4.3.2

[56] Siehe dazu unten Kap. 4.7

sammeln und je nach Bedarf weitere eigene Funktionsmodule oder andere (Schad-)Software nachladen. Zugänge zu infizierten Geräten werden dann im Untergrundmarkt von Cyberkriminellen gehandelt.

Die folgende Grafik zeigt Malware-Familien, welche vom NCSC im vergangenen halben Jahr analysiert und identifiziert wurden. Die analysierten Dateien und Codes stammen dabei aus verschiedenen Quellen wie Sensoren, Meldungen von Sicherheitsverantwortlichen kritischer Infrastrukturen, von Bürgern und KMUs. Die gemeldeten Dateien und Codes werden analysiert und einer Malware-Familie zugeordnet. Gefundene Erkennungsmerkmale («Indicators of Compromise», IOCs) teilt das NCSC mit Betreiberinnen kritischer Infrastrukturen, damit diese sich schützen können.

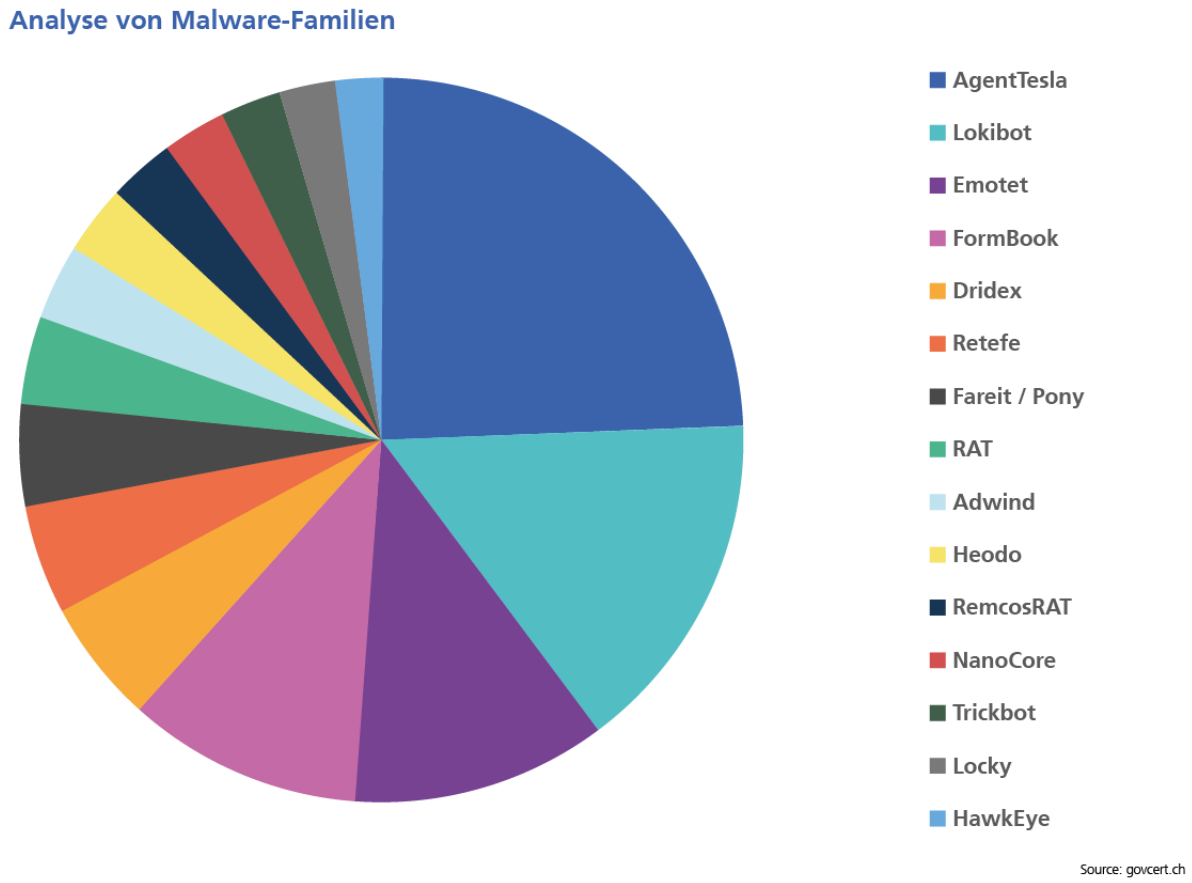


Abb. 5: Analysen des NCSC von Malware-Familien in der Schweiz im ersten Halbjahr 2021.

Nachdem Strafverfolgungsbehörden Anfang 2021 die Infrastruktur von «Emotet» ausgehoben und abgeschaltet haben,[57] kommen (wieder) vermehrt andere Malware-Familien zum Zug. Nebst bekannten Namen wie «TrickBot», «Retefe», «Dridex» und «Qbot» finden sich auch vorher seltener verwendete unter den aktuell beobachteten Malware-Familien, etwa «IcedID».

Im Februar 2021 wurde eine grosse Malspam-Kampagne beobachtet, bei der die Marke «DocuSign» missbraucht und «TrickBot» via bösartige Excel-Dateien verbreitet wurde. Es war

[57] Siehe World's most dangerous malware EMOTET disrupted through global action (europol.europa.eu) und NCSC HJB 2020-2, Kap. 4.3.2.

dies die erste grössere «TrickBot»-Verbreitungswelle seit Oktober 2020. Die für die breit gestreute Kampagne verwendeten E-Mails und Dokumente waren auf Englisch verfasst und sehr generisch gehalten.

Über «SilentBuilder», ein bösartiges Makro in Excel-Dokumenten, wird die Malware «QBot» (alias «QakBot» und «QuakBot») installiert. Dem NCSC wurden mehrere Fälle gemeldet, in denen schadhaft präparierte Excel-Dokumente unbemerkt mehrere Sicherheitsebenen passierten und von Endbenutzern geöffnet wurden. Dabei setzten die Täterschaften verschiedene Social Engineering-Techniken ein, um Empfängerinnen und Empfänger davon zu überzeugen, die angehängte Excel-Datei zu öffnen und das Makro zu aktivieren. Sobald der Computer infiziert ist, wird ein «Cobalt Strike Beacon»[58] installiert, der den Angreifenden interaktiven Zugriff auf das System und damit Aufklärung, laterale Bewegungen und die Ausweitung von Berechtigungen ermöglicht.

Seit März ist ein starker Anstieg der Verbreitung von «IcedID» festzustellen – auch in deutschsprachigen E-Mails.[59] «IcedID» wurde seither insbesondere in Ransomware-Infektionsketten beobachtet. Dabei wurde «IcedID» über Google-Links, resp. Google Sites, via Webkontaktformulare verbreitet und diente dazu, Firmen mit «Cobalt Strike» zu infizieren.[60] So konnten Angreifer die Kontrolle über das Netzwerk erlangen und die Daten schliesslich mit Ransomware verschlüsseln.

«Retefe» wird auf andere Weise verbreitet: Meist werden (z. B. auf der Firmenwebsite) öffentlich einsehbare Telefonnummern angerufen und die Angerufenen unter einem Vorwand dazu aufgefordert, einen Google-Link zu öffnen, wodurch die Installation von «Retefe» ausgelöst wird.[61]

Empfehlungen:

- Prüfen Sie, wie Ihre Sicherheitsprodukte die Erkennung und oder Blockierung von Dokumenten unterstützen, die Makros enthalten. Stellen Sie sicher, dass dies auch in Archiv-Dateien geschieht.
- Blockieren Sie wenn möglich Dateitypen gemäss dieser Liste des NCSC.
- Erlauben Sie in Ihrem Netzwerk nur die Ausführung digital signierter Makros und kontrollieren Sie, welche Anwendungen von welchem Pfad aus ausgeführt werden können (z. B. mit «AppLocker»).
- Stellen Sie sicher, dass Ihr internes Netzwerk ausreichend gepatcht ist. Stellen Sie z. B. sicher, dass kein Domänencontroller mehr anfällig ist für die Sicherheitslücke «Zerologon» (CVE-2020-1472).[62]
- Erhöhen Sie die Sichtbarkeit auf den Endpunkten durch den Einsatz eines EDR-Tools (Endpoint Detection and Response) und oder Sysmon (System-Monitoring).

---

58 Vgl. Kap. 4.2.2 hiernach.

59 Aufstieg von IcedID (computerworld.ch)

60 Investigating a unique "form" of email delivery for IcedID malware (microsoft.com)

61 Vgl. Schadsoftware nach Anruf (ncsc.admin.ch); Aktuelle Ransomware-Angriffe mit Pakettrick (infoguard.ch).

62 CVE-2020-1472 (mitre.org); NVD - CVE-2020-1472 (nist.gov); Was ist Zerologon? (trendmicro.com).

- Sensibilisieren Sie Ihre Mitarbeitenden, damit sie verdächtige Nachrichten und Anrufe erkennen und wissen, wie sie reagieren sollen.
- Etablieren Sie interne Meldeprozesse an die Sicherheitsverantwortlichen.

