3. November 2022 | Nationales Zentrum für Cybersicherheit NCSC

Halbjahresbericht 2022/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

Management Summary

Cyber in bewaffneten Konflikten

Bewaffnete Konflikte werden zunehmend auch mithilfe von Cyberangriffen geführt. Urheber solcher Angriffe können nebst staatlicher Akteure auch nichtstaatliche Angreifer wie Hacktivisten oder kriminelle Gruppierungen sein. Insbesondere der Ukraine-Konflikt zeigt, wo Cyber als Mittel eingesetzt werden kann. Diese vielschichtige Thematik bildet das Fokusthema und wird im aktuellen Bericht von den verschiedensten Seiten her beleuchtet.

Droh-Mails: Massive Zunahme

Im ersten Halbjahr 2022 verzeichnete das NCSC eine massive Zunahme von Meldungen aus der Bevölkerung. Bis Ende Juni gingen beim NCSC 17'186 Meldungen ein. Im Vergleich zur Vorhalbjahresperiode mit 10’234 Meldungen entspricht dies einer Zunahme von rund 70 Prozent. Hauptursache dieser beachtlichen Steigerung sind vor allem Meldungen zu Droh-E-Mails im Namen der Polizei, so genannte Fake-Extortion-E-Mails.

Betrugsfälle weiterhin als nationale Spitzenreiter

Im Berichtszeitraum betrafen die meisten Meldungen an das NCSC verschiedenste Betrugsformen (10'447 Meldungen). Rund die Hälfte davon waren Meldungen zu Fake-Extortion-E-Mails (5'872 Meldungen). Weitere Betrugsfälle fielen auf Vorschussbetrug (1'834), Fake Sextortion (615) und Kleinanzeigenbetrug (419). Meldungen zu Phishing und Schadsoftware bewegten sich im Vergleich zur Vorhalbjahresperiode auf dem gleichen Niveau.

Hohe Schäden bei Investment-Betrug und Rechnungsmanipulationsbetrug

Das höchste Schadenspotential bei Unternehmen verzeichnete das NCSC neben Ransomware beim Phänomen des Rechnungsmanipulationsbetrugs (Business E-Mail-Compromise). Im ersten Halbjahr 2022 erhielt das NCSC diesbezüglich 47 Meldungen mit einer Schadenssumme von insgesamt 2.3 Millionen Schweizer Franken. Der Investment-Betrug gehört, insbesondere bei Privatpersonen, zu den Delikten mit den höchsten Schadenssummen. In der ersten Jahreshälfte 2022 wurden dem NCSC Fälle mit einer Schadenssumme von insgesamt mehr als drei Millionen Schweizer Franken gemeldet.

Leichter Rückgang bei Meldungen zu Ransomware

Obwohl die Meldungen zu Ransomware im Vergleich zur Vorhalbjahresperiode von 91 auf 83 Meldungen leicht zurückgegangen sind, ist diese Angriffsform weiterhin die akuteste Cyberbedrohung, der Organisationen in der Schweiz ausgesetzt sind. Seit Jahresbeginn sind in der Schweiz verschiedene Organisationen in diversen Sektoren Ziele von Ransomware-Angriffen geworden.

Spoofing im Aufwind

Einen enormen Anstieg verzeichnete das NCSC auch bei den Meldungen zu gefälschten (gespooften) Telefonnummern. Dabei fälschen dubiose Callcenter die angezeigte Rufnummer, in dem sie Telefonnummern von Privatpersonen anzeigen lassen. So sollen die Angerufenen verleitet werden, den Anruf entgegenzunehmen. Im ersten Halbjahr 2022 gingen beim NCSC 319 Meldungen ein. Im Berichtszeitraum des Vorjahres waren es nur gerade 17 Meldungen.

Editorial

Im letzten halben Jahr kommt man nicht darum herum beim Thema Cyber auch über den Ukraine-Konflikt zu sprechen. Direkt hatte der Konflikt zwar kaum Auswirkungen auf den Cyberraum der Schweiz – abgesehen davon, dass die Bedrohung durch Ransomware etwas nachliess. Dies hat primär zwei Gründe. Gruppierungen, welche russische und ukrainische Mitglieder hatten, haben sich zerstritten und diverse Gruppierungen begannen sich im Konflikt zu engagieren und waren damit beschäftigt.

Der Ukraine-Konflikt zeigt auch, wo Cyber als Mittel eingesetzt werden kann und wo die Grenzen sind. Cyber wird im Konflikt vor allem für Informationsoperationen oder taktische Angriffe, primär auf Kommunikationsmittel, welche militärischen Zwecken dienen, genutzt. Breit angelegte Cyberangriffe auf Infrastrukturen zeigen im Konflikt nur wenig Wirkung. Bomben sind oft ein effizienteres und günstigeres Mittel. Auch können die Kollateralschäden dieser Angriffe nur schlecht kontrolliert werden und es besteht das Risiko von sogenannten «Spillover»-Effekten, welche zu einer unkontrollierten Ausweitung führen könnten.

Anders sieht dies im Vorfeld des Konfliktes aus, wo versucht wurde, strategisch wichtige Infrastrukturen der Ukraine mittels Cyberangriffen lahmzulegen. Diese Angriffe waren jedoch nur sehr bedingt erfolgreich. Dies primär, da sich die Cyberabwehr in der Ukraine gut vorbereitet hat. Der Schlüssel hierbei sind zivile Behörden und Firmen. Denn der Konflikt zeigt: Die Armee muss auch im Cyberspace kämpfen, ist aber mit der Kriegsführung absorbiert. Vor und auch während dem Konflikt ist es daher existentiell wichtig, dass digitale Infrastrukturen durch zivile Mittel gesichert werden können und im Krisenfall die Zusammenarbeit zwischen den zivilen und militärischen Stellen sichergestellt ist. Ganz wie im physischen Raum, wo bei einem Bombeneinschlag auch die Feuerwehr löschen muss, da die Armee mit Kampfhandlungen beschäftigt ist. In seinem Gastbeitrag geht Stéphane Duguin vom CyberPeace Institute auf die Problematik von Cyberangriffen auf zivile Infrastrukturen ein. Es folgt eine Diskussion von Auswirkungen von Cyberoperationen in der Ukraine sowohl in der Region als auch weltweit.

Für die Schweiz dominieren weiterhin Meldungen über Online-Betrug, welche um 70 Prozent zugenommen haben. Hierbei sind vor allem Fake Extortion, Vorschussbetrug, Fake Sextortion und Kleinenzeigenbetrug die Mittel der Betrüger. In diesem Bericht diskutieren wir die aktuellen Maschen und ihre Auswirkungen.

In der Lageübersicht diskutieren wir in diesem Bericht als Schwerpunkt, wie der initiale Zugang zu Systemen erlangt wird. Natürlich gibt es auch Empfehlungen, wie solche Angriffe erschwert werden können. Denn leider ist es immer noch so, dass viele grundlegende Cyber-Hygienemassnahmen wie zum Beispiel das Aktuell-Halten von Systemen von vielen nicht getroffen werden. Dies macht es den Angreifern einfacher als es sein muss. Selbstredend gibt es auch wieder eine Übersicht über die wichtigsten Malware-Familien und zum Thema Ransomware. Abgerundet wird der Bericht mit dem Vorstellen einiger konkreter Fälle.

Ich wünsche viel Spass bei der Lektüre. Wie auch in der Vergangenheit bitten wir Sie, werte Leserschaft, uns Ihr Feedback zu geben. Nur so können wir den Halbjahresbericht laufend an Ihre Bedürfnisse anpassen.

Florian Schütz, Delegierter des Bundes für Cybersicherheit

2 Gastbeitrag des CyberPeace Institute

Stéphane Duguin ist Geschäftsführer des CyberPeace Institute, einer neutralen und unabhängigen Nichtregierungsorganisation (NRO), die sich für den Cyberfrieden einsetzt. Das Institut verfolgt und analysiert Cyberangriffe gegen zivile Objekte über seine Cyber Attacks in Times of Conflict Platform #Ukraine.

Wie ein bewaffneter Konflikt den Cyberspace für uns alle destabilisiert

Stéphane Duguin,
CEO CyberPeace Institute

Neben dem Land-, See- und Luftraum werden bewaffnete Konflikte zunehmend auch im Weltraum, im Informationsraum und im Cyberspace ausgetragen. Der grenzenlose Charakter dieser Bereiche hat dazu geführt, dass ein bewaffneter Konflikt zwischen Staaten Auswirkungen haben kann, die über die militärischen Ziele der Parteien hinausgehen. Die militärische Invasion in der Ukraine im Februar 2022, der eine Reihe von Cyberangriffen auf ukrainische öffentliche Einrichtungen und Organisationen vorausging, setzte den Rahmen für einen Krieg, der heute sowohl online als auch am Boden ausgetragen wird. Angriffe und Operationen, die im Zusammenhang mit dem Krieg zwischen der Russischen Föderation und der Ukraine im Cyberspace durchgeführt wurden, haben den Cyberspace destabilisiert und bedrohen die sichere und vertrauenswürdige Nutzung von Technologie.

Wenn kritische Infrastrukturen unter Beschuss geraten

Cyberangriffe auf kritische Infrastrukturen sind keine Seltenheit – eine Ölpipeline (Vereinigte Staaten, 2021), Wasserpumpstationen (Israel, 2020), Gesundheitsdienste (Vereinigtes Königreich, 2017) – und der bewaffnete Konflikt in der Ukraine hat dies deutlich gezeigt. Im Vorfeld und in den ersten Tagen des Konflikts wurden sechs verschiedene Malware-Stränge zur Datenlöschung gegen ukrainische Organisationen in kritischen Sektoren eingesetzt. Malware kann erheblichen Schaden anrichten, wenn sie wichtige Dienste für die Zivilbevölkerung unterbricht. Der Angriff auf das KA-SAT-Satellitennetz von Viasat, der Berichten zufolge auf Aspekte der militärischen Führung in der Ukraine abzielte, führte zu einem erheblichen Verlust der Internetkommunikation für Nutzer in ganz Europa und hatte Auswirkungen auf ein deutsches Energieunternehmen, das den Fernüberwachungszugriff auf über 5’800 Windkraftanlagen verlor. Dieser Angriff und andere Malware, die während des Konflikts zur Datenlöschung eingesetzt wurde, werden hochentwickelten staatlichen Akteuren zugeschrieben.

Unkonventionelle Akteure, die den Cyberspace stören

Neben traditionellen Konfliktparteien haben in diesem bewaffneten Konflikt auch andere Akteure eine wichtige Rolle gespielt, und die Grenzen zwischen ihnen verschwimmen zunehmend. Die von der ukrainischen Regierung ins Leben gerufene «IT Army of Ukraine» ist ein weniger konventioneller Akteur, dessen DDoS-Angriffe (Distributed Denial of Service) die russischen Online-Ressourcen stark beeinträchtigen. Sogenannte Hacktivistenkollektive haben die Netzwerke von Regierungseinrichtungen, staatlichen Unternehmen und anderen Organisationen mit DDoS-Angriffen überflutet. Diese Akteure haben eine aktive Rolle bei der Störung

der für die Öffentlichkeit zugänglichen Online-Infrastruktur ihrer Ziele gespielt, was zum Ausfall von Websites und Portalen führte, von denen viele von der Bevölkerung für Routinetätigkeiten wie die Buchung von Fahrkarten oder die Abgabe von Steuererklärungen genutzt werden.

Eine beträchtliche Anzahl von NATO-Mitgliedsstaaten, notabene nicht Konfliktparteien, waren in den letzten Monaten besonders von Cyberangriffen durch Hacktivistenkollektive betroffen, die offenbar als Reaktion auf ihre öffentlichen Positionen zu geopolitischen, ideologischen oder wirtschaftlichen Themen erfolgten.

Die Veröffentlichung grosser Mengen sensibler Daten ist während des Konflikts zu einem festen Bestandteil der Cyberbedrohungslandschaft geworden. Im Namen des Anti-Kriegs-Aktivismus haben Kollektive eine beträchtliche Anzahl von Hack- und Leak-Angriffen durchgeführt, die dazu führten, dass sensible Kunden- und Unternehmensdaten, einschliesslich personenbezogener Daten, öffentlich zugänglich gemacht wurden. Diese Angriffe werfen erhebliche Fragen in Bezug auf den Schutz von Personen, den Datenschutz und das Potenzial für eine böswillige Nutzung dieser Daten in der Zukunft auf.

Eine Reihe von Fragen stellt sich bezüglich dieser weniger traditionellen Akteure, die an dem bewaffneten Konflikt beteiligt sind, nicht zuletzt im Hinblick auf Versuche, Angriffe zuzuordnen – d. h. zu bestimmen, wer einen bestimmten Cyberangriff entwickelt, gestartet oder autorisiert hat.

Schutz «unseres» Cyberspace

Cyberangriffe und -operationen, die im Rahmen eines Krieges oder in Friedenszeiten von staatlichen und nichtstaatlichen Akteuren durchgeführt werden, haben zur Destabilisierung des Cyberraums und damit der Gesellschaft beigetragen, die so stark von der Technologie abhängig ist. Diese Destabilisierung hat lang anhaltende Auswirkungen, von denen viele noch nicht erforscht sind. Um ein offenes, freies, stabiles und sicheres digitales Umfeld zu gewährleisten, ist ein verantwortungsbewusstes Verhalten im Cyberspace unabdingbar und erfordert von allen Beteiligten Engagement und Einsatz:

- Ob im Krieg oder in Friedenszeiten, Cyberangriffe sollten internationales Recht und Normen respektieren und sich nicht gegen kritische Infrastrukturen richten, die für das Überleben der Zivilbevölkerung unerlässlich sind.
- Der potenzielle Schaden und die Auswirkungen auf die Menschen sowie die humanitären Folgen des Einsatzes von Cyberangriffen müssen eine vorrangige Erwägung sein, bevor diese eingesetzt werden.
- Die Staaten müssen sicherstellen, dass Cyberangriffe, die gegen internationale Gesetze und Normen verstossen, geahndet werden.
- Öffentliche Einrichtungen wie Computer Emergency Response Teams (CERTs) sind für den Schutz von Systemen und die Untersuchung von Angriffen durch effektive Zusammenarbeit und Informationsaustausch unerlässlich.
- Private Unternehmen können eine Rolle bei der Entwicklung und Bereitstellung sicherer Produkte und Dienstleistungen für die Schwächsten der Gesellschaft spielen und Regierungen und ihre Bürger proaktiv schützen.
- Und nicht zuletzt können zivilgesellschaftliche Organisationen dazu beitragen, Cyberangriffe und deren Auswirkungen auf die Menschen zu dokumentieren und zu analysieren, um Untersuchungen zu erleichtern und die politische Debatte zu unterstützen.

3 Fokus: Cyber in bewaffneten Konflikten

Dieser Artikel beleuchtet die wichtigsten Ereignisse, die sich während des gegenwärtigen Kriegs zwischen Russland und der Ukraine im Cyberspace zugetragen haben. Ein wesentlicher Teil dessen, was sich im Cyberspace abspielt, sind Beeinflussungsaktivitäten. Diese haben zum Ziel, Ideen, Meinungen oder Motivationen bestimmter Zielgruppen zu beeinflussen und in deren Entscheidungsprozesse einzugreifen. In diesem Artikel geht es jedoch nicht um solche Beeinflussungsaktivitäten, sondern um Aktivitäten im Cyberspace, die direkte Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder auch physische Auswirkungen haben.[1]

3.1 Cyberaktivitäten vor der Invasion

Die Ukraine sieht sich seit mehreren Jahren mit Cybersabotageaktivitäten konfrontiert. Hier drei prominente Beispiele:

- 2015 verursachte die dem russischen Cyberakteur Sandworm zugeschriebene Malware «BlackEnergy3» Stromausfälle von bis zu sechs Stunden, von denen mehrere Hunderttausend Verbraucherinnen und Verbraucher betroffen waren.[2]
- 2016 wurde Sandworm wiederum aktiv, diesmal mit «Industroyer», einer speziell entwickelten Malware, um industrielle Kontrollsysteme der Stromversorgung zu befallen, was in Teilen Kiews zu etwa einstündigen Stromausfällen führte.[3]
- Im Unterschied zu den gezielten Angriffen auf die Stromversorgung 2015 und 2016 kam es 2017 zur massenhaften Verbreitung der Malware «NotPetya». Diese verschlüsselt zuerst die Daten des infizierten Systems und lässt dann eine Mitteilung erscheinen, in der ein bescheidenes Lösegeld gefordert wird. Ausgangspunkt des «NotPetya»-Befalls war ein manipuliertes Update einer ukrainischen Buchhaltungssoftware, das zahlreiche Infektionen von Systemen in der Ukraine zur Folge hatte. Die Malware verbreitete sich aber auch über die ukrainischen Grenzen hinaus und befiel Systeme in mehr als 65 Ländern. Ihre Funktionsweise, die Ausrichtung auf die Ukraine und das für Ransomware ungewöhnliche Fehlen einer Entschlüsselungsmöglichkeit deuten darauf hin, dass es nicht um Erpressung, sondern um Sabotage ging.[4]

Der ukrainische Nachrichtendienst SBU gibt an, allein im Jahr 2021 mehr als zweitausend Cyberangriffe gegen Regierungssysteme und kritische Infrastrukturen in der Ukraine abgewehrt zu haben, wobei der SBU einen Teil dieser Angriffe mit russischen Nachrichtendiensten in Verbindung bringt.[5] Anfang 2022 gab es dann gleich mehrere aufsehenerregende Cybervorfälle in der Ukraine. So verkündete Microsoft am 15. Januar 2022, eine auf den Namen «WhisperGate» getaufte Malware entdeckt zu haben, die seit dem

---

1 Für Beispiele von Beeinflussungsaktivitäten im Rahmen des Ukraine-Kriegs siehe Kap. 4 des Microsoft-Berichts vom 22. Juni 2022 zum Krieg in der Ukraine (microsoft.com); s. a. EU vs DISINFORMATION (euvsdisinfo.eu)

2 Siehe Halbjahresbericht 2015/2 (ncsc.admin.ch), Kap. 5.3.1.

3 Siehe Halbjahresberichte 2016/2 (ncsc.admin.ch), Kap. 5.3.1 und 2017/1 (ncsc.admin.ch), Kap. 5.3.1.

4 Siehe Halbjahresbericht 2017/1 (ncsc.admin.ch), Kap. 3.

5 SSU neutralizes over 2,000 cyber attacks on government resources in 2021 (ssu.gov.ua)

13. Januar 2022 in der Ukraine die Systeme von Regierungseinrichtungen, IT-Unternehmen und gemeinnützigen Organisationen befalle.[6] «WhisperGate» gab sich den Anschein einer Ransomware, das Fehlen eines Datenwiederherstellungsmechanismus lässt jedoch darauf schliessen, dass es sich in Tat und Wahrheit um einen Wiper handelt – eine Malware, die die Daten auf den befallenen Zielsystemen überschreibt und damit unwiderruflich löscht. Nach einer Analyse der Malware sprach die ukrainische Regierung von einer unter falscher Flagge durchgeführten russischen Operation mit dem Ziel, ukrainischen Cyberkriminellen die Verantwortung für «WhisperGate» zuzuschieben.[7] Gleichzeitig mit dem Auftreten von «WhisperGate» wurden unzählige ukrainische Regierungswebseiten mittels Defacement-Angriffen verunstaltet.[8] Mitte Februar fanden dann zahlreiche DDoS-Angriffe statt, die die Verfügbarkeit etlicher Internetseiten und Online-Dienste in der Ukraine beeinträchtigten. Betroffen waren unter anderem Finanzinstitute und staatliche Behörden.[9]

3.2 Prägnante Cybervorfälle im aktuellen Ukraine-Krieg

3.2.1 Störung von Satellitenverbindungen

Am 24. Februar 2022, etwa eine Stunde vor Beginn der russischen Offensive gegen die Ukraine, fielen in Europa verschiedentlich die Verbindungen mit dem Satelliten KA-SAT des US-Unternehmens ViaSat aus. Zahlreiche europäische Firmen, Behörden und private Nutzerinnen und Nutzer verwenden diesen Telekommunikationssatelliten für den Internet-zugang, insbesondere in entlegenen Regionen. So führte der Vorfall zu Störungen in der Ukraine, aber auch über deren Grenzen hinaus. Beispielsweise waren in Deutschland Zugriffe auf Überwachungs- und Fernsteuerungssysteme von Windkraftanlagen nicht mehr möglich. Am 30. März 2022 veröffentlichte ViaSat eine Analyse des Vorfalls. Aus dieser geht hervor, dass es sich um einen gezielten Angriff handelte, der lediglich auf den für die Abdeckung der Ukraine zuständigen Teil des Satellitennetzes ausgerichtet war,[10] jedoch seine Auswirkungen nicht darauf beschränkt blieben. Die Angreifer nutzten die fehlerhafte Konfiguration einer VPN-Verbindung aus, um sich Zugang zur Administratorenschnittstelle zu verschaffen. So konnten sie für zahlreiche Kundengeräte ein manipuliertes Firmware-Update veranlassen. Dies führte dazu, dass die betroffenen Systeme keine Verbindung mehr aufbauen konnten und vor Ort manuell wiederhergestellt werden mussten. Anfang Mai 2022 verurteilten die Europäische Union und ihre Mitgliedsstaaten sowie die USA, das Vereinigte Königreich und weitere Staaten den Angriff, für den sie offiziell Russland verantwortlich machten.[11]

---

6 Destructive malware targeting Ukrainian organizations (microsoft.com)

7 Information on the possible provocation (cip.gov.ua)

8 Ukraine hit by ‘massive’ cyber-attack on government websites (theguardian.com)

9 Ukraine Ministry of Defense confirms DDoS attack; state banks lose connectivity (zdnet.com); DDoS attacks hit Ukrainian government websites (therecord.media)

10 KA-SAT Network cyber attack overview (viasat.com)

11 Russische Cyberoperationen gegen die Ukraine: Erklärung […] der Europäischen Union (europa.eu); Attribution of Russia’s Malicious Cyber Activity Against Ukraine (state.gov); Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion (www.gov.uk)

Kommentar:

Cyberangriffe auf Infrastrukturen, die militärisch und zivil sowie international genutzt werden, werfen einige Fragen bezüglich Verhaltensnormen von Staaten im Cyberspace auf. Diese dürften in den nächsten Jahren breit diskutiert werden, u. a. in den Bereichen Kollateralschäden und Verhältnismässigkeit sowie Rücksichtspflichten von staatlichen Angreifern.

3.2.2 Versuchte Sabotage der Stromversorgung: «Industroyer2»

Am 12. April 2022 gab das ukrainische Computer Emergency Response Team CERT-UA gemeinsam mit Microsoft und dem slowakischen IT-Sicherheitsunternehmen ESET bekannt, mit «Industroyer2» die erste auf industrielle Kontrollsysteme ausgerichtete Malware dieses Angriffskriegs entdeckt und ausgeschaltet zu haben.[12] Es soll sich dabei um eine neue Version der 2016 eingesetzten Malware «Industroyer» gehandelt haben, die damals Stromausfälle in Kiew herbeigeführt hatte (siehe Kap. 3.1), wobei die neue Version ebenfalls vom Akteur Sandworm entwickelt worden sein soll.[13] Ziel des Angriffs war ein Stromversorger in der Ukraine, dessen IT-Netzwerk bereits im Februar 2022 von den Angreifern infiltriert worden war. Die Angreifer schafften es, über das IT-Netzwerk ins Kontroll- und Steuernetzwerk der operativen Technologie einzudringen und dort die Malware «Industroyer2» zu platzieren. Seine zerstörerische Wirkung hätte der Angriff dann am 8. April 2022 entfalten sollen, indem elektrische Unterwerke vom Netz genommen und Teile der Unternehmensinfrastruktur lahmgelegt worden wären. Neben «Industroyer2» soll gleichzeitig der Wiper «CaddyWiper» aktiv gewesen sein. Dies wahrscheinlich mit dem Ziel, die Wiederherstellung der Systeme zu erschweren und die Spuren des Angriffs zu beseitigen. Einige Tage nach der Mitteilung des CERT-UA gab die ukrainische Regierung an, dass seit Beginn des Kriegs mehr als 50 ähnliche Angriffe vereitelt worden seien. Im Widerspruch zu dieser Meldung hiess es in einem durchgesickerten vertraulichen Bericht, dass bei einem kurz zuvor erfolgten Cyberangriff neun Unterwerke lahmgelegt worden seien.[14]

Kommentar:

«Industroyer2» ist die erste seit Beginn der Invasion in der Ukraine entdeckte Malware, mit der auf Grund ihrer Funktionalität nicht nur IT-Systeme gestört, sondern durch direkte Interaktion mit industriellen Kontrollsystemen beabsichtigt wurde, physische Prozesse zu beeinträchtigen.

---

12 Heavy cyberattack on Ukraine's energy sector prevented (cip.gov.ua);
Industroyer2: Industroyer reloaded (welivesecurity.com)

13 Ukraine Power Grid Cyberattacks (securityboulevard.com);
INDUSTROYER.V2: Old Malware Learns New Tricks (mandiant.com)

14 Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine (wired.com);
Russian hackers tried to bring down Ukraine's power grid to help the invasion (technologyreview.com)

3.2.3 Wiper

Seit Beginn des Kriegs in der Ukraine sind zahlreiche verschiedene Wiper aufgetaucht.[15] Ziel derartiger Malware ist es, Daten zu zerstören, respektive sie durch Verschlüsselung oder Überschreiben unlesbar zu machen und damit unwiderruflich zu löschen. Es wurden Organisationen unterschiedlicher Bereiche wie der öffentlichen Verwaltung, dem Energie- und dem Finanzsektor ins Visier genommen. Informationen aus offiziellen Quellen zum konkreten Ausmass und Erfolg der Angriffe sind jedoch keine verfügbar. Analysen zufolge ist die Malware jeweils so programmiert, dass eine unkontrollierte Verbreitung, wie dies 2017 bei «NotPetya» der Fall war, vermieden wird. Dennoch wurde am 23. Februar 2022 der «HermeticWiper» in Litauen und Lettland beobachtet – bei Unternehmen, die auch Dienstleistungen für die ukrainische Regierung erbringen.[16]

Kommentar:

Die russischen staatlichen Akteure scheinen sehr darauf bedacht zu sein, die Auswirkungen ihrer Cybersabotageangriffe auf die Ukraine zu beschränken. Es soll wohl keinem Land und erst recht nicht der NATO ein Vorwand geliefert werden, um aktiv in den Konflikt einzugreifen.

3.3 Nichtstaatliche Angreifer auf beiden Seiten

Nach der russischen Offensive vom 24. Februar 2022 haben zahlreiche nichtstaatliche Akteure (Hacktivisten-Organisationen und kriminelle Gruppierungen) angekündigt, sich im Cyberspace am Krieg zu beteiligen. Sie nehmen Angriffe für sich in Anspruch oder drohen denjenigen, die «ihre» Kriegspartei angreifen, mit Repressalien. Insgesamt wurden mehr als 80 solcher nichtstaatlicher Gruppierungen festgestellt.

Eine der bedeutendsten Gruppierungen auf russischer Seite ist Killnet. Als Reaktion auf die der Ukraine zuteil gewordene Unterstützung sowie auf die Sanktionen gegen Russland hat die Gruppierung zahlreiche DDoS-Angriffe durchgeführt. Der daraus resultierende Schaden richtet sich stark danach, wie abhängig die jeweiligen Opfer von ihrer Internetpräsenz und wie gut sie auf solche Angriffe vorbereitet sind. Zumeist können DDoS-Angriffe relativ schnell abgewehrt, respektive unschädlich gemacht werden. Betroffen waren insbesondere Internetseiten von Flughäfen, staatlichen Einrichtungen sowie Finanzinstituten zahlreicher europäischer Länder. Auf ukrainischer Seite hat das Kollektiv Anonymous zahlreiche Angriffe auf russische Organisationen, aber auch auf in Russland tätige westliche Unternehmen für sich beansprucht. So rief Anonymous am 20. März 2022 in Russland tätige westliche Unternehmen dazu auf, sich innert 48 Stunden aus dem russischen Markt zurückzuziehen. Andernfalls bestehe das Risiko, zum Ziel dieser Gruppierung zu werden. Seither hat Anonymous zahlreiche «Hack-and-Leak»-Angriffe durchgeführt: Vertrauliche Unternehmens- oder Regierungsdaten, hauptsächlich aus Russland, wurden gestohlen und veröffentlicht.