Die untenstehende Grafik zeigt Daten aus DNS-Sinkholes. Ein DNS-Sinkhole wird dazu verwendet, Malware unschädlich zu machen, indem dazugehörende Domainnamen dem Zugriff der Kriminellen entzogen und auf eine Sicherheitsorganisation umregistriert werden. Auf diese Weise können infizierte Geräte identifiziert werden, da sie sich nun nicht mehr zu den Servern der Malware-Betreibenden verbinden, sondern bei den Servern der Sicherheitsorganisation melden. Das NCSC sammelt und analysiert diese Daten für den gesamten schweizerischen IP-Adressraum und informiert die Besitzer dieser Geräte via ISPs über die Infektion.

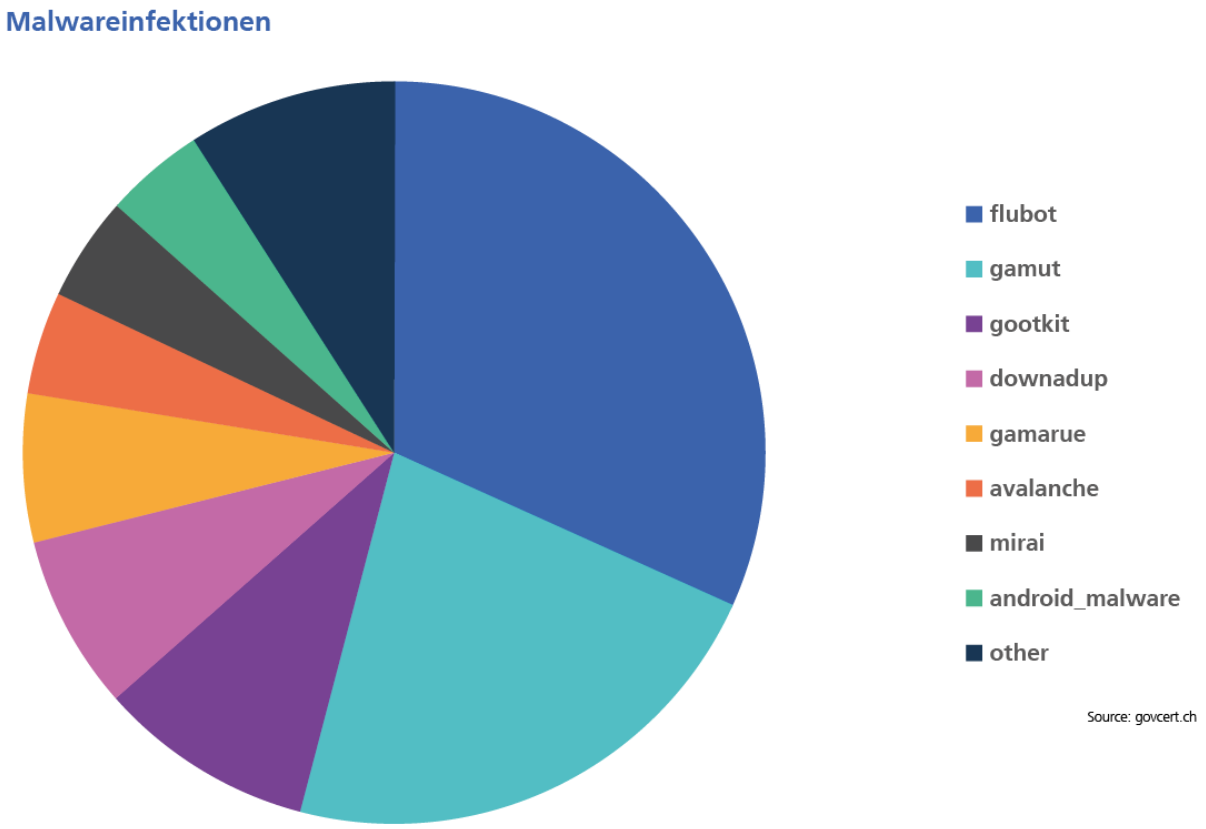


Abb. 6: Verteilung der vom NCSC festgestellten Malwareinfektionen in der Schweiz im ersten Halbjahr 2021.

In der ersten Jahreshälfte hat sich die Malware «Flubot» über grosse SMS-Verbreitungskampagnen in ganz Europa verteilt. Nachdem zuerst Nutzerinnen und Nutzer von Android-Smartphones in den nordischen Ländern und Grossbritannien im Fokus waren, erreichte die Bedrohung im Juni die Schweiz und Österreich.

Es gibt verschiedene Szenarien für die SMS-Verbreitung mit «Flubot»-infiziertem Link. In der Schweiz weist ein SMS auf Deutsch auf eine vermeintliche Sprachnachricht hin. Wer auf den

Link klickt, wird zu einem Download aufgefordert, mit dem die Schadsoftware auf dem Gerät installiert wird.[63]

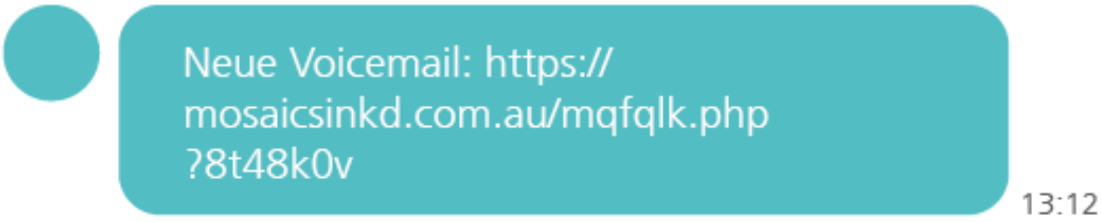


Abb. 7: Beispiel eines SMS mit Flubot-Link.

«Flubot» kann sich über andere Apps legen («overlay attack») und so z. B. E-Banking-Aktivitäten des Opfers ausspähen. Sie kann sich auch als Wurm über die Kontaktliste des Opfers weiterverbreiten, die automatisch das gleiche SMS an alle Kontakte verschickt. Das erklärt die jeweils rasche Verbreitung der Bedrohung in den betroffenen Ländern.

Das NCSC hat Unternehmen und Bevölkerung über «Flubot» informiert.[64]

Empfehlungen bei verdächtigen SMS und anderen Kurznachrichten

- Nicht auf Links von unbekannten Absendern klicken.
- SMS oder Nachricht löschen.
- Falls eine App installiert wurde:
  - Werkeinstellungen auf dem Telefon wiederherstellen,
  - Mobilfunkanbieterin informieren,
  - Kreditkarten sperren,
  - Zugriff auf Bank- und Krypto-Konten sowie E-Mail zurücksetzen.

4.2.2 Dual-Use-Software «Cobalt Strike»

Das kommerzielle Sicherheitsprüfwerkzeug «Cobalt Strike» wurde entwickelt, um einen fortgeschrittenen Akteur (Advanced Persistent Threat, APT) im Netzwerk zu simulieren, entsprechende Aktivitäten durchzuführen und die Erkennungs- und Verteidigungsfähigkeiten der Netzwerkadministratoren zu testen. Natürlich kann so ein Tool auch von echten Angreifenden verwendet werden. Raubkopien von «Cobalt Strike» werden von Kriminellen wie auch von staatlichen Akteuren gerne eingesetzt, um sich in Systemen nach einer erfolgreichen Infektion zu bewegen und auszubreiten. Es wird von Kriminellen zudem für die Extraktion von Daten und den anschliessenden Einsatz von Ransomware verwendet. Durch den Einsatz von «Cobalt Strike» können staatliche Akteure die Erkennung und oder die Attribution eines gezielten Spionageangriffs erschweren.

---

63 Das SMS "Neue Voicemail" ist die gefährliche Schadsoftware FluBot (cybercrimepolice.ch)

64 Die Woche 24 im Rückblick (ncsc.admin.ch)

4.2.3 Ransomware

Durch Ransomware, auch Verschlüsselungstrojaner genannt, werden Betriebsprozesse gestört und Unternehmen in ihrer Handlungsfähigkeit eingeschränkt. Dies kann weitreichende Folgen haben, von Produktionsausfällen über Lieferstopps bis hin zum Konkurs eines Unternehmens. Auch Kundinnen und Kunden, die von Leistungen des angegriffenen Unternehmens abhängig sind, können beeinträchtigt werden.