---

15 An Overview of the Increasing Wiper Malware Threat (fortinet.com)

16 Russia unleashed data-wiper malware on Ukraine (theguardian.com)

Am 26. Februar 2022 verkündete die Ukraine die Schaffung einer «IT Army of Ukraine» und rief Freiwillige aus der ganzen Welt dazu auf, dieser beizutreten und zugunsten der Ukraine Angriffe im Cyberspace durchzuführen. Einer der wichtigsten Pfeiler dieser Gruppierung ist ihr Telegram-Kanal, über den sie die Ziele ihrer DDoS-Angriffe kommuniziert.

Trotz der hohen Frequenz von Angriffen seitens nichtstaatlicher Gruppierungen erscheint die Wirkung dieser Angriffe auf den Kriegsverlauf bisher marginal.

Kommentar:

Im Rahmen politisch motivierter Demonstrationen auf der Strasse werden immer wieder strafbare Handlungen wie z. B. Sachbeschädigungen begangen. Vergleichbare virtuelle Aktionen (Defacement, DDoS) werden auch im Internet durchgeführt. Wenn sich Hacktivisten jedoch im Rahmen eines bewaffneten zwischenstaatlichen Konflikts engagieren, könnten sie unter Umständen als Kriegsteilnehmende (Kombattante) qualifiziert und dadurch legitime Ziele für Gegenschläge werden. Fragen stellen sich hierzu auch bezüglich der Verantwortlichkeiten der Staaten, von deren Territorium aus solche Angriffe ausgeführt werden.

3.4 Weitere Aspekte des Konflikts im Cyberspace

3.4.1 Unterstützung durch Staaten und Unternehmen

Zu Beginn des Jahres 2022 wurden verschiedene Unterstützungsmassnahmen für die Ukraine im Bereich der Cybersicherheit angekündigt. Am 14. Januar 2022 stellte der NATO-Generalsekretär die Unterzeichnung einer Vereinbarung mit der Ukraine zur stärkeren Unterstützung bei der Cyberabwehr in Aussicht. In der Erklärung hiess es zudem, dass die NATO seit Jahren gemeinsam mit der Ukraine daran arbeite, die Cyberabwehr des Landes zu verbessern, und dabei auch Vor-Ort-Unterstützung leiste. Die Europäische Union hat ihrerseits am 22. Februar 2022 die Bildung einer etwa zehnköpfigen Expertengruppe mit Vertreterinnen und Vertretern aus verschiedenen europäischen Ländern angekündigt, um der Ukraine sowohl vor Ort als auch aus der Ferne bei der Bewältigung der zunehmenden Cyberbedrohungen zu helfen.

Konkretere Daten dazu, wie andere Staaten die Ukraine unterstützen, wurden am 10. Mai 2022 bekannt. In einer Erklärung verurteilten die Europäische Union und ihre Mitgliedsstaaten sowie die USA, das Vereinigte Königreich und weitere Staaten die Angriffe auf ViaSat (siehe Kapitel 3.2.1) und kündigten an, die Ukraine weiterhin zu unterstützen, um deren Cyberresilienz zu stärken. Gleichzeitig machten die USA genauere Angaben dazu, wie das Land die Ukraine dabei unterstützt, den Zugang zum Internet sicherzustellen und die Cybersicherheit zu gewährleisten.[17]

Am 1. Juni 2022 verkündete der Kommandant des US Cyber Command, dass die Vereinigten Staaten zur Unterstützung der Ukraine eine Reihe von offensiven und defensiven Operationen sowie Informationsmassnahmen im Cyberspace umgesetzt hätten.[18] Da der Grossteil dieser

[17] U.S. Support for Connectivity and Cybersecurity in Ukraine (state.gov)

[18] US military hackers conducting offensive operations in support of Ukraine (sky.com)

Massnahmen nicht öffentlich gemacht worden ist, ist es schwierig, deren Tragweite zu beurteilen. Die im April 2022 veröffentlichte Analyse einer Malware, die für Angriffe auf industrielle Kontrollsysteme konzipiert worden war (siehe Kap. 5.4.1), aber bis dahin noch nicht zum Einsatz gekommen war, dürfte im Zusammenhang mit den erwähnten Massnahmen des US Cyber Command stehen. Die Malware hätte für künftige Angriffe gegen die Ukraine, aber auch gegen andere Staaten eingesetzt werden können. Eine weitere Operation, die der Ukraine potenziell geholfen hat und die öffentlich gemacht worden ist, ist die teilweise Stilllegung der Infrastruktur des vom Akteur Sandworm genutzten «CyclopsBlink»-BotNetzes (siehe Kap. 5.2.4).

Zahlreiche IT-Sicherheitsunternehmen messen dem Krieg in der Ukraine eine besondere Bedeutung bei und widmen diesem Thema Analysen und Berichte. So haben beispielsweise ESET und Microsoft gemeinsam mit dem ukrainischen CERT die Entdeckung von «Industroyer2» publik gemacht. Am 22. Juni 2022 veröffentlichte Microsoft einen Bericht zu den Beobachtungen des Unternehmens im Zusammenhang mit Cyberbedrohungen im Krieg in der Ukraine.[19] Im Bericht heisst es unter anderem, Microsoft und weitere Technologieunternehmen hätten die Ukraine dabei unterstützt, innerhalb von zehn Wochen den Grossteil der Daten und digitalen Aktivitäten der ukrainischen Regierung in Clouds ausserhalb der ukrainischen Grenzen zu verlagern. Als zu Beginn der russischen Offensive bei Raketenangriffen ukrainische Rechenzentren zerstört worden waren, konnte die Ukraine somit dennoch weiter digital funktionieren. Ferner wird die enge Zusammenarbeit des IT-Unternehmens mit der ukrainischen Regierung erwähnt. Microsoft gibt in seinem Bericht an, die Ukraine mit kostenlosen Leistungen im Gesamtwert von geschätzten 239 Millionen US-Dollar unterstützt zu haben. Hilfe von Privatunternehmen ist für die Ukraine zweifellos grundlegend, da diese auch unter normalen Umständen Systemschutz gewährleisten und typischerweise Einblick in wesentlich mehr Systeme und Vorgänge haben als irgendwelche Behörden.

3.4.2 Verwendung von Cyberinstrumenten im Rahmen bewaffneter Konflikte

Die bislang öffentlich gewordenen Cyberangriffe in der Ukraine seit dem 24. Februar 2022 zeichnen weder ein vollständiges Bild, noch lassen sie eine abschliessende Beurteilung über die mögliche Nutzung des Cyberspace im Rahmen bewaffneter Konflikte zu.

Da es sich um einen andauernden Krieg handelt, werden zahlreiche Vorfälle, bzw. deren Tragweite, nicht öffentlich gemacht. Die Protagonisten beanspruchen erfolgreiche oder abgewehrte Angriffe für sich, ohne dass sich dies von unabhängiger Seite verifizieren lässt. Entsprechende Mitteilungen dienen oft dazu, die öffentliche Meinung und die Stimmung in der Bevölkerung positiv oder negativ zu beeinflussen. So wurde beispielsweise kein Fall eines Cyberangriffs gegen militärische Systeme öffentlich, wie er zum Beispiel 2007 in Syrien vermutet worden ist, als die israelischen Streitkräfte ihre Cyberkompetenz genutzt haben sollen, um Luftabwehrsysteme ausser Gefecht zu setzen, damit sie einen Luftangriff gegen Ziele in Syrien fliegen konnten.[20]

---

19 Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)

20 Operation Orchard/Outside the Box (2007) - International cyber law: interactive toolkit (ccdcoe.org); Cyberattacken auf syrische Luftabwehr (cyber-peace.org)

Nach der Annexion der Krim 2014 schwelte der Konflikt zwischen der Ukraine und Russland respektive den Separatistengebieten im Osten der Ukraine, mit Phasen schwächerer und dann wieder stärkerer Aktivität. In dieser Zeit wurden auch Cyberoperationen durchgeführt (siehe oben Kap. 3.1), die der vermeintliche Urheber mehr oder weniger glaubhaft abstreiten kann. Seit Beginn der russischen Offensive könnte aber auch die Nutzung konventioneller militärischer Mittel den Einsatz von Cyberinstrumenten in den Hintergrund gedrängt haben. Tatsächlich lassen sich viele militärische Ziele mit konventionellen militärischen Mitteln schneller, präziser, einfacher und nachhaltiger erreichen als mit Cyberangriffen.

Es gibt verschiedene Hypothesen dafür, dass keine Berichte über erfolgreiche zerstörerische russische Cyberangriffe (d. h. Angriffe mit physischer Zerstörung als Auswirkung) gegen die Ukraine vorliegen:

1. Russland führt erfolgreich zerstörerische Cyberangriffe gegen die Ukraine durch, allerdings werden diese nicht publik gemacht, namentlich weil es sich um einen andauernden Krieg handelt;
2. Russland führt zerstörerische Cyberangriffe gegen die Ukraine durch, allerdings verteidigt sich die Ukraine erfolgreich, nicht zuletzt dank der Unterstützung durch andere Staaten und private Partner;
3. Russland führt keine zerstörerischen Cyberangriffe gegen die Ukraine durch, insbesondere weil die Nutzung konventioneller militärischer Mittel besser geeignet ist, bestimmte Ziele zu erreichen.

Letztlich ist das scheinbare Ausbleiben solcher Angriffe wahrscheinlich auf eine Kombination der verschiedenen Hypothesen zurückzuführen und es finden vermutlich mehr Ereignisse im Cyberspace statt, als öffentlich bekannt wird.

4 Meldungen aus der Bevölkerung

4.1 Eingegangene Meldungen zu Cybervorfällen – Überblick

Im ersten Halbjahr 2022 hat das NCSC insgesamt 17’186 Meldungen registriert. Im Vergleich zur Vorhalbjahresperiode mit 10’234 Meldungen entspricht dies einer Zunahme von rund 70 Prozent. Hauptursache dieser beachtlichen Steigerung sind vor allem Meldungen zu Fake-Extortion-E-Mails, die mittlerweile rund einen Drittel der Gesamtmeldungen und die Hälfte der Betrugsmeldungen ausmachen. Meldungen in der Hauptkategorie Betrug sind mit 10'447 Meldungen dann auch die mit Abstand häufigsten. Neben den bereits erwähnten Meldungen zu Fake Extortion sind weitere relevante Betrugsarten Vorschussbetrug (1'834), Fake Sextortion (615) und Kleinanzeigenbetrug (419). Meldungen zu Phishing und Schadsoftware bewegen sich im Vergleich zur Vorhalbjahresperiode auf dem gleichen Niveau.

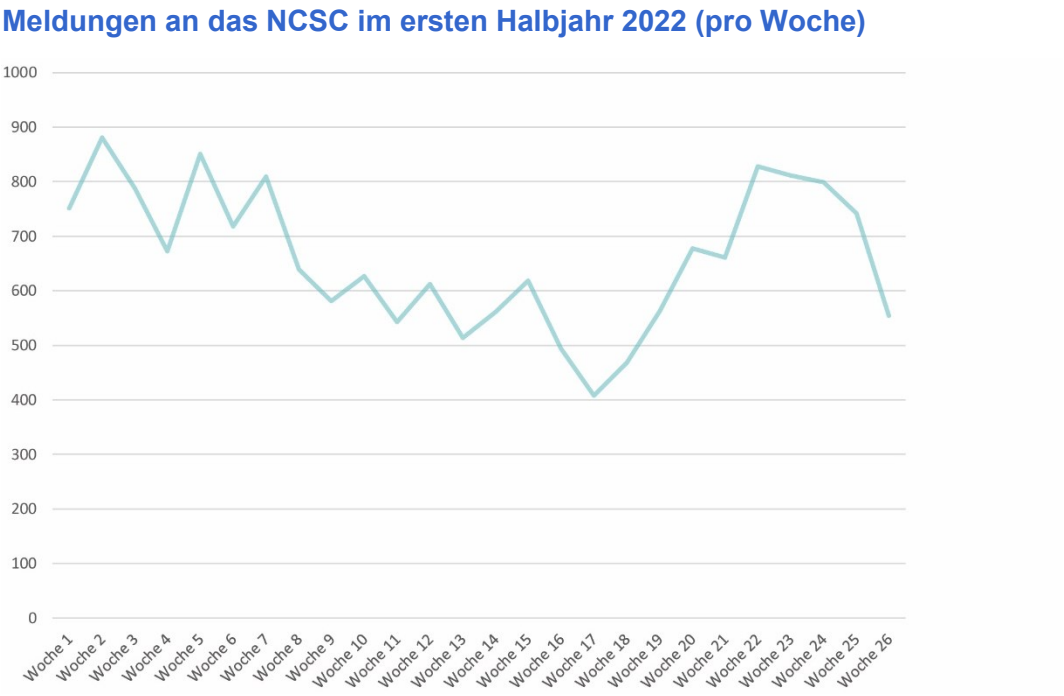


Abb. 1: Anzahl Meldungen pro Woche beim NCSC vom Januar bis Juni 2022, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

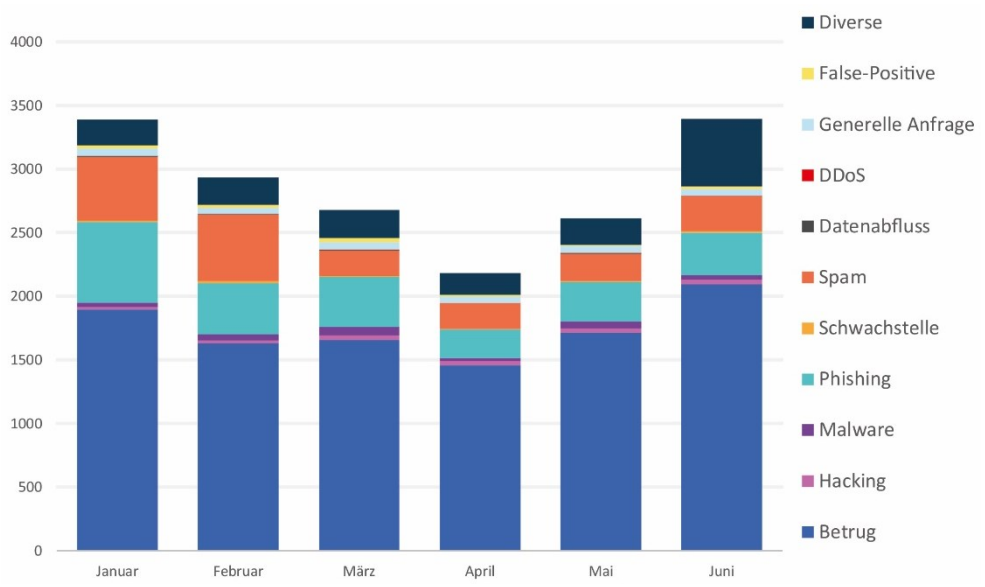
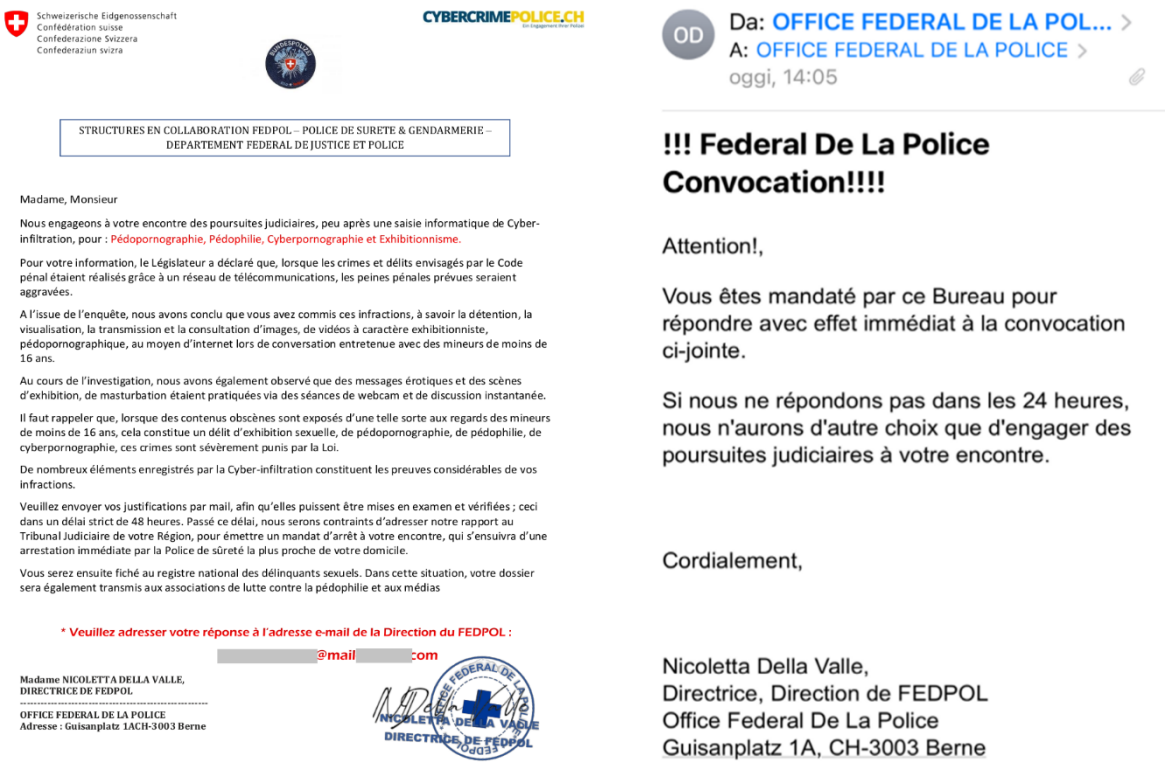


Abb. 2: Meldungen an das NCSC im ersten Halbjahr 2022 nach Kategorien, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

4.2 Am häufigsten gemeldet: Betrug

4.2.1 Anhaltender Trend zu mehr Fake Extortion

Der Trend der Zunahme von Droh-E-Mails im Namen der Polizei, der sich bereits Ende des letzten Jahres abzeichnet hatte, setzte sich auch im ersten Halbjahr 2022 fort. Solche sogenannten Fake-Extortion-E-Mails machen mittlerweile rund einen Drittel (5'872) aller eingegangenen Meldungen und rund die Hälfte der Betrugsmeldungen aus. Fake Extortion ist eine Betrugsart, bei der vorgegeben wird, dass die angeschriebene Person eines massiven Fehlverhaltens (typischerweise in Zusammenhang mit Kinderpornographie) überführt worden sei und die Anklage gegen sie nur durch eine Geldzahlung fallengelassen werden könne. Die Masche wurde in Frankreich bereits seit mehreren Jahren beobachtet und ist dann auf die Schweiz übergeschwappt. Zu Beginn wurden die betrügerischen E-Mails nur auf Französisch beobachtet, dann aber auch auf Deutsch und ab Mitte Mai 2022 wurden dem NCSC erste derartige Schreiben auch in italienischer Sprache gemeldet. Die häufigste Variante gibt vor, vom Bundesamt für Polizei oder genauer von dessen Direktorin, Nicoletta Della Valle, zu stammen.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

CYBERCRIMEPOLICE.CH

STRUCTURES EN COLLABORATION FEDPOL – POLICE DE SURETE & GENDARMERIE –
DEPARTEMENT FEDERAL DE JUSTICE ET POLICE

Madame, Monsieur

Nous engageons à votre encontre des poursuites judiciaires, peu après une saisie informatique de Cyber-infiltration, pour : Pédopornographie, Pédophilie, Cyberpornographie et Exhibitionnisme.

Pour votre information, le Législateur a déclaré que, lorsque les crimes et délits envisagés par le Code pénal étaient réalisés grâce à un réseau de télécommunications, les peines pénales prévues seraient aggravées.

A l'issue de l'enquête, nous avons conclu que vous avez commis ces infractions, à savoir la détention, la visualisation, la transmission et la consultation d'images, de vidéos à caractère exhibitionniste, pédopornographique, au moyen d'internet lors de conversation entretenue avec des mineurs de moins de 16 ans.

Au cours de l'investigation, nous avons également observé que des messages érotiques et des scènes d'exhibition, de masturbation étaient pratiquées via des séances de webcam et de discussion instantanée.

Il faut rappeler que, lorsque des contenus obscènes sont exposés d'une telle sorte aux regards des mineurs de moins de 16 ans, cela constitue un délit d'exhibition sexuelle, de pédopornographie, de pédophilie, de cyberpornographie, ces crimes sont sévèrement punis par la Loi.

De nombreux éléments enregistrés par la Cyber-infiltration constituent les preuves considérables de vos infractions.

Veuillez envoyer vos justifications par mail, afin qu'elles puissent être mises en examen et vérifiées ; ceci dans un délai strict de 48 heures. Passé ce délai, nous serons contraints d'adresser notre rapport au Tribunal Judiciaire de votre Région, pour émettre un mandat d'arrêt à votre encontre, qui s'ensuivra d'une arrestation immédiate par la Police de sûreté la plus proche de votre domicile.

Vous serez ensuite fiché au registre national des délinquants sexuels. Dans cette situation, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux médias

* Veuillez adresser votre réponse à l'adresse e-mail de la Direction du FEDPOL :

[redacted]@mail[redacted].com

Madame NICOLETTA DELLA VALLE,
DIRECTRICE DE FEDPOL

OFFICE FEDERAL DE LA POLICE
Adresse : Guisanplatz 1ACH-3003 Berne

OD Da: OFFICE FEDERAL DE LA POL...
A: OFFICE FEDERAL DE LA POLICE
oggi, 14:05

!!! Federal De La Police Convocation!!!!

Attention!,

Vous êtes mandaté par ce Bureau pour répondre avec effet immédiat à la convocation ci-jointe.

Si nous ne répondons pas dans les 24 heures, nous n'aurons d'autre choix que d'engager des poursuites judiciaires à votre encontre.

Cordialement,

Nicoletta Della Valle,
Directrice, Direction de FEDPOL
Office Federal De La Police
Guisanplatz 1A, CH-3003 Berne

Abb. 3: Droh-E-Mails im Namen der fedpol-Direktorin Nicoletta Della Valle.

Die in den Droh-E-Mails verwendeten Absender der angeblichen Behörden wechseln aber häufig und werden auch völlig zusammenhangslos aneinandergereiht. So wurden auch andere Varianten im Namen von diversen Kantonspolizeien oder dem Polizeiportal Cybercrimepolice versendet. Auch der Name des NCSC wurde missbraucht, um den betrügerischen E-Mails einen offiziellen Anstrich zu geben. Zur Kommunikation mit den Opfern verwenden die Täter

häufig gehackte E-Mail-Konten von Studenten verschiedener Universitäten in Europa und Brasilien. Das NCSC meldete in diesem Zusammenhang den entsprechenden Providern bereits hunderte gefälschte oder gehackte E-Mail-Accounts, damit diese Massnahmen gegen den Missbrauch ergreifen konnten.

4.2.2 Hohe Schäden bei Investment-Betrug und Rechnungsmanipulationsbetrug

Investment-Betrug gehört weiterhin zu den Delikten mit den höchsten Schadenssummen. In der ersten Jahreshälfte 2022 wurden dem NCSC Fälle mit einer Schadenssumme von insgesamt mehr als drei Millionen Schweizer Franken gemeldet. Verluste in sechsstelliger Höhe pro Fall sind dabei keine Seltenheit. In Zeiten von steigender Teuerung und tiefen Zinsen scheinen solche Investitionsangebote Hochkonjunktur zu haben. Geblendet von den versprochenen (verdächtig) hohen Renditen, schlagen die Opfer dabei sämtliche Anzeichen und Hinweise, welche auf einen Betrug hindeuten, in den Wind. Zum Beispiel sind in den meisten Fällen die dubiosen Investment-Websites nur ein paar Monate alt.

Das höchste Schadenspotential bei Unternehmen verzeichnete das NCSC neben Ransomware beim Phänomen des Rechnungsmanipulationsbetrugs (Business E-Mail-Compromise). Im Berichtszeitraum erhielt das NCSC diesbezüglich 47 Meldungen. Bei dieser Betrugsform wird jeweils auf eine bestehende E-Mail-Kommunikation zwischen den Vertragsparteien Bezug genommen, die eine Zahlungsanweisung oder eine Rechnung enthält. Die Betrüger ändern jeweils die IBAN-Nummer, auf die der Betrag einbezahlt werden soll. Um an die E-Mail-Kommunikation zu kommen, müssen Angreifer entweder Zugriff auf das E-Mail-Konto des Absenders oder des Empfängers haben. Im Visier sind dabei vor allem Zulieferfirmen. Erstens sind die Rechnungsbeträge häufig hoch und zweitens werden in der Regel diverse Rechnungen zur gleichen Zeit versendet, was die Erfolgschancen der Betrüger erhöht. In dieser Kategorie wurden dem NCSC Schadenssummen von insgesamt 2.3 Millionen Schweizer Franken gemeldet.

4.2.3 Spoofing im Aufwind

Meldungen zu gefälschten (gespooften) Telefonnummern sind geradezu explodiert. Verglichen mit der Vorhalbjahresperiode stieg der Meldeeingang von 17 auf 319! Hintergrund sind Anrufe von dubiosen Callcentern mit gefälschten Telefonnummern, die eigentlich Privatpersonen zugeordnet sind. Bei Betrugsanrufen oder Anrufen von dubiosen Callcentern ist es eine gängige Praxis, die angezeigte Rufnummer zu fälschen und eine unverfängliche Schweizer Nummer anzuzeigen, um die Angerufenen dadurch zu verleiten, den Anruf entgegenzunehmen. Wenn immer die gleichen Nummern für das Spoofing verwendet werden, hat dies zur Folge, dass die eigentlichen Besitzer dieser Rufnummern mit Rückrufen geradezu überschwemmt werden. Einige Melder erhielten so bis zu 50 Anrufe pro Tag. Normalerweise wechseln die Callcenter die gefälschten Nummern regelmässig, so dass die Rückrufe wieder aufhören. In einigen Fällen wurden nun jedoch die gleichen Telefonnummern über Wochen, respektive Monate, verwendet. Für den eigentlichen Nummernbesitzer ist dies mehr als ärgerlich, zumal sich dagegen kaum etwas unternehmen lässt.[21]

[21] Vgl. hierzu BBl 2017 6559 - Botschaft zur Revision des Fernmeldegesetzes (admin.ch), 6581 und 6596.

4.3 Meldungen zu Phishing

Meldungen zu Phishing bewegen sich in etwa auf dem gleichen Niveau wie im vorangehenden Halbjahr. Über das Meldeformular wurden zwar mit 2'308 Fällen 100 Meldungen weniger gezählt. Direkt über das spezialisierte Portal antiphishing.ch wurden aber insgesamt 4’535 Seiten verarbeitet. Dominant bleiben hierbei vor allem die E-Mails mit den falschen Paketankündigungen im Namen diverser Paketdienstleister. Alleine 464 Meldungen gehen auf das Konto dieser Variante. Ebenfalls ein Dauerbrenner in der Kategorie Phishing sind die angeblich doppelt bezahlten Rechnungen von Internetprovidern wie Swisscom oder Sunrise. Dabei wird in Aussicht gestellt, das Geld werde auf die Kreditkarte überwiesen, sofern man die Kreditkartennummer angebe.

Mit insgesamt 145 Meldungen im ersten Halbjahr 2022 haben zudem Phishing-Versuche im Zusammenhang mit Kleinanzeigen zugenommen. Bei dieser Phishing-Variante wird durch die Täterschaft Interesse an einem Produkt vorgetäuscht. Hat man sich auf einen Verkaufspreis geeinigt, gibt der Käufer an, er werde den Transport organisieren und das Geld überweisen. Die entstehenden Transportkosten würden zusammen mit dem Kaufpreis ebenfalls überwiesen. Der Verkäufer soll dann seinerseits die Transportfirma entschädigen. Auf den Webseiten eines angeblichen Paketdienstleisters, der sich dann meldet, soll mit der Kreditkarte bezahlt und dafür die Kreditkartendaten angegeben werden. Diese Webseiten sind zum Teil stark personalisiert und enthalten neben Adresse und Namen des Verkäufers oft auch ein Bild des Verkaufsobjektes, das die Phisher zuvor von der Kleinanzeigenplattform kopiert haben. Seitens Angreifer wird also ein relativ grosser Aufwand betrieben, der sich jedoch zu lohnen scheint.