Oft wenden Kriminelle eine doppelte oder sogar eine dreifache Erpressungstaktik an.[65] Haben die Kriminellen einmal Zugriff auf die Opfersysteme, kopieren sie zuerst die Daten. Weigert sich das Opfer, das Lösegeld für die Entschlüsselung zu bezahlen, drohen die Angreifenden mit der Veröffentlichung der Daten. Geht das Opfer auf die beiden ersten Forderungen nicht ein, werden allenfalls Personen und Organisationen kontaktiert, welche einen direkten Bezug zu den Daten haben, wie z. B. Vertragspartner oder Kunden. Gelegentlich starten die Kriminellen zusätzlich einen DDoS-Angriff auf das Opferunternehmen, um den Druck zu erhöhen.[66]

In der Berichtsperiode sind in der Schweiz Angriffe auf Privatpersonen und KMUs aus verschiedenen Wirtschaftssektoren mit verschiedensten Ransomware verübt worden.[67]

International gab es einige aufsehenerregende Vorfälle. In Erinnerung bleiben werden z. B. die langen Schlangen vor Tankstellen im Südosten der USA, als viele Amerikanerinnen und Amerikaner aus Angst vor Versorgungsengpässen noch einmal ihre Tanks auffüllen wollten.[68] Am 7. Mai 2021 unterbrach nämlich die Colonial Pipeline Company den Betrieb ihrer Öl und Gas befördernden Rohrleitungen, nachdem ihre administrativen IT-Systeme einer Infektion der «Darkside[69]»-Ransomware zum Opfer gefallen waren.[70] Die für den physischen Betriebsprozess der Pipeline eingesetzten Steuerungssysteme waren vom Verschlüsselungstrojaner zwar nicht direkt betroffen, als Vorsichtsmassnahme wurden diese Systeme aber ebenfalls heruntergefahren. Gegenseitige Abhängigkeiten zwischen den IT- und OT-Umgebungen zur Optimierung der übergeordneten Geschäftsprozesse stellen einen autarken Betrieb der industriellen Kontrollsysteme vor grosse Herausforderungen. Bisher wurden in erster Linie Ransomware-Angriffe spezifischer Familien als Bedrohung für industrielle Kontrollsysteme wahrgenommen, von denen bekannt ist, dass sie gezielt industrielle Prozesse miteinbeziehen, etwa «EKANS»[71] oder «Mega Cortex».[72] Die mediale und behördliche Aufmerksamkeit veranlasste die «Darkside»-Gruppe, sich von einem Grossteil ihrer Aktivitäten zurückzuziehen.[73] Später

---

65 Siehe NCSC HJB 2020-2, Kap. 4.3.1.

66 Extortion Payments Hit New Records as Ransomware Crisis Intensifies (paloaltonetworks.com)

67 Erfolgreiche Ransomware-Angriffe auf Schweizer Unternehmen (ncsc.admin.ch); Ransomware-Angreifer erpressen Schweizer Industriefirma Griesser (netzwoche.ch); Ransomware Angriffe in der Schweiz – was steckt dahinter? (entec.ch).

68 Colonial Pipeline systems resumes operations but Southeast still reeling from panic buying and gas price spikes (washingtonpost.com); Ransomware: Last Week Tonight with John Oliver (HBO) (youtube.com).

69 DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (cisa.gov)

70 The Colonial Pipeline Hack Is a New Extreme for Ransomware (wired.com)

71 This is how EKANS ransomware is targeting industrial control systems (zdnet.com)

72 Siehe MELANI HJB 2020-1, Kap. 4.3.1.

73 DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized (krebsonsecurity.com)

wurde bekannt, dass Colonial trotz vorhandener Backups auch Lösegeld bezahlt hatte.[74] Einen Teil des bezahlten Lösegelds konnte die amerikanische Justiz im Rahmen ihrer Ermittlungen sicherstellen.[75] Dieser Vorfall, der Angriff auf den grossen Fleischverarbeiter JBS Ende Mai[76] und weitere Vorfälle, in welchen Cyberkriminelle den Betrieb kritischer Infrastrukturen beeinträchtigen, bestärkten die US-Regierung, Regulierungen und Bestrebungen der Cybersicherheit prioritär voranzutreiben.[77]

Für Aufsehen hat auch die Ransomware «Conti» gesorgt, mit welcher das Gesundheitsministerium und der Gesundheitsdienst von Irland angegriffen wurde.[78] Am 13. Mai 2021 wurde das irische National Cyber Security Centre (NCSC) auf verdächtige Aktivitäten im Netzwerk des irischen Gesundheitsministeriums aufmerksam. Es handelte sich dabei um den Versuch eines Fernzugriffs mit der Software «Cobalt Strike».[79] Beim irischen Gesundheitsministerium wurde der Verschlüsselungsversuch am 14. Mai 2021 rechtzeitig gestoppt. Die staatlichen Gesundheitsdienste Irlands (HSE) wurden jedoch am selben Tag Opfer von «Conti». Grosse Teile des HSE-Netzwerks wurden zur Sicherheit vorübergehend offline gestellt. Leistungen waren entsprechend nur eingeschränkt verfügbar; diverse Behandlungen und Diagnoseprozesse mussten verschoben werden. Kritische Funktionen im Bereich Intensivpflege und Notfallbehandlungen waren gemäss HSE jedoch sichergestellt. Im Nachgang hat die Täterschaft zwar ein Entschlüsselungsprogramm kostenlos zur Verfügung gestellt. Sie haben jedoch Daten von Patientinnen und Patienten aus dem Netzwerk des HSE gestohlen und drohten damit, diese zu veröffentlichen, sollte kein Lösegeld bezahlt werden. Vereinzelt wurden Datensätze zum Beweis publiziert.

Es können jedoch auch Erfolge bei der Bekämpfung von Ransomware vermeldet werden: Die Strafverfolgungsbehörden der Ukraine konnten einige Mitglieder der «Clop»-Ransomware-Bande verhaften und die Infrastruktur abschalten, welche diese Gruppe für ihre Angriffe eingesetzt hatte. «Clop» hat weltweit einen finanziellen Gesamtschaden von ca. 500 Mio. Dollar verursacht.[80]

Schlussfolgerungen / Empfehlungen:

Ransomware kann erheblichen Schaden verursachen, insbesondere dann, wenn auch Datensicherungen (Backups) davon betroffen sind. Bleiben Sie bei einem solchen Vorfall ruhig und handeln Sie überlegt. Wichtige Aspekte der Vorfallsbewältigung sind das Auffinden des Infektionsweges sowie die Verhinderung einer neuen Infektion. Setzen Sie die betroffenen Systeme neu auf und stellen Sie Daten mit vorhandenen Backups wieder her.

---

74 Colonial Pipeline CEO: Paying DarkSide ransom was the ‘right thing to do for the country’ (zdnet.com)

75 DoJ Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (justice.gov)

76 JBS: FBI says Russia-linked group hacked meat supplier (bbc.com);
Ransomware: Meat firm JBS says it paid out $11m after attack (zdnet.com).

77 Executive Order on Improving the Nation's Cybersecurity (whitehouse.gov)

78 Department of Health hit by cyberattack similar to that on HSE (irishtimes.com)

79 Vgl. Kap. 4.2.2 hiervor zu «Cobalt Strike».

80 Ukraine arrests Clop ransomware gang members, seizes servers (bleepingcomputer.com)

Falls in Ihrem Unternehmen die notwendigen Fachkenntnisse nicht vorhanden sind, holen Sie sich Unterstützung bei einem spezialisierten Unternehmen.

Das NCSC empfiehlt Betroffenen, nie Lösegeld zu bezahlen. Mit der Leistung einer Zahlung bestätigt man das Geschäftsmodell der Kriminellen, unterstützt diese finanziell und regt sie zur Weiterführung und Weiterentwicklung ihrer Tätigkeiten an. Im schlimmsten Fall verliert man die Daten und das Geld. Das NCSC rät, bei der zuständigen Polizeibehörde Anzeige zu erstatten.

Die Absicherung von Cybervorfällen durch eine Cyberversicherung ist in den letzten Jahren mehr und mehr in den Fokus gerückt. Solche Versicherungsprodukte haben durchaus ihre Berechtigung, denn sie decken u. a. Risiken im Zusammenhang mit Internetkriminalität ab und bieten gute Unterstützung bei Problemen mit z. B. Internethandel, Rufschädigung, Virenangriffen, Daten- und oder Identitätsdiebstahl. Wenn Zahlungen von Lösegeld jedoch durch Versicherungen gedeckt werden, kann dies dazu führen, dass sich Erpresser auf Unternehmen fokussieren, die entsprechend versichert sind und die Kriminellen deshalb eine grössere Chance auf Bezahlung haben. Die Entscheidung pro oder kontra Abschluss einer Cyberversicherung liegt in der alleinigen Kompetenz der Unternehmen. Diese Entscheidung sollte gut abgewogen werden. Keinesfalls darf der Abschluss einer Cyberversicherung dazu führen, dass deshalb das IT-Budget gekürzt oder der sichere Betrieb der IT vernachlässigt wird.

Weitere Informationen auf der NCSC-Website: Ransomware (ncsc.admin.ch).

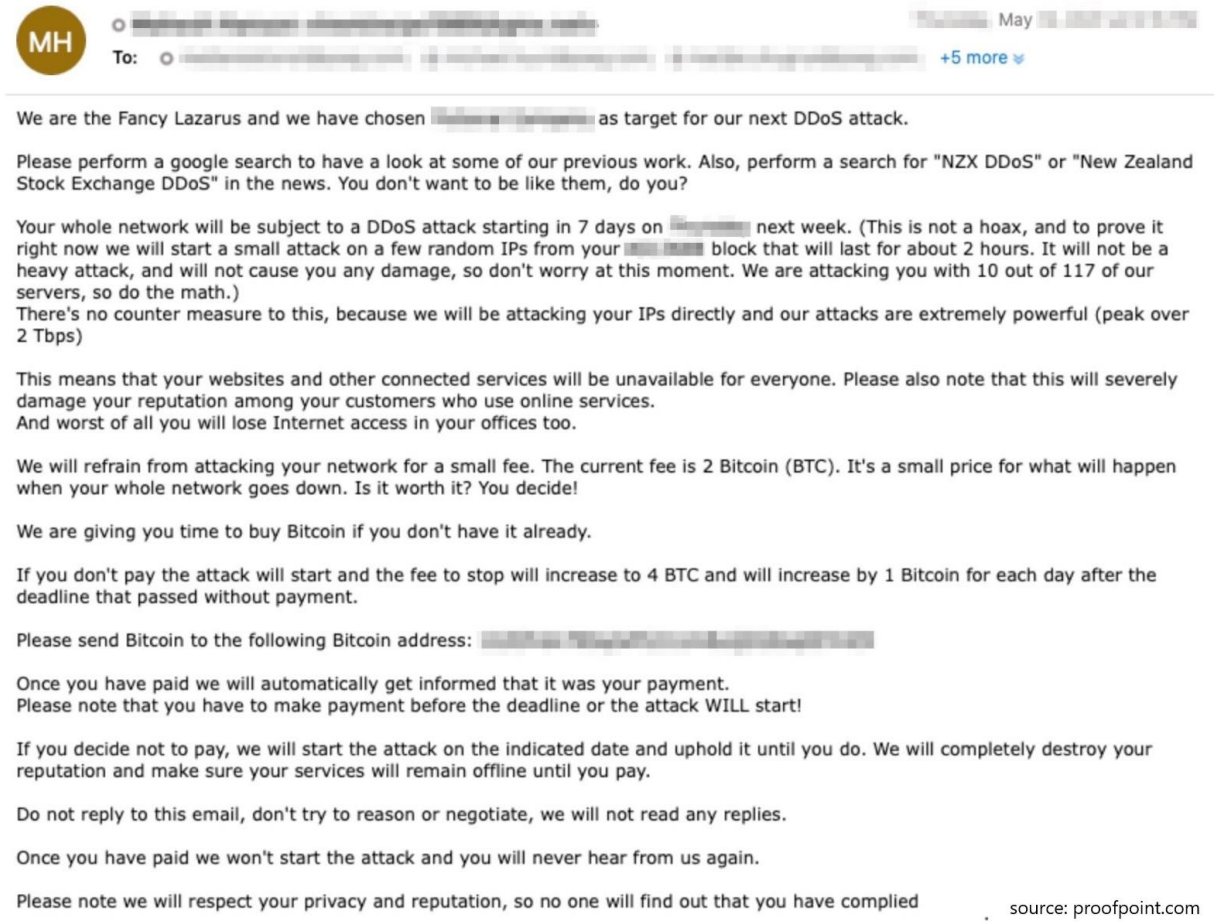
4.3 Angriffe auf Websites und -dienste

4.3.1 DDoS

Wie schon 2020 kam es auch im ersten Halbjahr 2021 zu DDoS-Angriffen («Distributed Denial of Service») in der Schweiz und im Ausland. So wurden dem NCSC 26 Vorfälle dieser Art gemeldet. Die Mehrheit der Meldungen beschrieb folgende Vorgehensweise der Täter: Es begann mit einem beachtlich starken aber grundsätzlich abwehrbaren Demonstrationsangriff (meist zwischen 40 und 120 Gigabit pro Sekunde), dem ein Erpressungs-Mail folgte oder voranging. In diesem wurde ein Lösegeld verlangt, bei dessen Nichtbezahlung ein massiverer Angriff von über 2 Terabit pro Sekunde folgen werde. Es handelt sich dabei um einen Bluff, um die anvisierten Organisationen einzuschüchtern. In den beobachteten Fällen wurden die angedrohten massiven Angriffe trotz Nichtbezahlen des Lösegelds nicht ausgeführt. Betroffen waren Organisationen aus verschiedenen Bereichen wie Finanzen, Gesundheit und Luftfahrt. Auch wurden mehrere Internetdienstanbieter angegriffen. Die Angriffe hatten jedoch dank den Abwehrmassnahmen der Provider kaum Auswirkungen für deren Kundschaft. Ausser in einem Fall, bei welchem ein Webhosting-Provider unter Beschuss kam: Bei diesem Angriff wurden die Internetseiten des Kantons, der Stadt und der Polizei St. Gallen für mehrere Stunden lahmgelegt.[81] Die Erpresser haben sich in der Vergangenheit die Namen von zwei sehr bekannten

[81] Hackergruppe greift St. Galler Hoster nicht mehr an (netzwoche.ch)

staatlichen Cyberakteuren angemasst («Lazarus» und «Fancy Bear»).[82] In den letzten Angriffswellen nennt sich die Täterschaft nun «Fancy Lazarus».



MH

To:

May

+5 more

We are the Fancy Lazarus and we have chosen as target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days on next week. (This is not a hoax, and to prove it right now we will start a small attack on a few random IPs from your block that will last for about 2 hours. It will not be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.)
There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.
And worst of all you will lose Internet access in your offices too.

We will refrain from attacking your network for a small fee. The current fee is 2 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to 4 BTC and will increase by 1 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address:

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

Please note we will respect your privacy and reputation, so no one will find out that you have complied

source: proofpoint.com

Abb. 8: Beispiel Erpresser-E-Mail von Fancy Lazarus.

In Belgien kam es im Mai zu einem massiven simultanen Angriff auf Belnet und andere Telecom-Anbieterinnen, der zu einer mehrstündigen Störung von Internetverbindungen führte und als Dominoeffekt den Unterbruch zahlreicher Dienste wie den (per Videokonferenz abgehaltenen) Debatten des belgischen Parlaments, Online-Kursen der Universität oder der Internetseiten verschiedener öffentlicher Dienste zur Folge hatte.[83]

Schlussfolgerung / Empfehlungen:

DDoS-Erpressung ist ein Massengeschäft. Die Angreifenden versuchen relativ undifferenziert bei möglichst vielen Unternehmen ihr Glück. Hat dies keinen Erfolg, versuchen sie es anderswo. Gelingt es aber, mit einem (Demonstrations-)DDoS-Angriff die Systeme eines Unternehmens zu stören, so gerät dieses Unternehmen als potenzielles Opfer in den Fokus. In der

[82] Vgl. NCSC HJB 2020-2, Kap. 4.4.1.

[83] Belgium's government network goes down after massive DDoS attack (therecord.media)

Hoffnung, dass Lösegeld bezahlt wird, verstärken die Täter ihre Anstrengungen. Deshalb ist es ratsam, gut auf allfällige DDoS-Angriffe vorbereitet zu sein.

Das NCSC empfiehlt, für kritische Systeme einen kommerziellen DDoS-Schutz zu abonnieren («DDoS Mitigation Service»). Viele Internet-Service-Provider bieten solche Dienste an.

Auf der Internetseite des NCSC finden Sie verschiedene Massnahmen zur Prävention und Abwehr von DDoS-Angriffen: Angriff auf die Verfügbarkeit (DDoS) (ncsc.admin.ch)

4.3.2 Webseitenkompromittierungen

Angreifer können mit gestohlenen Zugangsdaten oder via nicht-gepatchte Sicherheitslücken auf die Website-Administration zugreifen und dort beliebigen Code platzieren. Ein Anwendungsfall ist das Einfügen von so genannten Drive-by Infektionen, mit welchen versucht wird, die Geräte von Besuchern der Website mit Schadsoftware zu infizieren. Andere Phänomene sind das Weiterleiten von Besuchenden auf fragwürdige Werbung, betrügerische Websites oder dubiose Angebote. Websitezugänge können auch für so genannte «Black Hat SEO»[84] genutzt werden, d. h. es werden Inhalte auf der Website eingefügt, um Suchmaschinenergebnisse zu beeinflussen.