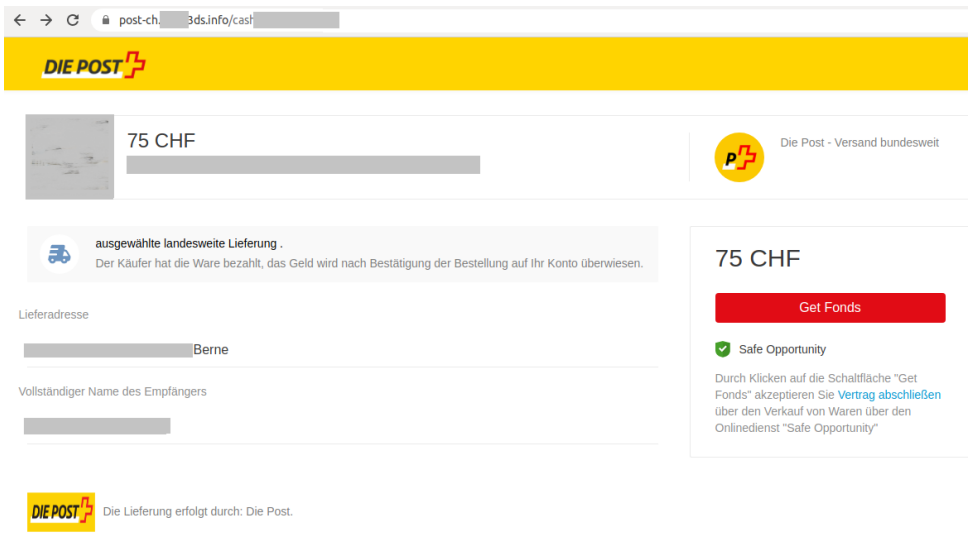


Abb. 4: Personalisierte Webseite mit Adresse des Verkäufers und einem Bild des Produktes.

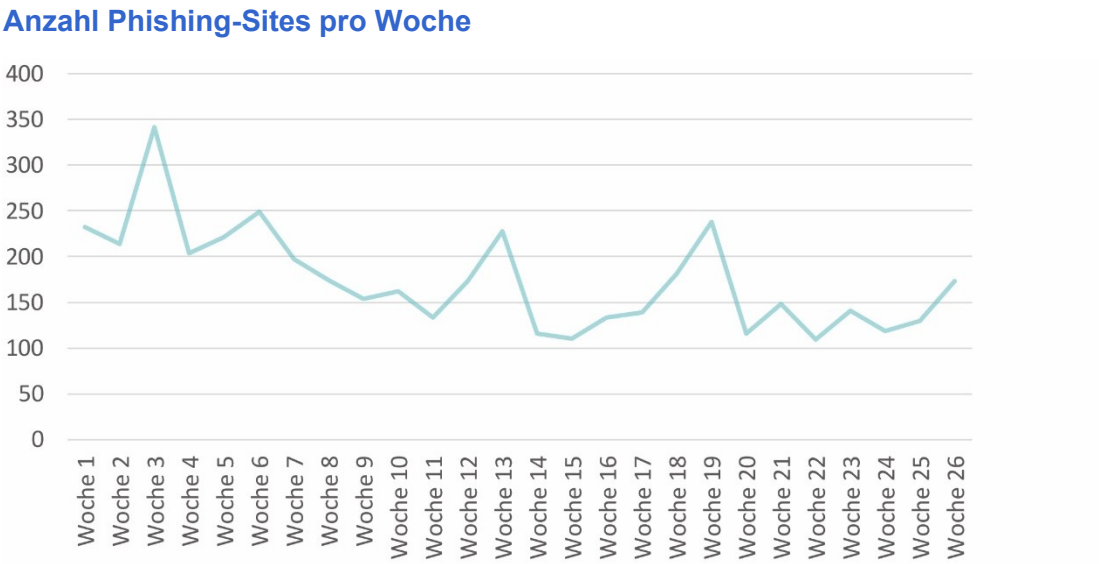


Abb. 5: Anzahl durch das NCSC überprüfte und bestätigte Phishing-URLs pro Woche im ersten Halbjahr 2022. Aktuelle Daten finden Sie unter: https://www.govcert.admin.ch/statistics/phishing/

4.4 Meldungen zu Schadsoftware und Hacking

Im ersten Halbjahr 2022 wurden insgesamt 255 Meldungen zu Schadsoftware registriert. Im Vergleich zur Vorhalbjahresperiode ist dies ein Rückgang um 20 Prozent. Die grossen Wellen blieben dabei aus. Aufgefallen sind zwei kleinere Wellen mit «Flubot» im März und im Mai mit insgesamt 56 Meldungen. In diesen Fällen wurden SMS mit Benachrichtigungen zu angeblichen Paketlieferungen in diversen Textvarianten versendet. Der Link unter dem Text führte auf eine Webseite, welche das Opfer aufforderte, eine Software des Paketdienstleisters auf das Android-Smartphone herunterzuladen und zu installieren. Internationale Ermittler konnten das Netzwerk hinter dem Trojaner «Flubot» im Juni 2022 lahmlegen (siehe Kap. 5.2.3).

Eine weitere Welle mit 30 Meldungen betraf die Schadsoftware «QakBot» (auch bekannt als «QuakBot» oder «Qbot»). Diese Schadsoftware wird über E-Mails verbreitet. Die Cyberkriminellen verwenden dabei häufig bestehende E-Mail-Konversationen der Unternehmen (z. B. mit Lieferanten oder Kundinnen und Kunden), die durch frühere Angriffe in ihre Hände geraten sind, um die Empfängerinnen und Empfänger zum Öffnen des bösartigen Anhangs zu bewegen. Auf diese Weise wird die Schadsoftware installiert, die als Einfallstor dient, um in Unternehmensnetzwerke einzudringen (vgl. Kap.5.1.2) und danach Verschlüsselungstrojaner (sogenannte Ransomware) zu installieren.

Meldungen zu Ransomware gingen im Vergleich zur Vorhalbjahresperiode von 91 auf 83 Meldungen leicht zurück. Dabei wurden vor allem die Ransomware-Familien «QLocker» und «Deadbolt» gegen NAS-Geräte sowie «LockBit 2.0», «Sodinokibi» und «Conti» gemeldet. Zugenommen haben hingegen Hacking-Vorfälle (von 139 auf 184 Meldungen). Hier stehen vor allem Konten von Sozialen Medien im Fokus. Allein 91 Meldungen betrafen soziale Netzwerke wie Facebook, Instagram, Twitter.

5 Ereignisse / Lage

5.1 Initialer Zugang

Die Erlangung von Fernzugriffen auf Computersysteme oder Zugang zu Nutzerkonten ist bei den meisten Arten von Cyberangriffen der erste Schritt. Denn nur damit können die Angreifer das eigentliche Ziel erreichen, sei dies das System oder Konto für Betrügereien zu missbrauchen, Daten unbefugt zu beschaffen oder Verschlüsselungs-Schadsoftware (Ransomware) einzuschleusen. Ein solcher initialer Zugang kann auf verschiedene Weise erlangt werden.

5.1.1 Nutzername / Passwort

Am einfachsten gelingt die Erlangung eines Zugriffs, wenn ein Zugang zu einem Konto oder System nur mit Nutzername (häufig die E-Mail-Adresse) und Passwort gesichert ist. Dann kann durch einfaches Phishing an die E-Mail-Adresse das gesuchte Passwort ergattert und damit auf das Konto oder System zugegriffen werden. Angreifer haben dadurch vollen Zugriff und können damit alles machen, wie die rechtmässigen Nutzenden – unabhängig davon, ob diese gerade online sind oder nicht.

Bei Zugängen, die nur mit Nutzername und Passwort gesichert sind, besteht zudem die Gefahr, dass bei Mehrfachverwendung des gleichen Passwortes mehrere Konten angegriffen werden können. Cyberkriminelle setzen dazu oft «Credential Stuffing» ein. Das heisst, die ergatterten Zugangsdaten werden bei allen gängigen Diensten (E-Mail-Anbieterin, Twitter, Facebook, Instagram, Amazon, usw.) ausprobiert. Anschliessend werden die so verifizierten Zugangsdaten weiterverkauft.

Schlussfolgerung / Empfehlung:

Schutz vor dieser Bedrohung bietet zum Beispiel eine Zwei- oder Mehrfaktor-Authentisierung.

Der Eigenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat an einem Bericht[22] sowie Richtlinien[23] des Global Privacy Assembly zu Credential Stuffing mitgearbeitet.

5.1.2 Schadsoftware (Trojaner)

Eine andere Methode, um einen unerlaubten Zugang zu erlangen, ist die Verwendung einer Schadsoftware, die eine Hintertür zum System einrichtet. Analog der griechischen Legende vom trojanischen Pferd wird die Schadsoftware unbemerkt in ein System geschleust und öffnet dann den Angreifenden einen Weg zur Installation weiterer Schadsoftware. Um die Nutzenden dazu zu bringen, den entscheidenden Klick auf einen Link auszuführen oder eine «trojani-

22 22-06-27-Credential-Stuffing-General-Public-Awareness.pdf (globalprivacyassembly.org)

23 22-06-27-Credential-stuffing-guidelines.pdf (globalprivacyassembly.org)

sierte» Datei zu öffnen, werden diverse Methoden des Social Engineering angewendet. Typische Elemente dieser Manipulationsversuche sind das Wecken von Neugier oder von Befürchtungen, dass man etwas verpasst hat, und das Anführen von Dringlichkeit.

Die meisten Trojaner enthalten heutzutage Funktionalitäten für das Nachladen und Installieren weiterer Schadsoftware (beispielsweise «Emotet»[24], «Qakbot»[25], «Formbook/XLoader»[26]). Es gibt jedoch weiterhin auch Trojaner, die vor allem Bildschirmfotos machen und Tastatureingaben aufzeichnen (sogenannte Keylogger). Auf diese Weise erlangte Nutzernamen und Passwörter (wie auch Kreditkartendaten und weitere Informationen) werden vom Trojaner selbständig in regelmässigen Abständen an seine Betreiber resp. die Angreifer versendet oder im Internet an Orten – sogenannten Dropzones – gespeichert, wo sie von den Kriminellen abgeholt werden können. Ein im Berichtszeitraum sehr aktiver solcher Trojaner ist der «Snake Keylogger».[27]

Schlussfolgerung / Empfehlung:

Der beliebteste Verbreitungsvektor für Trojaner ist nach wie vor E-Mail. Häufig bezieht sich der Text in den E-Mails auf alltägliche Geschäfte wie Offerten, Lieferungen oder Rechnungen. Manchmal werden auch exklusive Informationen zu aktuellen Ereignissen wie der Pandemie, dem Krieg in der Ukraine, Naturkatastrophen oder Sportanlässen als Aufhänger in Aussicht gestellt, um Neugier zu wecken. Häufig wird auch Dringlichkeit vorgetäuscht, um Empfängerinnen und Empfänger zu unbedachten Aktionen zu verleiten.

Klicken Sie in verdächtigen E-Mails nicht auf Links und öffnen Sie keine angehängten Dateien.

5.1.3 Ausnutzen von Schwachstellen

Verwundbarkeiten in Software wie auch Fehlkonfigurationen führen zu Schwachstellen, die entweder direkt als Zugang oder für die Erlangung eines Zugangs genutzt werden können. Gefährdet sind insbesondere direkt aus dem Internet erreichbare Systeme, da diese nicht in jedem Fall von einer weiteren Sicherheitsschicht geschützt werden (können).

Eine Software, deren Verwundbarkeiten seit Anfang 2021 regelmässig für Aufregung sorgen, ist Microsoft Exchange.[28] Seit dem ersten grossen Aufsehen im März 2021 sind verschiedene weitere Schwachstellen in Exchange bekannt geworden. Da sehr viele Unternehmen diese Mail-Server-Software verwenden, haben Angreifer eine riesige Auswahl von potenziellen Opfern, zumal nicht alle Systemverantwortlichen zeitnah verfügbare Updates einspielen. Nicht aktuell gehaltene Produkte für Fernzugriffe und Firewalls sind ebenfalls beliebte Einfallstore für Cyberakteure, um in Netzwerke einzudringen.[29]

---

[24] Emotet (fraunhofer.de); Emotet Botnet C&Cs (abuse.ch); URLhaus | emotet (abuse.ch)

[25] QakBot (fraunhofer.de); Qakbot Botnet C&Cs (abuse.ch); URLhaus | Qakbot (abuse.ch); s. a. Halbjahresbericht 2021/2 (ncsc.admin.ch), Kap. 4.2.3.

[26] Formbook (fraunhofer.de); Xloader (fraunhofer.de); URLhaus | Formbook (abuse.ch)

[27] 404 Keylogger (fraunhofer.de); URLhaus | SnakeKeylogger (abuse.ch)

[28] Siehe Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 3.1.1.

[29] Vgl. Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 3.1.2.

Plattformen, die in der Cloud betrieben werden, sind ebenfalls exponiert und können bei mangelhafter Absicherung, fehlerhafter Konfiguration oder via Software-Verwundbarkeiten angegriffen werden. Ähnlich verhält es sich mit Bedienoberflächen («Webinterfaces») von Systemen, die aus der Ferne überwacht und gesteuert werden.

Schlussfolgerung / Empfehlung:

Sobald eine Verwundbarkeit in einem Produkt bekannt wird, beginnen verschiedene Akteure, das Internet nach verwundbaren Systemen abzusuchen. Nach einigen Stunden oder Tagen beginnt das Ausnutzen dieser Schwachstelle.

Sowohl Privatpersonen als auch Unternehmen sollten Software auf allen Geräten immer auf dem neuesten Stand halten, am besten mittels automatischer Update-Funktion.

Das NCSC informiert regelmässig Organisationen, die über veraltete Systeme angreifbar sind.[30] Es erhält entsprechende Hinweise von Sicherheitsforschern, die das Internet nach solchen Systemen absuchen. In gleicher Weise können auch Kriminelle verwundbare Systeme suchen und angreifen. Systembetreibende sollten deshalb nicht darauf warten, vom NCSC eine Nachricht zu bekommen. Ein eigenes, effektives Software-Management mit Inventar und Update-Prozessen ist dringend empfohlen.[31] Spätestens jedoch wenn ein eingeschriebener Brief vom NCSC bei der Organisation eintrifft, ist rascher Handlungsbedarf gegeben.

5.2 Schadsoftware / Malware

5.2.1 Generelle Lage

Die folgende Grafik zeigt Malware-Familien, welche vom NCSC im vergangenen halben Jahr analysiert und identifiziert worden sind. 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 Betreibenden kritischer Infrastrukturen, damit diese sich schützen können.