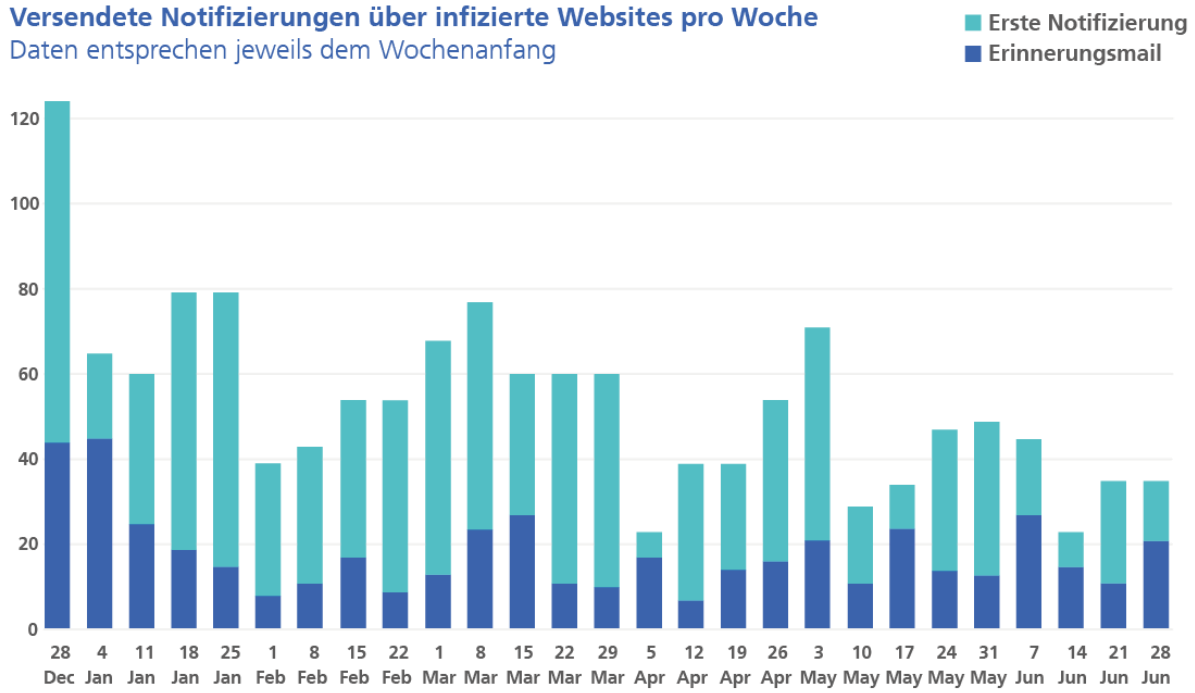


Abb. 9: Vom NCSC versendete Notifizierungen an Websitebetreiber respektive Webmaster und Hosting-Provider.

Wenn das NCSC kompromittierte Websites feststellt, informiert es deren Betreiber respektive Webmaster und Hosting-Provider, damit sie Gegenmassnahmen ergreifen können. Im ersten

[84] Black hat SEO and You Won (ncsc.nl); SEO steht für «Search Engine Optimization» (Suchmaschinenoptimierung). Dabei werden Massnahmen ergriffen, durch welche eine Website in den Ergebnissen von Internetsuchmaschinen möglichst weit oben angezeigt werden soll. S. a. Suchmaschinenoptimierung (wikipedia.org).

Halbjahr 2021 wurden 803 entsprechende Erst-Notifikationen und 445 Erinnerungs-Mails an bezüglich Websites im Schweizer Domainraum (Websites mit der Endung «.ch» oder «.swiss») versendet.

Empfehlungen:

Wurde die Website gehackt, ist eine systematische Bereinigung durch Lokalisierung und Entfernung des Schadcodes respektive der fremden Inhalte auf der Website erforderlich. Weiter ist die aktuellste Version des Content Management Systems (CMS) und der Plug-Ins einzuspielen. Sämtliche Computer, welche für die Website-Administration genutzt werden, müssen auf Schadsoftware durchsucht und gegebenenfalls bereinigt werden. Schliesslich sind alle Zugangspasswörter zu ändern. Informationen auf der Website des NCSC: Webseite gehackt - Was nun? (ncsc.admin.ch)

Nach der Bereinigung der Website empfehlen sich zusätzliche Massnahmen, um den Cyberkriminellen in Zukunft einen erneuten Zugang zu verwehren. Auf der Website des NCSC finden Sie dazu Massnahmen zum Schutz von CMS (ncsc.admin.ch)

4.4 Industrielle Kontrollsysteme & OT

Die Pandemie und extreme Wetterbedingungen haben die Wichtigkeit kritischer Infrastrukturen in den letzten Monaten zusätzlich in den Vordergrund gerückt. Viele Prozesse der kritischen Infrastrukturen werden durch operationelle Technologie (OT) unterstützt oder erst ermöglicht und von industriellen Kontrollsystemen (IKS) gesteuert. Neben Umwelteinflüssen und Fehlmanipulationen stellen auch böswillige Angriffe gegen diese Systeme oder damit verbundene Geräte ein Risiko der Verfügbarkeit und Integrität der kritischen Infrastrukturen dar.

4.4.1 «RedEcho» infiltriert indische Stromversorgung

Sicherheitsforschende von RecordedFuture berichteten Ende Februar von erfolgreichem Eindringen des im Bericht als «RedEcho»[85] bezeichneten Akteurs in Systeme mehrerer kritischer Infrastrukturbetreiber in Indien. Neben zwei Häfen waren vor allem Organisationen der Stromversorgung, speziell regionale Lastausgleichzentren, unter den Zielen der Angriffsreihe, welche unter anderem auf die Malware «Shadowpad»[86] setzte.

RecordedFuture findet in seiner Analyse keine Anzeichen auf Sabotageversuche, weist aber auf die zeitlich korrelierenden anhaltenden Spannungen an der indisch-chinesischen Grenze hin. In begleitender Berichterstattung der New York Times[87] wird die Hypothese einer abschreckenden Drohkulisse dieser missbräuchlich infiltrierten Netzwerke ins Spiel gebracht. Als Beispiel wird auch der Stromausfall in Mumbai vom Herbst 2020[88] erwähnt, ein Zusammenhang mit den Aktivitäten von «RedEcho» kann aber laut RecordedFuture nicht belegt werden.

---

85 Chinese Group RedEcho Targets the Indian Power Sector (recordedfuture.com)

86 ShadowPad (Malware Family) (fraunhofer.de)

87 China Appears to Warn India: Push Too Hard and the Lights Could Go Out (nytimes.com)

88 Siehe NCSC HJB 2020-2, Kap. 4.5.1.

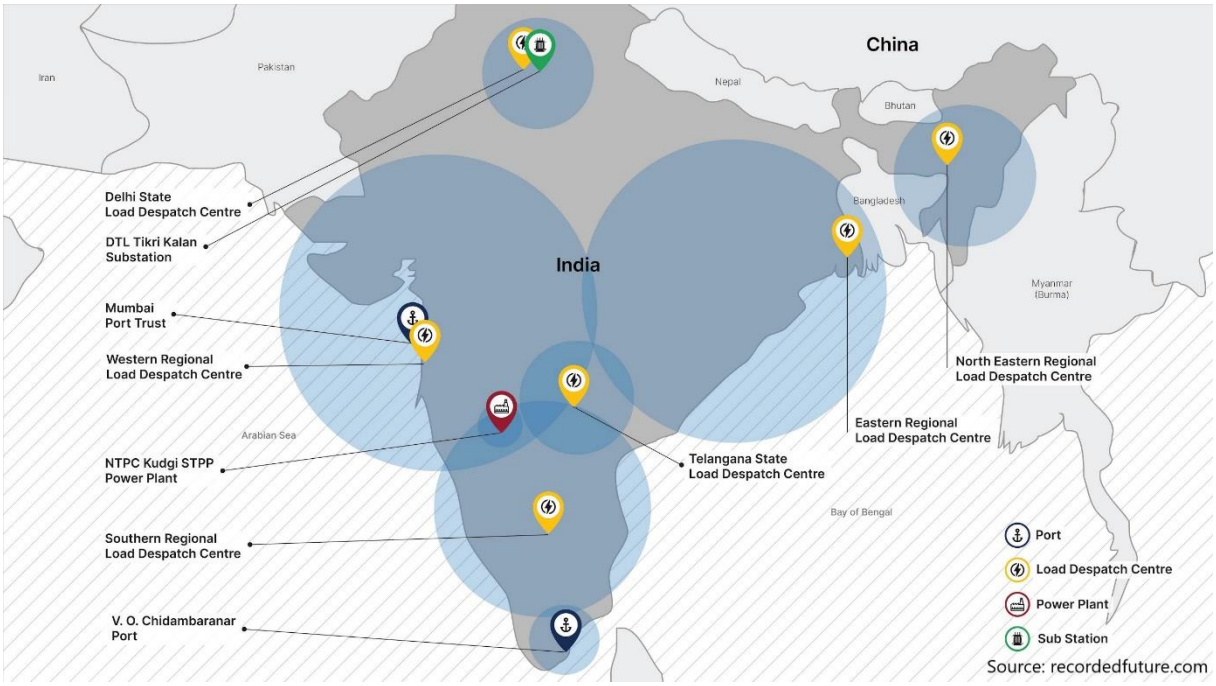


Abb. 10: Ziele von RedEcho.