[30] Höchste Zeit, die Sicherheitslücken bei Microsoft Exchange-Server zu schliessen (ncsc.admin.ch); MS Exchange-Lücken werden noch immer nicht geschlossen (ncsc.admin.ch)

[31] Siehe Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 3.2.

Analyse von Malware-Familien

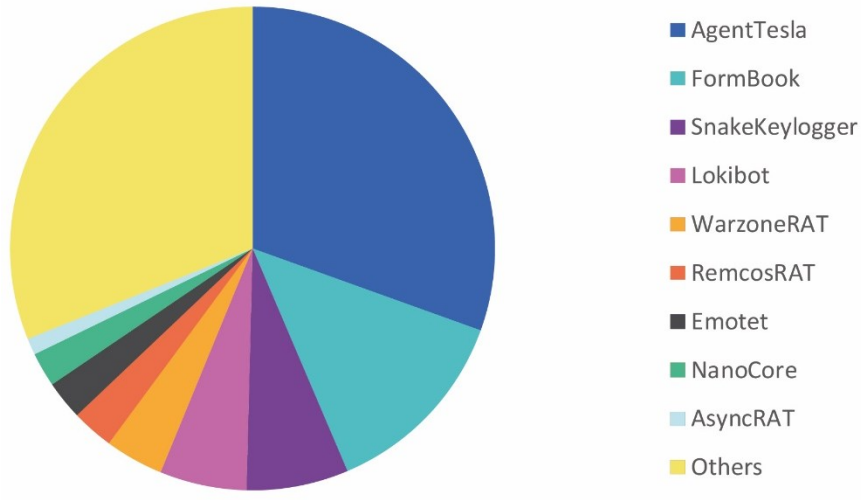


Abb. 6: Analysen des NCSC von Malware-Familien in der Schweiz im ersten Semester 2022.

Die folgende Grafik zeigt die Malware-Familien, die im Berichtszeitraum in der Schweiz durch Analysen von DNS-Sinkhole-Daten festgestellt wurden. DNS-Sinkholes werden dazu verwendet, Schadsoftware abzuwehren, indem der Zugriff der Malware auf die vorgesehenen Domains verhindert und diese Domains auf eine Sicherheitsorganisation umregistriert werden. So können infizierte Geräte identifiziert werden, die sich nun, statt mit dem Server des Malware-Betreibers, mit dem Server der Sicherheitsorganisation verbinden. Das NCSC erhält diese Daten von verschiedenen internationalen Partnern für den gesamten Schweizer Adressraum und informiert die Besitzer dieser Geräte via deren Provider über die Infektion.

Malware-Infektionen

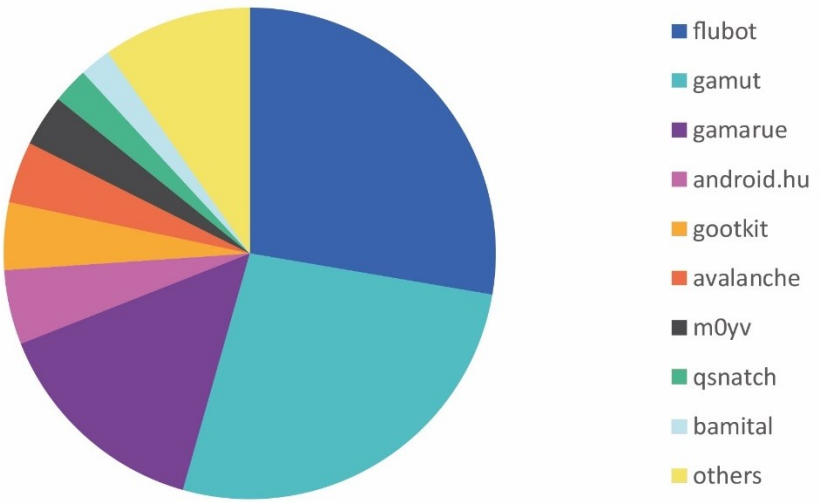


Abb. 7: Verteilung der vom NCSC festgestellten Malware-Infektionen in der Schweiz im ersten Semester 2022.

5.2.2 Ransomware

Auch in diesem Jahr führen Cyberkriminelle Ransomware-Kampagnen durch. Mittlerweile sind weltweit sämtliche Branchen von derartigen Angriffen betroffen[32] und Ransomware[33] ist weiterhin die akuteste Cyberbedrohung, der Organisationen in der Schweiz ausgesetzt sind.

5.2.2.1 Vorfälle in der Schweiz

Seit Jahresbeginn sind in der Schweiz verschiedene Organisationen in diversen Sektoren Ziele von Angriffen geworden.[34]

In den Fällen im Gesundheitswesen griffen die Täter häufig zum Mittel der doppelten Erpressung («Double Extortion») mithilfe der Ransomware «LockBit 2.0»,[35] bei der sensible Daten eines Opfers zuerst kopiert und anschliessend auf den Opfersystemen verschlüsselt werden. So sahen sich zahlreiche Einrichtungen im Schweizer Gesundheitswesen mit der Verschlüsselung ihrer Server sowie mit Datenlecks konfrontiert. Die Informationen landeten oft im Darknet. Betroffen von solchen Angriffen sind deshalb nicht nur die Institutionen, sondern indirekt auch die Patientinnen und Patienten, denn die abgeflossenen Informationen enthalten neben deren Personalien vielfach auch sensible Daten wie Krankengeschichten.[36]

In Sektoren wie Verkehr und Logistik, von deren Funktionieren viele andere Sektoren abhängig sind, versuchen die Täter den Geschäftsbetrieb grösstmöglich zu stören, um das Opfer unter Druck zu setzen und zur Zahlung von Lösegeld zu bewegen.[37] Im Fall von Swissport haben das Betriebskontinuitätsmanagement und Backups dabei geholfen, dass sich die Auswirkungen auf andere Unternehmen in Grenzen hielten.[38]

Im Bildungssektor war im Februar 2022 die Universität Neuenburg von einem Ransomware-Angriff betroffen. Dies führte immerhin zu einer Beschleunigung der Umsetzung neuer Sicherheitsmassnahmen, die der Kanton angesichts früherer Cyberangriffe auf die Waadtländer Gemeinden Rolle und Montreux bereits geplant hatte.[39] Diese Massnahmen umfassen insbesondere wiederholte Penetrationstests und eine verbesserte Angriffsfrüherkennung.[40]

Die vorgenannten Beispiele stellen nur einen Teil der Ransomware-Angriffe dar, die dieses Jahr bislang in der Schweiz stattgefunden haben. Eine umfassendere Auflistung der Ransomware-Angriffe im In- und Ausland im Jahr 2022 ist in verschiedenen Medien zu finden.[41]

---

32 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)

33 Ransomware (ncsc.admin.ch); What Is Ransomware? (trellix.com)

34 Hackerangriff auf Schweizer Spitalverband (inside-it.ch); Hackerangriff auf Swissport sorgt für Verspätungen im Flugbetrieb (computerworld.ch); Cyberangriff auf Luzerner ÖV bleibt ohne grössere Folgen (inside-it.ch); Cyberattaque contre Emil Frey: des données publiées sur le darkweb (ictjournal.ch); Ransomware-Attacke: «BlackByte» hackt Schweizer Logistikkonzern (watson.ch); Le pire est survenu: les données volées à l'Université de Neuchâtel ont été publiées (letemps.ch)

35 Hacker veröffentlichen erneut sensible Schweizer Gesundheitsdaten (inside-it.ch)

36 Des hackers diffusent les données médicales de Neuchâtelois (watson.ch)

37 The future of cyber security: Ransomware groups aim for maximum disruption (darktrace.com)

38 BlackCat ransomware gang claims responsibility for Swissport attack (computerweekly.com)

39 Neuchâtel a amélioré sa cybersécurité (rtn.ch)

40 Cyberattaque: le canton a pris des mesures (swissinfo.ch)

41 The terrifying list of cyber attacks worldwide (konbriefing.com);
Hacker schlagen in der Schweiz zu: Die unfassbar lange Opfer-Liste (watson.ch)

5.2.2.2 Vorfälle im Ausland

Angriffe auf Regierungen und Behörden

Seit April 2022 sind in Lateinamerika mehrere Regierungsbehörden Opfer von Ransomware-Angriffen geworden, an denen wahrscheinlich russischsprachige Täter beteiligt waren.[42] Länder wie Costa Rica, Peru, Mexiko, Ecuador, Brasilien und Argentinien gehören zu denjenigen Staaten, die an der Generalversammlung der Vereinten Nationen Russlands Invasion der Ukraine verurteilt hatten. Costa Rica musste aufgrund der Angriffe sogar den nationalen Notstand ausrufen. An diesen Angriffen auf südamerikanische Regierungen beteiligt waren unter anderem Ransomware-Gruppen wie Conti, ALPHV/BlackCat, LockBit und BlackByte. Am 24. Mai erlitten die IT-Systeme des österreichischen Landes Kärnten einen Ransomware-Angriff der BlackCat-Gruppe, der zu temporären Betriebsstörungen bei den staatlichen Diensten führte.[43]

Angriffe auf Energieinfrastrukturen

In Europa waren ab Ende Januar 2022 aufgrund von Angriffen mit Ransomware mehrere Ölterminals in den Niederlanden und Belgien (Amsterdam, Rotterdam und Antwerpen) sowie in Deutschland (Oiltanking GmbH) von IT-Problemen betroffen.[44] Cybersicherheitsspezialisten dieser Länder erklärten, sie hätten keinen Grund zur Annahme, dass diese Angriffe miteinander verbunden seien.[45] Von den Vorfällen waren insgesamt rund zehn Ölterminals auf der ganzen Welt betroffen, welche Betriebsstörungen meldeten.[46] Die russischen Ransomware-Gruppen BlackCat und Conti werden mit diesen Vorfällen in Verbindung gebracht.[47]

5.2.2.3 Überblick über die aktivsten Akteure

Conti und die Nachfolger

Die erfolgreiche russische Gruppe Conti[48] hat im Mai 2022 ihre Aktivitäten eingestellt.[49] Nach der Zusicherung ihrer Unterstützung für Russland, kurz nach dessen Invasion in die Ukraine, machte die Gruppe im Frühling viel von sich reden,[50] insbesondere als ein Insider interne Chats der Mitglieder durchsickern liess, die die Vorgehensweise der Gruppe enthüllten.[51] Dieses als «Conti-Leaks»[52] bezeichnete Ereignis sowie unterschiedliche politische Einstellungen haben wohl zur Auflösung der Gruppe geführt. Verschiedene Mitglieder haben sich danach in

---

42 Latin American Governments Targeted By Ransomware (recordedfuture.com)
43 Hackerangriff auf Land Kärnten: "Black Cat" will fünf Millionen Dollar in Bitcoin (derstandard.at)
44 Des cyberattaques signalées contre des sites portuaires en Allemagne, en Belgique et aux Pays-Bas (lemonde.fr)
45 String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say (therecord.media)
46 Oil terminals in Europe's biggest ports hit by a cyberattack (securityaffairs.co)
47 BlackCat ransomware implicated in attack on German oil companies (zdnet.com)
48 The Conti Enterprise: ransomware gang that published data belonging to 850 companies (group-ib.com); The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs (securelist.com)
49 Conti ransomware finally shuts down data leak, negotiation sites (bleepingcomputer.com); Ransomware-Gang Conti schließt Leak- und Verhandlungsplattform (heise.de)
50 Conti ransomware gang backs Russia, threatens US (techtarget.com)
51 Inside Conti leaks: The Panama Papers of ransomware (therecord.media)
52 Conti-nuation: methods and techniques observed in operations post the leaks (nccgroup.com)

kleineren Gruppen organisiert, die sich stärker auf einzelne Phasen eines Ransomware-Angriffs wie Netzwerkzugriffe oder Datendiebstahl spezialisierten.[53] So bestehen zum Beispiel gewisse Ähnlichkeiten zwischen den Taktiken, Techniken und Vorgehensweisen (Tactics, Techniques, and Procedures – TTPs) von Conti und denen der neuen Gruppen BlackBasta[54] und BlackByte[55]. BlackBasta katapultierte sich schon im April ins Rampenlicht, als sie innerhalb weniger Wochen mindestens ein Dutzend Unternehmen auf der ganzen Welt mit Malware infizierte.[56] Sie weist Gemeinsamkeiten mit Conti in Bezug auf Datenleck-Blogs, Zahlungsseiten, Wiederherstellungsportale, Kommunikation mit Opfern und Verhandlungsmethoden auf.[57] Was BlackByte betrifft, so verfügt deren Ransomware über Funktionalitäten und Merkmale, die grosse Ähnlichkeit mit Conti aufweisen.[58]

BlackCat neu in Erscheinung getreten

BlackCat, auch bekannt als ALPHV, dessen gleichnamige Betreibergruppe sich aus ehemaligen Mitgliedern der berüchtigten Organisation BlackMatter/DarkSide[59] zusammensetzt, ist im November 2021 erstmals in Erscheinung getreten. Diese Ransomware ist hochgradig anpassbar und bietet verschiedene Verschlüsselungsmethoden und -optionen, die Angriffe auf eine Vielzahl von Unternehmen (insbesondere Grossunternehmen) ermöglichen.[60] Eine Besonderheit des angewendeten Geschäftsmodells liegt darin, dass in der ersten Erpressungsphase der Name des Opfers nicht sofort veröffentlicht, sondern lediglich eine Beschreibung der betroffenen Organisation auf der Data-Leak-Site aufgeschaltet wird. Alternativ wird eine versteckte Webseite erstellt, deren Adresse dann ausschliesslich dem Opfer zur Verifikation gesendet wird. Auf diese Weise geben die Täter ihren Opfern Gelegenheit zur diskreten Verhandlung des Lösegelds und halten den Druck mit der Veröffentlichungsdrohung aufrecht.[61] Entscheidet sich die Gruppe schliesslich für die Veröffentlichung der Daten, nutzt sie dazu eine reguläre Website statt einer Darknet-Seite. Dies erlaubt es ihr, ein breiteres Publikum zu erreichen. So können auch technisch weniger versierte vom Datenleck des Opfers betroffene Personen (wie Angestellte oder Kundinnen und Kunden) prüfen, ob ihre Daten kompromittiert wurden, und können sogar alle Daten und Dokumente herunterladen, die dem Unternehmen gestohlen worden sind.[62]

---

53 Conti ransomware shuts down operation, rebrands into smaller units (bleepingcomputer.com); Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com)
54 Shining the Light on Black Basta (nccgroup.com)
55 Threat Spotlight: The BlackByte ransomware group is striking users all over the globe (talosintelligence.com)
56 New Black Basta ransomware springs into action with a dozen breaches (bleepingcomputer.com)
57 New Black Basta Ransomware Possibly Linked to Conti Group (securityweek.com)
58 Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com)
59 Aggressive BlackCat Ransomware on the Rise (darkreading.com)
60 Threat Assessment: BlackCat Ransomware (paloaltonetworks.com)
61 Ransomware gangs now give victims time to save their reputation (bleepingcomputer.com)
62 Ransomware gang publishes stolen victim data on the public Internet (helpnetsecurity.com)

Comeback von REvil und Cl0p

Das Frühjahr 2022 war durch das Auftauchen neuer Ransomware-Gruppen, aber auch durch die Rückkehr anderer geprägt.

Die berüchtigte Ransomware-Organisation REvil ist Ende April wieder aktiv geworden, mit neuer Infrastruktur und einer weiterentwickelten Ransomware.[63] Die REvil-Ransomware-Bande hatte ihre Tätigkeit im Oktober 2021 eingestellt. Ein koordinierter Polizeieinsatz zwischen den USA und Russland führte zur Festnahme von REvil-Mitgliedern in Russland im Januar 2022.[64] Nach russischen Angaben sei die Kommunikation zwischen den beiden Ländern nach dem russischen Militärangriff auf die Ukraine eingestellt worden und zudem habe die US-Regierung nicht genügend Informationen weitergegeben, damit Anklage hätte erhoben werden können.[65]

Die Gruppierung Cl0p ist nach einigen Monaten der vermeintlichen Untätigkeit im April ebenfalls wieder in Erscheinung getreten. Forschende bemerkten die Rückkehr, nachdem die Ransomware-Gruppe in einem einzigen Monat 21 neue Opfer zu ihrer Datenleck-Site hinzugefügt hatte.[66]

LockBit

Die Ransomware-as-a-Service (RaaS)-Gruppe[67] LockBit war dieses Jahr bereits für viele Vorfälle verantwortlich.[68] Auf ihrer Datenleck-Site werden jeweils die vermeintlichen Opfer genannt und mit einem Countdown wird angekündigt, wann die gestohlenen Daten veröffentlicht werden. Mehrfach hat sich jedoch herausgestellt, dass es LockBit mit den Ankündigungen nicht so genau nimmt. So wurde beispielsweise nicht, wie behauptet, das französische Justizministerium gehackt, sondern eine Anwaltskanzlei in Caen.[69] Auch die Behauptung, Daten des amerikanischen Sicherheitsdienstleisters Mandiant erbeutet zu haben, entpuppte sich als unwahr.[70] Es scheint, dass die Gruppe manchmal vor allem Aufmerksamkeit erregen will. Die Schlagkraft dieser Ransomware-Gruppe ist dennoch nicht zu unterschätzen, schliesslich gab es in Europa innert eines halben Jahres pro Monat rund hundert Opfer.[71]

Die eingesetzte Ransomware wird ähnlich wie normale Software regelmässig aktualisiert. Nachdem im Juni 2021 die Version 2.0 erschien,[72] existiert inzwischen bereits die Version 3.0.[73]

---

63 REvil ransomware returns: New malware sample confirms gang is back (bleepingcomputer.com)

64 Russia takes down REvil hacking group at U.S. request - FSB (reuters.com)

65 REvil prosecutions reach a 'dead end,' Russian media reports (cyberscoop.com)

66 Clop ransomware gang is back, hits 21 victims in a single month (bleepingcomputer.com)

67 Ransomware as a Service (RaaS) ist ein Geschäftsmodell zwischen Betreibenden von Ransomware und ihren Partnern, wobei die Partner dafür bezahlen, dass mit der von den Betreibenden entwickelten Ransomware Angriffe lanciert werden. Dies kann als eine Variante des Software-as-a-Service(SaaS)-Geschäftsmodells angesehen werden; Ransomware as a Service (RaaS) Explained (crowdstrike.com)

68 LockBit overtakes Conti as most active ransomware group so far in 2022 (scmagazine.com)

69 Ministère de la Justice : Le groupe Lockbit publie des données, mais pas les bonnes (zdnet.fr)

70 Mandiant: “No evidence” we were hacked by LockBit ransomware (bleepingcomputer.com)

71 Ransomware LockBit : une centaine de victimes par mois au premier semestre (lemagit.fr)

72 LockBit 2.0: How This RaaS Operates and How to Protect Against It (paloaltonetworks.com)

73 LockBit 3.0: Significantly Improved Ransomware Helps the Gang Stay on Top (darkreading.com)

Schlussfolgerungen, Ausblick und Empfehlungen:

Die Zahl der Ransomware-Angriffe dürfte in diesem Jahr weiter zunehmen und vermehrt auch kritische Infrastrukturen treffen. Die US-amerikanische Cybersecurity and Infrastructure Security Agency (CISA) stellte bereits 2021 fest, dass ausgeklügelte Angriffe auf kritische Infrastrukturen mit schwerwiegenden Folgen zunehmen.[74] Tatsächlich haben sich Ransomware-Strategien und -Techniken im Jahr 2021 weiterentwickelt, was sich neben dem Fortschritt der Technologien in einer Zunahme der Ransomware-Bedrohung für alle Arten von Organisationen auf der Welt zeigt.[75]

Obwohl der Kriegsausbruch in der Ukraine zu einigen Reorganisationen im Ökosystem der Cyberkriminalität geführt hat, erweisen sich die Ransomware-Akteure als resilient. Gruppen lösen sich auf, formieren sich neu, ändern Namen oder ersetzen Funktionäre nach Bedarf – z. B wenn der Druck durch Strafverfolgungsbehörden zu hoch wird oder wie bezüglich dem Ukrainekrieg, wenn Meinungsverschiedenheiten die Zusammenarbeit in einer Gruppe beeinträchtigen.

Neben Cybersicherheitsmassnahmen, welche die Systeme vor Infektionen mit Malware generell und damit auch vor Ransomware schützen, gibt es auch Massnahmen, die hinter der ersten Verteidigungslinie eingesetzt werden können. Forschende haben in einigen Ransomware «Schwachstellen» gefunden, die ausgenutzt werden können, um zumindest die finale Datenverschlüsselung zu verhindern.[76]

Ransomware kann erheblichen Schaden verursachen, insbesondere dann, wenn auch Datensicherungen (Backups) davon betroffen sind. Wichtige Aspekte der Vorfallsbewältigung sind auf der NCSC-Website beschrieben: Ransomware - Was nun? (ncsc.admin.ch).

Darüber hinaus hat die US-amerikanische Cybersicherheitsbehörde CISA ein Dokument veröffentlicht, das sich an Unternehmen richtet, um Datenlecks durch Ransomware-Angriffe zu verhindern und darauf zu reagieren.[77]

5.2.3 Mobile Malware

Nach der letzten grossen Welle im Herbst 2021, war ab dem 18. März 2022 in der Schweiz erneut die Schadsoftware «Flubot» im Umlauf. Mittels SMS versuchte man die Opfer zu verleiten, die Schadsoftware auf dem Smartphone zu installieren. Diese Welle zielte international[78] auf Android-Geräte ab. In der Schweiz wurden mehrheitlich SMS mit gefälschten Paketbenachrichtigungen verbreitet, wobei International auch SMS mit dem Text «Bist Du das auf dem Video?» oder gefälschte Aufforderungen zur Aktualisierung von Browser oder Betriebssystem beobachtet wurden. Das NCSC hat diese Thematik im Wochenrückblick Nr. 12 aufgenommen.[79]

---

74 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)
75 Ransomware: Over half of attacks are targeting these three industries (zdnet.com)
76 Conti, REvil, LockBit ransomware bugs exploited to block encryption (bleepingcomputer.com)
77 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches (cisa.gov)
78 New FluBot and TeaBot campaigns target Android devices worldwide (bleepingcomputer.com)
79 Woche 12: Schadsoftware «FluBot» in der Schweiz wieder aktiv (ncsc.admin.ch)

«FluBot» hat sich unter anderem auf den Diebstahl von SMS auf Mobiltelefonen spezialisiert. Ziel dabei war, in den gestohlenen SMS so genannte Einmal-Passwörter zu finden. Nach einer Infektion wurde zudem das ganze Adressbuch des infizierten Smartphones an den Kontrollserver der Angreifer gesendet. Das Smartphone erhielt danach eine Liste mit Telefonnummern, die von anderen gehackten Smartphones stammen, an die es das bösartige SMS senden sollte. Im ersten Halbjahr 2022 hat das NCSC 56 Meldungen zu «Flubot» erhalten.

Die Infrastruktur von «Flubot» wurde Anfang Mai erfolgreich von der niederländischen Polizei gestört, wodurch dieser Malware-Stamm inaktiv wurde. Diese Aktion folgte auf eine komplexe Untersuchung, an der die Strafverfolgungsbehörden Australiens, Belgiens, Finnlands, Ungarns, Irlands, Spaniens, Schwedens, der Schweiz, der Niederlande und der USA beteiligt waren. Die internationalen Aktivitäten wurden vom Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) von Europol koordiniert.[80] Seit diesem Zeitpunkt wurde in der Schweiz keine neue Aktivität von «Flubot» festgestellt.

Empfehlungen:

- Installieren Sie auf Ihrem Mobiltelefon keine Apps, die ausserhalb der offiziellen Stores angeboten werden.
- Insbesondere sollten Sie keine App installieren, die Sie über einen Link in einem SMS oder über einen anderen Messenger-Dienst (WhatsApp, Telegram, usw.) erhalten haben.

5.2.4 «CyclopsBlink» Botnetz – Störung des «VPNFilter» Nachfolgers

Im May 2018 veröffentlichte das Sicherheitsunternehmen Cisco Talos neuste Erkenntnisse zur «VPNFilter»-Malware[81], welche vornehmlich Router von Klein- und Heimbüronutzern (Small Office Home Office, SOHO) sowie Netzwerkspeicher (Network Attached Storage, NAS) infizierte. Nach einem grösstenteils erfolgreichen Takedown durch die amerikanische Justiz[82] gegen die VPN-Filter-Infrastruktur wurde es ruhig um die Aktivitäten, welche der Akteurgruppe Sandorm[83] zugeschrieben wurden.

Am Vorabend des russischen Angriffs auf die Ukraine publizierten britische[84] und amerikanische Sicherheitsbehörden Details zum mutmasslichen Nachfolger-Botnet «CyclopsBlink», welches hauptsächlich Watchguard-Geräte und Asus-Router[85] infizierte.

Betreibende von infizierten Geräten, darunter auch einzelne in der Schweiz, wurden via ihre Internetanbieterinnen oder nationalen CERTs benachrichtigt.[86] Bei einigen Steuergeräten des

---

80 Takedown of SMS-based FluBot spyware infecting Android phones (europol.europa.eu)

81 New VPNFilter malware targets at least 500K networking devices worldwide (thalosintelligence.com)

82 Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices (justice.gov)

83 Sandworm (Threat Actor) (fraunhofer.de); s.a. Kap. 3.1 und 3.2.2

84 New Sandworm malware Cyclops Blink replaces VPNFilter (ncsc.gov.uk)

85 Cyclops Blink Sets Sights on Asus Routers (trendmicro.com)

86 Shadowserver Special Reports – Cyclops Blink (shadowserver.org)

Botnets, bei welchen die Betreibenden keine Bereinigung durchführten, wurde das amerikanische Justizministerium selbst aktiv und entfernte die Malware nach einem Gerichtsbeschluss.[87]

Somit konnte die westliche Cybersicherheitsgemeinschaft die Angriffsinfrastruktur von Sandworm wirkungsvoll beeinträchtigen und potentiell weitere Angriffe, wie im Fokusthema (Kap. 3.1 und 3.2) oder im Kapitel zu industriellen Kontrollsystemen (Kap. 5.4.1) beschrieben, verhindern oder zumindest stören.

Empfehlungen

Das NCSC gibt auf seiner Website Empfehlungen zum sicheren Umgang mit Geräten für Endnutzende und für Betreibende von Geräten des Internet of Things (IoT).

5.3 Angriffe auf Websites und -dienste

Die Beeinträchtigung der Verfügbarkeit von Websites durch DDoS-Angriffe bleibt wie bereits zuvor ein anhaltendes Phänomen im In- und Ausland. Im ersten Halbjahr 2022 wurden dem NCSC 10 Vorfälle dieser Art von diversen Schweizer KMUs aus unterschiedlichen Branchen gemeldet. Solche Angriffe können zwecks Erpressung, zur Schädigung von Konkurrenzunternehmen aber auch aus politischer Motivation erfolgen.

Berichten von weltweit tätigen Sicherheitsunternehmen zufolge gibt es zwar immer stärkere (Rekord 1,4 Tbit/s) und komplexere (Kombination von verschiedenen Angriffsmethoden) Angriffe,[88] die allermeisten DDoS-Angriffe werden jedoch weiterhin mit relativ geringer Intensität (unter 10 Gbit/s) ausgeführt.[89] Zu beachten sind neben der Datenübertragungsrate auch Faktoren wie Pakete pro Sekunde (pps) sowie Anfragen pro Sekunde (rps). Cloudflare registrierte beispielsweise einen Angriff mit 26 Mio. Anfragen pro Sekunde, welcher von einem kleinen aber diesbezüglich leistungsstarken Botnetz mit nur 5'067 Geräten ausging.[90]

Im Angriffskrieg auf die Ukraine führte eine pro-russische respektive Anti-NATO Hacktivistengruppe, die sich Killnet nennt, seit April 2022 eine Reihe von DDoS-Angriffen gegen Länder durch, welche die Ukraine durch Waffenlieferungen, Geld oder Sanktionen unterstützten. Unter anderem wurden Websites der UNO, der OSZE, der NATO sowie Organisationen in der Ukraine, der Tschechischen Republik, Estland, Lettland, Litauen, Deutschland, Norwegen, Polen, Rumänien, Grossbritannien, Italien und den USA angegriffen. Darunter befanden sich viele Flughäfen,[91] zahlreiche Behörden, Banken, Eisenbahngesellschaften, Energiekonzerne und Internet Service Provider (siehe auch Kap. 3.3).