4.4.2 Manipulationsversuche bei Wasserversorgung in Florida

Im Februar 2021 mache sich der Mauszeiger eines Steuerungscomputers in der Trinkwasseraufbereitung in Oldsmar, Florida, selbstständig.[89] Der diensthabende Techniker konnte gerade noch einschreiten, als der Eindringling aus der Ferne versuchte, den Natriumhydroxid-Pegel auf gesundheitsgefährdendes Niveau zu heben. Beinahe zum Verhängnis wurde der städtischen Infrastruktur eine ungenügend abgesicherte Fernzugriffsoftware,[90] über die sich der Saboteur Zugang zum Gerät verschaffte, über welches die Steuerung der Trinkwasseraufbereitung bedient wurde.

Hinweis / Empfehlungen:

Um auf Bedrohungen gegen industrielle Kontrollsysteme in der Prozesssteuerung vorbereitet zu sein, haben Branchenverbände von Strom-, Wasser-, Abwasser-, Gas- und Lebensmittelindustrie sowie Betriebe des öffentlichen Verkehrs zusammen mit dem Bundesamt für wirtschaftliche Landesversorgung (BWL) Branchenstandards als Hilfestellung erarbeitet:

Branchenstandards (bwl.admin.ch)

89 A Hacker Tried to Poison a Florida City's Water Supply, Officials Say (wired.com)

90 Compromise of U.S. Water Treatment Facility (cisa.gov)

4.5 Datenabflüsse

Auch in diesem Halbjahr sind Datenlecks ein aktuelles Phänomen, das in unterschiedlichen Zusammenhängen aufgetreten ist. Neben Ransomware-Gruppen, die die Drohung der Veröffentlichung von Daten in ihre Vorgehensweise integriert haben (siehe Kap. 4.2.3), können Datenlecks auch im Rahmen von Spionagekampagnen auftreten. In diesem Fall sind oft die Daten staatlicher Stellen oder Daten über geistiges Eigentum betroffen.

Der monetäre Wert bestimmter Datentypen, wie medizinische Daten, Kunden- oder Identitätsdaten und auch Bankdaten, macht sie zu bevorzugten Zielen. Aber auch vermeintlich weniger wertvolle Daten können von Cyberkriminellen für eine Vielzahl von Zwecken verwendet werden, z. B. um Szenarien zu erstellen, mit welchen dann Betrügereien via soziale Netzwerke durchgeführt werden, aber auch schlicht um E-Mail-Adressen zu sammeln, an die dann gezielt oder massenweise Phishing-, Malware- oder Betrugs-E-Mails gesendet werden können.

4.5.1 SITA: Diebstahl von Passagierdaten

Die Société Internationale de Télécommunications Aéronautiques (SITA), die weltweit führende Anbieterin von Passagierabfertigungssystemen für die Luftfahrtindustrie, war Opfer eines Cyberangriffs,[91] bei dem Passagierdaten von diversen Fluggesellschaften abgegriffen wurden.

Der Vorfall betraf das «Passenger Service System (PSS)», d. h. die Server, auf denen Passagierdaten von verschiedensten Fluggesellschaften gespeichert sind. Insbesondere wurden Millionen von Daten der Vielfliegerprogramme von Star Alliance und OneWorld kompromittiert. Betroffen sind dabei auch Kundendaten von etwa 1,35 Millionen Teilnehmenden des Programms «Miles-and-More».[92] Zu den Kunden der IT-Dienstleisterin gehört unter anderem die Swiss. Obwohl es im März, als SITA den Angriff meldete, den Anschein hatte, dass keine sicherheitskritischen persönlichen Daten gestohlen worden waren, informierte z. B. die indische Fluggesellschaft Air India fünf Wochen später, dass der Vorfall auch die Daten von 4,5 Millionen ihrer Fluggäste betraf und die gestohlenen Informationen in diesem Fall auch Pass- und Kreditkartendaten umfassten.[93]

4.5.2 Angriffe auf Social Networks und Data Scraping

Anfang April wurden die Daten von rund 533 Millionen Facebook-Profilen auf einem Hackerforum veröffentlicht. Betroffen waren Nutzerinnen und Nutzer aus mehr als hundert Ländern. Offenbar waren die Daten, welche u. a. Telefonnummern, E-Mail-Adressen, vollständige Namen, Geburtsdaten und Standorte der Nutzenden enthielten, schon seit Januar bekannt und wurden im Untergrundmarkt zum Kauf angeboten. Der eigentliche Datenabfluss geht aber wahrscheinlich auf einen früheren Zeitpunkt zurück. Facebook berichtete, das Datenleck sei

---

91 SITA statement about security incident (sita.aero)

92 Hacker erbeuten 1,3 Millionen Datensätze von Swiss- und Star-Alliance-Kunden (inside-it.ch)

93 Data-Breach-Notification.pdf (airindia.in)

vermutlich auf eine Sicherheitslücke zurückzuführen, die im August 2019 behoben worden war.[94]

Ende Juni wurde eine Datenbank mit 700 Millionen LinkedIn-Profilen zum Verkauf im Darknet angekündigt. Die Informationen, die über 90 Prozent der Nutzenden des sozialen Netzwerks betrafen, umfassen offenbar auch in diesem Fall keine Informationen über Kreditkarten oder Passwörter. Obwohl die Nutzenden vorsichtshalber aufgefordert wurden, ihre Passwörter zu ändern, bestreitet LinkedIn einen möglichen Einbruch in die Server und behauptet, dass es sich um einen Fall von «Data Scraping» handelt.[95]

Tatsächlich können grosse Datenmengen durch «Data Scraping» erlangt werden: Inhalte wie Telefonnummern und E-Mail-Adressen können von Websites, die öffentlich zugänglich sind, mit verschiedensten Techniken systematisch extrahiert werden. Solche Tätigkeiten werden auch von Unternehmen in unterschiedlichen Bereichen ausgeübt, z. B. zur Marketing-Optimierung oder für Business Intelligence. Dazu gehört das chinesische Unternehmen SocialArks, eine Datenverwaltungsplattform für gezielte Werbung, die Daten von sozialen Netzwerkplattformen wie Facebook, Instagram und LinkedIn sammelt. Dies enthüllte ein falsch konfigurierten Server, der mehr als 400 GB an öffentlichen und privaten Profildaten von 214 Millionen Social-Media-Nutzenden und insgesamt 318 Millionen ungeschützte Datensätze umfasste. In diesem Fall enthielt die Datenbank aus unerklärlichen Gründen auch Daten, die nicht öffentlich zugänglich waren.[96]

Schliesslich können Daten aus verschiedenen Datenlecks zu einem grossen Informationspaket kombiniert werden, das durch seinen Umfang besonders attraktiv ist. Dies ist der Fall bei der so genannten «Compilation of Many Breaches», dem grössten bisher gefundenen Datensatz, der 3,2 Milliarden E-Mail/Passwort-Kombinationen aus alten Datenlecks verschiedener Unternehmen enthält, darunter auch solche von Netflix und LinkedIn.[97]

Schlussfolgerung / Empfehlungen:

Der sorgfältige und verantwortungsbewusste Umgang mit Daten ist für Unternehmen ein wichtiges Themenfeld. Neben angemessenen Sicherheitsmassnahmen sollte sich jedes Unternehmen auch auf das Szenario «Datenleck» vorbereiten und einen entsprechenden Notfallplan (sog. «Data Breach Response-Plan») vorgängig erstellen, welcher im Ereignisfall ein schnelles und koordiniertes Handeln ermöglicht.

Internetdienste, die Datensammlungen öffentlich zugänglich machen, sollten ihre Plattformen durch geeignete Vorkehrungen vor automatisierten (Massen-) Abfragen schützen.

---

94 Bot Lets Hackers Easily Look Up Facebook Users' Phone Numbers (vice.com); 533 million Facebook users' personal data leaked online (cyberscoop.com).

95 LinkedIn denies exposure of 700 million user records is a data breach (computerweekly.com)

96 The SocialArk Data Breach Uncovered the Open Source Paradox (cybersecurity-magazine.com); Millions of Social Profiles Leaked by Chinese Data-Scrapers (threatpost.com).

97 COMB: over 3.2 Billion Email/Password Combinations Leaked (cybernews.com)

Um sich als Privatperson vor «Scraping» zu schützen, sollten Sie den öffentlichen Zugang zu Ihren sozialen Profilen einschränken und generell über die Inhalte nachdenken, die Sie online veröffentlichen.

Es ist auch ratsam, auf die Einstellungen der von Ihnen verwendeten Anwendungen zu achten und diesen nicht mehr Berechtigungen geben, als sie benötigen.

Weitere Informationen finden Sie auf der NCSC Website: Datenabfluss (ncsc.admin.ch)

4.6 Spionage

4.6.1 Nobelium: neue Kampagnen nach SolarWinds

Am 27. Mai veröffentlichte Microsoft einen Artikel und warnte darin vor einer neuen E-Mail-Kampagne zur Verbreitung von Malware durch den von Microsoft als «Nobelium» bezeichneten fortschrittlichen Akteur (Advanced Persistent Threat, APT). «Nobelium» war unter anderem für den Angriff auf SolarWinds[98] verantwortlich. Die Kampagne folgte auf eine Versuchsphase, die von Anfang 2021 bis Ende Mai dauerte. In diesem Zeitraum beobachtete Microsoft eine Reihe technischer Entwicklungen bei der Übermittlungsmethode von Phishing-Nachrichten sowie bei der Erstellung von Profilen der Empfängerinnen und Empfänger. Diese Fähigkeit zur ständigen Innovation und zur Übernahme von zielspezifischen Tools und Infrastrukturen macht «Nobelium» zu einer hochentwickelten Bedrohung und erschwert seine Entdeckung. Am 25. Mai nutzte die Kampagne dann den seriösen Massen-Mailingdienst «Constant Contact», um sich als amerikanische Entwicklungsorganisation auszugeben, und richtete sich an über 3'000 Konten von 150 Organisationen, hauptsächlich in den USA. Insbesondere wurde auf NGOs, Forschungseinrichtungen, Regierungsstellen und internationale Agenturen gezielt. Die E-Mails wiesen auf ausländische Bedrohungen für die US-Wahlen von 2020 hin und enthielten eine URL, die die Opfer zunächst auf den legitimen «Constant Contact»-Dienst verwies, der sie dann auf die von der Gruppe kontrollierte Infrastruktur umleitete.[99]

4.6.2 «Hafnium» nutzt MS Exchange aus

Im März 2021 gab Microsoft bekannt, dass eine Gruppe namens «Hafnium» eine Reihe von vormals unbekannten Schwachstellen in Microsoft Exchange-Servern[100] ausgenutzt habe.[101] «Hafnium» war bereits zuvor im Verdacht, sich mit gestohlenen Passwörtern Zugang zu Microsoft Exchange-Servern zu verschaffen. Dabei hatte die Akteurin über längere Zeit Zugriff auf die Netzwerke der betroffenen Unternehmen und Behörden. Unter den Zielen waren Hoch-

---

98 Siehe NCSC HJB 2020-2, Kap. 4.7.2.

99 New sophisticated email-based attack from NOBELIUM (microsoft.com)

100 Siehe oben Kap. 3.1.1.

101 HAFNIUM targeting Exchange Servers with 0-day exploits (microsoft.com)

schul- und Forschungseinrichtungen auf dem Gebiet der Infektionskrankheiten, Anwaltskanzleien, Verteidigungsunternehmen, ThinkThanks und NGOs.[102] «Hafnium» exfiltriert Daten in der Regel auf File-Sharing-Websites wie «MEGA».[103]

4.7 Phishing und Social Engineering

4.7.1 Phishing

Im ersten Halbjahr 2021 wurden 4'682 Phishing-Webseiten verifiziert, nachdem sie über das vom NCSC betriebenen Portal antiphishing.ch gemeldet wurden. Im Vergleich zur zweiten Jahreshälfte 2020 mit 4'498 detektierten Phishing-Webseiten ist das Niveau, mit einer leichten Zunahme, praktisch gleichgeblieben.

Das NCSC beobachtet dabei eine Verlagerung der Phishing-Versuche von grossen internationalen Marken zu Unternehmen, die auf dem Schweizer Markt tätig sind. Zu den derzeitigen Zielgruppen gehören nach wie vor der Finanzsektor,[104] aber auch Logistikunternehmen,[105] Internetanbieter[106] und weitere.

Abb. 11: Anzahl durch das NCSC überprüfte und bestätigte Phishing URLs pro Woche im ersten Semester 2021. Aktuelle Daten finden Sie unter: https://www.govcert.admin.ch/statistics/phishing/

---

[102] HAFNIUM, Operation Exchange Marauder, Group G0125 (mitre.org)

[103] HAFNIUM (Threat Actor) (fraunhofer.de)

[104] Viseca Phishing Mails - nicht autorisierte Transaktion - Zugriff eingeschränkt (cybercrimepolice.ch)

[105] Phishing Mail im Namen der Post - Paket konnte nicht geliefert werden, da kein Zoll bezahlt wurde (cybercrimepolice.ch)

[106] E-Mail angeblich von der Swisscom (Schweiz) AG betr. Rückerstattung (cybercrimepolice.ch); weiterhin aktuell sind auch Angriffe gegen Website-Inhaber: Phishing Attackers Targeting Webmasters (govcert.admin.ch).

Bei Phishing- und anderen Social Engineering-Angriffen sind die angewendeten Inhaltstaktiken vielseitig ausgelegt. In der Regel sind es Themen mit angeblichen Vorkommnissen, die einen alltäglichen Bezug vortäuschen und oft als real wahrgenommen werden. Die Nachrichten haben häufig auf den ersten Blick das Aussehen von einem vertrauenswürdigen und bekannten Unternehmen und beinhalten natürlich ein entsprechendes Firmenlogo, das für diese Zwecke missbräuchlich verwendet wird.

4.7.2 Smishing

Auch SMS und andere Kurznachrichtendienste werden zunehmend für Phishing, sogenanntes «Smishing»,[107] missbraucht. Solche Nachrichten kommen thematisch ebenfalls mit alltäglichem Inhalt, versehen mit einem Link, auf dem Mobiltelefon daher. Der Link in der Nachricht führt auf eine eigens von Kriminellen gestaltete Webseite, auf welcher man aufgefordert wird, persönliche Daten oder Kreditkartendetails einzugeben.

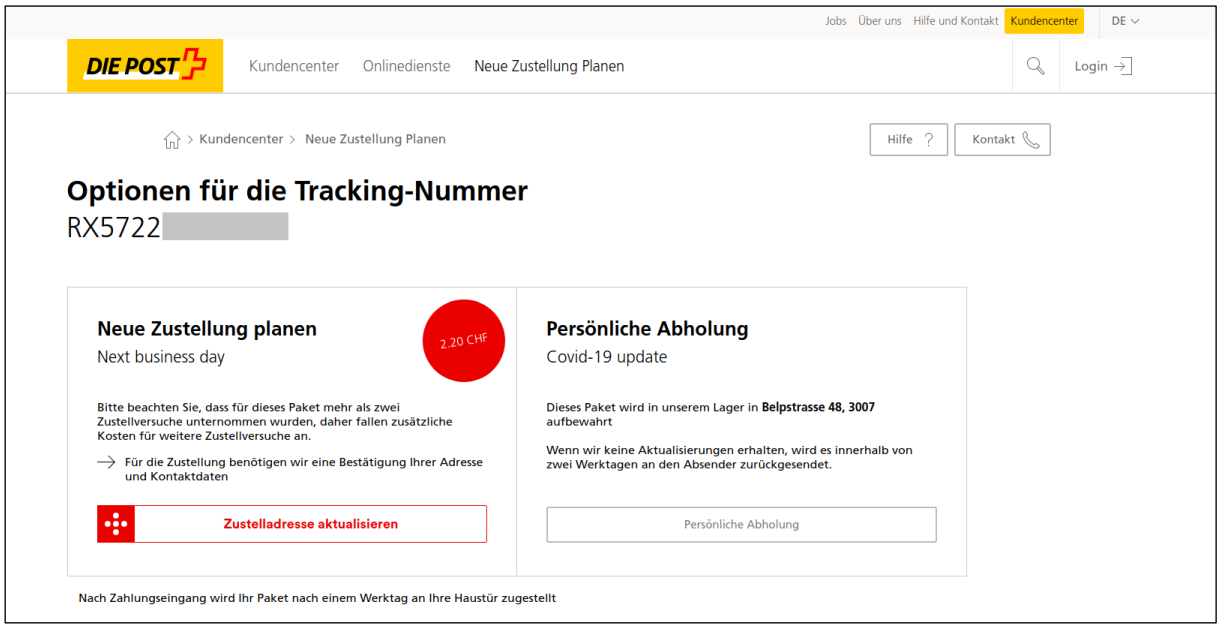


Abb. 12: Beispiel einer nachgeahmten Webseite zum Abgreifen von Zugangsdaten.

4.7.3 Social Engineering

Es gibt mittlerweile verschiedene Schadsoftware-Familien, die auf infizierten Systemen unter anderem E-Mail-Konversationen abgreifen. E-Mail-Konversationen können natürlich auch durch Zugriffe mit «gephishten» Zugangsdaten zu Kriminellen abfliessen. Als Konsequenz daraus werden vermehrt E-Mails gezielt an Personen versendet, die an solchen E-Mail-Konversationen beteiligt waren. Häufig ist der vermeintliche Absender eine andere Person aus dieser Konversation. Die Absenderadresse ist dabei entweder gefälscht oder aber das E-Mail wird von einem kompromittierten Konto und entsprechend mit der echten Adresse aber nicht von der berechtigten Person gesendet. Das E-Mail sieht dann so aus, als ob es (nun mit einem präparierten Anhang) erneut gesendet wurde oder dass es eine Fortsetzung der Konversation

---

107 SMS - Sie haben eine DIE POST-Sendung (cybercrimepolice.ch)

ist. Falls zusätzlicher Text eingefügt wird, ist dieser (bislang noch) meist auf Englisch und sehr generisch gehalten (z. B. «Guten Tag. Bitte überprüfen Sie die angehängten Dokumente» oder «Hallo, hier ist eine interessante Information in dem angehängten Dokument») und auch allfällige Dateianhänge haben entweder nichtssagende Namen (z. B. «Dokumentation (60243).xls», «docs_(20210412).xls» oder «Anwendung (756.466).xls») oder Bezeichnungen, die Neugier wecken sollen (z. B. «CompensationClaim.xls» oder «Lohnabrechnungen.xls». Das Anklicken eines solchen Anhangs ist der erste Schritt zu einer Infektion des Geräts.

Empfehlungen:

- Seien Sie nicht nur bei E-Mails und SMS von unbekannten Personen kritisch, sondern lassen Sie auch bei (vermeintlich) bekannten Absendern Vorsicht walten.
- Werden Sie misstrauisch, wenn Sie unerwartet Dokumente ohne weiteren Kommentar erhalten oder der Text im Mail sehr generisch gehalten ist.
- Wenn Sie beim Öffnen einer Datei dazu aufgefordert werden, Makros zu aktivieren, melden Sie dies Ihren Sicherheitsverantwortlichen.
- Seien Sie skeptisch, wenn Sie E-Mails oder SMS bekommen, die darauf ausgelegt sind, Ihre Neugier zu wecken oder eine Aktion von Ihnen verlangen (einem Link folgen oder ein Dokument öffnen). Häufig wird Ihnen zur Ausführung dieser Aktion eine Frist gesetzt, um den Druck zu erhöhen.
- Klicken Sie in verdächtigen Nachrichten auf keine Anhänge und folgen Sie keinen Links, auch nicht aus reiner Neugier – Sie riskieren sonst, Ihr Gerät mit Schadsoftware zu infizieren oder auf dubiosen Webseiten zu landen. Fragen Sie im Zweifelsfall beim vermeintlichen Absender über eine bereits bekannte oder z. B. auf seiner Webseite angegebene Kontaktmöglichkeit nach, worum es sich genau handelt und ob das Mail tatsächlich von ihm stammt.

4.8 Betrug: Aktuelle Varianten von Investitionsbetrug

Der Grossteil der beim NCSC eingehenden Meldungen betrifft verschiedene Arten von Betrugsversuchen. Eine Variante ist der so genannte Investitionsbetrug, auch bekannt als Anlagebetrug. Via E-Mail, Webseiten und Soziale Medien ist es sehr einfach, entsprechende Lockangebote zu verbreiten. Aktuell wird der Hype um Kryptowährungen stark ausgenutzt und Betrüger versprechen, dass man mit einer kleinen Investition in solche Währungen in kürzester Zeit einen hohen Gewinn erzielen könne. In manchen Fällen erfolgt nach einer Einzahlung sogar wieder eine (kleinere) Auszahlung. Dies jedoch nur, um Vertrauen aufzubauen und die Opfer zu überzeugen, grössere Investitionen zu tätigen.[108]

[108] Krypto Anlagebetrüger ködern Nutzer mit SMS (cybercrimepolice.ch)

Von: Zahlungsüberprüfung
Gesendet: Freitag, 6. August 2021
An: [redacted]
Betreff: Zahlung akzeptiert

Geschätzter Gewinn für August: €6.461,01 BitTraders

Mögliche Gewinne für August:
%-Rücklaufquote:
Startdatum:
End-Datum:

€6.461,01
2431%
03/08/2021
20/08/2021

Wenn Sie heute investieren, können Sie einen Gewinn von 6.461,01 Euro erwarten, wenn Ihre Investition am 03/08/2021 abgeschlossen ist.

Befolgen Sie die folgenden Anweisungen, um zu beginnen.

Profil erstellen
Anweisungen:
Profil erstellen --> Investitionen einleiten --> Sehen Sie, wie Ihr Geld wächst --> Ziehen Sie Ihren Investitionsgewinn auf Ihr Bankkonto ab

Mit freundlichen Grüßen,
BitTraders

Abb. 13: Beispiel eines Werbemails mit enorm hohen Gewinnversprechen.

Schon in den vergangenen Jahren gab es Meldungen bezüglich gefälschter Online-Handelsplattformen und entsprechender Werbeportale, welche oft die Namen von Persönlichkeiten wie Roger Federer und DJ Bobo verwendeten. In erfundenen Interviews wurde behauptet, sie hätten ihren Reichtum den Kryptowährungen zu verdanken.[109]

Von: Kronen Zeitung
Gesendet: Dienstag, 6. Juli 2021
An: [redacted]
Betreff: Dietrich Mateschitzs neueste Investition sorgt für Begeisterung bei Fachleuten und Angst bei den Großbanken

Dietrich Mateschitz neueste Investment-Überraschungsexperten und Großbanken.

ÖsterreicherInnen verdienen von zu Hause aus bereits Millionen Euro mit diesem "Vermögensschlupfloch" – aber ist es legitim?

Der österreichische Geschäftsmann Dietrich Mateschitz gibt ehrlich zu, wie er sein Geld verdient und teilt es jetzt mit allen.

aktuelles Interview mit Dietrich Mateschitzs

Lesen Sie die ganzen Nachrichten

Siehe auch
Was ist die deutsche BTC-Ära und wie funktioniert sie?

privacy policy | unsubscribe

Abb. 14: Beispiel eines betrügerischen Mails, das mit dem reichsten Österreicher wirbt.

[109] Siehe MELANI HJB 2019-2, Kap. 4.4.5.

Die aktuellen Varianten von Investmentbetrug sind jeweils in den NCSC-Wochenrückblicken beschrieben.[110] Um in der Werbeflut aufzufallen, scheinen sich die Betrüger zurzeit mit unrealistischen Renditen regelrecht zu überbieten. In einem Fall wurde bei einem Einsatz von 250 Euro ein Gewinn von 12'000 Euro innerhalb von 72 Stunden in Aussicht gestellt.[111] Weiter versuchen die Kriminellen die Opfer ein zweites Mal zu betrügen, indem sich nach einer Weile vermeintliche Anwälte, Notare oder sogar Strafverfolgungsbehörden und Regulatoren melden und dem Opfer versprechen, das Geld zurückzuholen. Dabei wird in einem ersten Schritt eine vertrauensvolle Beziehung aufgebaut und es müssen relativ sensible Daten wie beispielsweise eine Kopie eines Ausweises, eine IBAN-Nummer oder ähnliches angegeben werden. In einem zweiten Schritt werden für die angebliche Hilfe dann «Gebühren» verlangt. In einigen Fällen werden auch improvisierte Webseiten der angeblichen Hilfsorganisationen eingerichtet, um sich das Vertrauen der Opfer zu sichern.[112]

Die Gefahr besteht darin, grosse Geldbeträge zu verlieren. In einem dem NCSC gemeldeten Fall resultierte ein Verlust von über einer Million Schweizer Franken.[113]

Schlussfolgerung / Empfehlung:

Versprechen von aussergewöhnlichen Renditen in kurzer Zeit (und ohne Arbeit) sind dubios.

Falls Ihnen ein Schaden entstanden ist, so melden Sie sich persönlich bei Ihrer örtlichen Polizeistelle und erstatten eine Strafanzeige.

Seien Sie vorsichtig, wenn Ihnen nach einem Betrugsfall plötzlich von Dritten Hilfe angeboten wird. Leisten Sie insbesondere keine weiteren Zahlungen, auch nicht angebliche Gebühren, um das verlorene Geld zurück zu holen.

Weitere Informationen finden Sie auf der NCSC Website: Investmentbetrug (ncsc.admin.ch)

Auf der Seite der Schweizer Finanzmarktaufsicht FINMA finden Sie Informationen zu bewilligten Finanzdienstleistern in der Schweiz (finma.ch). Ist ein Finanzdienstleister nicht auf dieser Liste, ist besondere Vorsicht geboten. Überprüfen Sie den Finanzdienstleister anhand von Erfahrungsberichten im Internet. Die FINMA führt ebenfalls eine nicht abschliessende Warnliste mit Unternehmen, die möglicherweise ohne Bewilligung eine Tätigkeit ausüben, bewilligungspflichtig sind und unter die Aufsicht der FINMA fallen (finma.ch).

---

110 Im Fokus (ncsc.admin.ch)

111 Die Woche 14 im Rückblick (ncsc.admin.ch)

112 Die Woche 21 im Rückblick (ncsc.admin.ch)

113 Die Woche 11 im Rückblick (ncsc.admin.ch)