87 Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (justice.gov)
88 DDoS attacks becoming larger and more complex, finance most targeted sector (helpnetsecurity.com)
89 DDoS threats growing in sophistication, size, and frequency (helpnetsecurity.com)
90 Cloudflare mitigates 26 million request per second DDoS attack (cloudflare.com)
91 Russia-Ukraine: malicious cyber activity targeting aviation entities (ospreyflightsolutions.com)

Schlussfolgerung / Empfehlungen:

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

5.4 Industrielle Kontrollsysteme (ICS) & operative Technologie (OT)

Im Umfeld von geopolitischen Konflikten werden sporadisch auch zerstörerische Cybersabotageangriffe beobachtet.[92] Um Wirkung auf physische Prozesse zu erzielen, braucht es fast zwangsläufig eine Manipulation an der operativen Technologie, respektive deren Steuerungssystemen. Solche Angriffe sind zeit- und ressourcenintensiv, deren Wirkung bei einem bereits zu Waffengewalt eskalierten Konflikt mit dem Einsatz von kinetischen Mitteln tendenziell einfacher erreicht werden kann (siehe Fokusthema Kap. 3.2.2 zu «Industroyer2»).

5.4.1 Pipedream / Incontroller: OT-Angriffswerkzeuge

Einen Tag nach der Bekanntgabe der Angriffe mit «Industroyer2» (siehe Kap. 3.2.2) veröffentlichten mehrere US-Behörden in einer gemeinsamen Warnung Details zu einer weiteren Sammlung von modularen Angriffswerkzeugen,[93] welche zu Cybersabotagezwecken gegen Geräte in der Energieversorgung und verwandten Sektoren eingesetzt werden könnten. Die Veröffentlichung erfolgte präventiv bevor ein operativer Einsatz einer der beschriebenen Schadsoftware-Varianten beobachtet wurde.

Die Publikation der entdeckten Cybersabotagewerkzeuge durch die US-Regierung wurde in Zusammenarbeit mit zwei auf industrielle Systeme spezialisierten amerikanischen Cybersicherheitsunternehmen vorbereitet, welche die Schadsoftware-Sammlung «Pipedream»[94], respektive «Incontroller»[95] tauften. Die präventive Berichterstattung folgt in einer Reihe mit früheren Bekanntmachungen zu vorwiegend russischer Angriffsinfrastruktur. Neben der Beeinträchtigung des Einsatzpotenzials der aufgedeckten Angriffsmittel, nutzt die Biden-Administration das Aufzeigen der Fähigkeiten potentieller Angreifer gegenüber inländischen Betreibenden kritischer Infrastrukturen gleichzeitig zur Betonung der Dringlichkeit, empfohlene Schutzmassnahmen unter dem Slogan «Shields Up»[96] zeitnah umzusetzen.

---

92 Siehe insbesondere zu «Stuxnet» im Halbjahresbericht 2010/2 (ncsc.admin.ch), Kap. 4.1 und 5.1) und zu Triton/Trisis im Halbjahresbericht 2017/2 (ncsc.admin.ch), Kap. 5.3.2.

93 APT Cyber Tools Targeting ICS/SCADA Devices (cisa.gov)

94 CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS) (dragos.com)

95 INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple ICS (mandiant.com)

96 Shields Up (cisa.gov)

5.4.2 ICEFALL: 56 OT-Schwachstellen

Der Aufruf nach mehrschichtigen Abwehrdispositiven rührt nicht nur von neuen Erkenntnissen hinsichtlich der Fähigkeiten von Angreifern[97] industrieller Kontrollsysteme, sondern liegt auch in der teilweise ungenügend sicheren Ausgestaltung der eingesetzten Technologie. So publizierte das Cybersicherheitsunternehmen Forescout unter der Bezeichnung «ICEFALL»[98] eine Sammlung von 56 Schwachstellen in bekannten OT-Produkten. Das ICS-CERT der CISA publiziert zudem laufend neue Sicherheitsempfehlungen[99] der verschiedenen Hersteller. Um diesbezüglich den Überblick zu behalten, kann das Common Security Advisory Frameworks (CSAF) eingesetzt werden, welches vom Cyber Defense Campus der armasuisse zusammen mit den Experten des deutschen BSI mitentwickelt wurde.[100]

Schlussfolgerung / Empfehlungen:

Die neu aufgedeckten Angriffswerkzeuge und Schwachstellen zeigen, dass es notwendig ist, in die Absicherung des Zugriffs auf industrielle Kontrollsysteme zu investieren und den Betrieb sowie Manipulationen zu überwachen, damit bei Verdacht auf missbräuchliche Änderungen zeitnah reagiert werden kann.

Das NCSC empfiehlt auf seiner Website Massnahmen zum Schutz von ICS (ncsc.admin.ch)

5.5 Schwachstellen

5.5.1 Log4Shell

Die bereits im Halbjahresbericht 2021/2 des NCSC erwähnte Schwachstelle Log4Shell ist weiterhin aktuell. Im ersten Halbjahr 2022 wurde diese Schwachstelle insbesondere genutzt, um VMware-Server, auf denen die Patches nicht installiert waren, anzugreifen und zu kompromittieren.[101]

Aufgrund der Beschaffenheit dieser Schwachstelle kann sie in einer Anwendung oder einem System eingebettet sein, die bzw. das nicht unter die direkte Verantwortung des Sicherheitsteams einer Organisation fällt. Sie ist dadurch schwer zu erkennen und zu beheben.

Das Cyber Safety Review Board des US-Heimatschutzministeriums stellt in einem aktuellen Bericht fest: «Das Log4j-Ereignis ist noch nicht vorbei. Die Kommission ist der Ansicht, dass Log4j eine ‹endemische Schwachstelle› sei und dass anfällige Instanzen von Log4j noch viele Jahre, möglicherweise ein Jahrzehnt oder länger, in Systemen verbleiben werden. Es bleibt ein erhebliches Risiko bestehen.»[102]

97 Three new ICS threat groups discovered, one primed to disrupt energy targets (scmagazine.com)
98 OT:ICEFALL: 56 Vulnerabilities Caused by Insecure-by-Design Practices in OT (forescout.com)
99 ICS-CERT Advisories (cisa.gov)
100 Zusammenarbeit CYD Campus und BSI (admin.ch)
101 Log4Shell Vulnerability Targeted in VMware Servers to Exfiltrate Data (threatpost.com)
102 CSRB Report on Log4j - Public Report - July 11 2022_508 Compliant (cisa.gov)

Schlussfolgerung / Empfehlungen:

Angesichts dieser Art von Schwachstelle, die in der Infrastruktur einer Organisation durch von Drittanbietern bereitgestellte Software auftreten kann, wird empfohlen, innerhalb einer Organisation die Kapazität zu entwickeln, ein genaues Inventar der IT-Assets und -Anwendungen zu führen, der Durchführung von Softwareupdates Priorität einzuräumen und in die Fähigkeiten zur Erkennung anfälliger Systeme zu investieren. Der Bericht des Cyber Safety Review Board enthält ebenfalls detailliertere Empfehlungen zu Log4Shell.

5.5.2 Follina

Am 31. Mai 2022 wies Microsoft einer Schwachstelle namens «Follina» die Nummer CVE-2022-30190 zu. Diese Schwachstelle ermöglicht selbst bei deaktivierter Makrofunktion eine Remote-Code-Ausführung über msdt (ein Microsoft Support-Tool), wenn ein Dokument in den Anwendungen der Office-Suite geöffnet oder in der Vorschau angezeigt wird. Microsoft wurde im März 2021 über diese Schwachstelle informiert. Die Zuweisung einer CVE-Nummer ist jedoch erst erfolgt, als diese Schwachstelle bereits ausgenutzt wurde.

Sicherheitsforschende haben im Internet mehrere Abwehr- und Erkennungstechniken veröffentlicht, die Schwachstelle wurde jedoch erst anlässlich des «Patch Tuesday» im Juni 2022 behoben.

Eine Chronologie, die den Ablauf der Ereignisse von der Erkennung bis zur Umsetzung von Abwehrmassnahmen detailliert darstellt, dokumentiert die Ausnutzung dieser Schwachstelle, bevor sie öffentlich bekannt wurde.[103]

Schlussfolgerung / Empfehlungen:

Im Fall von Follina wurden die für einen Exploit erforderlichen Details veröffentlicht, bevor ein offizieller Patch verfügbar war und die Schwachstelle wurde bereits von verschiedenen Akteuren ausgenutzt. In solchen Fällen ist es für Unternehmen und Organisationen wichtig, sich kontinuierlich zu informieren, die neuesten Empfehlungen zu analysieren und gegebenenfalls risikomindernde Massnahmen umzusetzen, bis ein offizieller Patch verfügbar ist und installiert werden kann.

Es wird nach wie vor empfohlen, bewährte Verfahren in Bezug auf die Computersicherheit anzuwenden. Mitarbeitende, die darin geschult sind, bösartige E-Mails zu erkennen und Anhänge nicht herunterzuladen oder auszuführen, können dazu beitragen, diese Art von Angriffen zu vereiteln.[104]

[103] Follina — a Microsoft Office code execution vulnerability (doublepulsar.com)

[104] Verhalten bei E-Mail (ncsc.admin.ch)

5.5.3 Confluence

Am 2. Juni 2022 veröffentlichte Atlassian ein Sicherheitsbulletin über eine kritische Schwachstelle in ihrer Wiki-Software Confluence, die als CVE-2022-26134 gekennzeichnet wurde.[105] Ein erfolgreicher Exploit ermöglichte die Remote-Ausführung von beliebigem Code auf Confluence-Servern. Zum Zeitpunkt der Veröffentlichung des Bulletins war noch kein Patch verfügbar, obwohl die Details, die einen Exploit ermöglichen, öffentlich zugänglich waren und die Schwachstelle aktiv ausgenutzt wurde. Es wurde daher dringend empfohlen, den Zugriff auf Confluence-Instanzen aus dem Internet einzuschränken oder sie bis zur Behebung zu deaktivieren. Der Patch wurde am folgenden Tag veröffentlicht. Die Schwachstelle wurde in mindestens einem Ransomware-Fall in der Schweiz ausgenutzt.

Schlussfolgerung / Empfehlungen:

Wie bei Follina wurde die Schwachstelle CVE-2022-26134 aktiv ausgenutzt, noch bevor ein offizieller Patch verfügbar war. Daher ist es wichtig, schnell zu reagieren und den Empfehlungen – die bis zur Abschaltung des anfälligen Systems gehen können – zu folgen, bis ein offizieller Patch verfügbar ist.

Eine klare Strategie für den direkten Internetzugriff auf Verwaltungsschnittstellen und interne Anwendungen kann die Angriffsfläche einer Organisation verringern. Wenn sensible Anwendungen über das Internet zugänglich sein müssen, sollte der Zugriff darauf besonders geschützt werden (z. B. VPN mit Multi-Faktor-Authentifizierung, Liste der autorisierten IPs für die Wartung usw.). Falls es für eine aktiv ausgenutzte Schwachstelle noch keinen Patch gibt, kann man sich durch eine gute Verwaltung externer Zugriffe allenfalls zusätzliche Reaktionszeit für Verteidigungsmassnahmen verschaffen. Dies ersetzt jedoch nicht die Installation von Patches, sobald diese verfügbar werden.

5.6 Datenabflüsse

5.6.1 Datenschutz braucht Datensicherheit

Ein Abfluss von Daten ist für alle Betroffenen eine unangenehme Situation. Niemand will ungefragt persönliche oder schützenswerte Inhalte preisgeben oder jemandem sagen müssen, dass dies mit ihren oder seinen Daten passiert ist. Datenabflüsse kommen jedoch immer wieder vor: Infolge schlecht geschützter oder gewarteter Systeme, menschlicher Fehler, oder durch Angriffe mit kriminellen Absichten. Es ist auch möglich, dass bei einem Ransomware-Angriff die Täterschaft als weitere Erpressungsoption Daten aus einem System abzieht. In solchen Fällen können die betroffenen Personen im Nachgang auch direkt durch die Kriminellen bedroht werden. Dies nennt man dann dreifache Erpressung: Wenn das gehackte Unternehmen weder für eine Entschlüsselung noch für das Verhindern der Publikation der Daten etwas bezahlen will, wenden sich die Erpresser allenfalls direkt an die betroffenen Personen, sei dies ebenfalls mit der Veröffentlichungsdrohung oder in Form eines individuellen und sehr

[105] Confluence Security Advisory 2022-06-02 | Confluence Data Center and Server 7.18 (atlassian.com)

persönlichen Social Engineering Angriffs. Insbesondere bei besonders schützenswerten Personendaten wie Patientendaten stellt dies ein Risiko dar. Das NCSC stellt auf seiner Webseite einen Ratgeber für Unternehmen zum Thema Datenabfluss zur Verfügung.

Kommentar:

In der Schweiz gibt es noch keine gesetzliche Meldepflicht für Verletzungen der Datensicherheit oder Datenabflüsse. Jedoch sollen zukünftig Betreibende von kritischen Infrastrukturen den Behörden Cyberangriffe melden müssen und auch im neuen Datenschutzgesetz ist eine Melde- respektive Informationspflicht vorgesehen.

5.6.2 Lapsus$

Die Cyberkriminellengruppe Lapsus$ sorgte Ende 2021 mit zahlreichen Angriffen in Südamerika und Portugal für Aufmerksamkeit. Bei einem dieser Angriffe wurden mehr als 50 TB Daten des brasilianischen Gesundheitsministeriums gestohlen und dann bei der Behörde gelöscht.[106] Ein weiterer Angriff betraf Impresa, das grösste portugiesische Medienkonglomerat, und verunstaltete dessen Websites mit einer Lösegeldforderung, aus der hervorging, dass sich die kriminelle Gruppe Zugang zur Cloud des Unternehmens verschafft hatte.[107] In beiden Fällen erpresste Lapsus$ seine Opfer und forderte Geld für die Rückgabe der Daten bzw. deren Nichtveröffentlichung. In den ersten Monaten des Jahres 2022 gewann die Gruppe an Bekanntheit, nachdem sie Angriffe auf grosse internationale Technologieunternehmen wie NVIDIA,[108] Samsung,[109] Vodafone,[110] Ubisoft,[111] Microsoft[112] oder noch Okta[113] erfolgreich durchführte. Diese Angriffe führten dazu, dass vertrauliche Daten der betroffenen Unternehmen offengelegt wurden. In der Folge soll Lapsus$ einen Gegenangriff von NVIDIA erlitten und sich dann darüber beschwert haben, dass Daten der Gruppe verschlüsselt worden seien.[114] Ende März 2022 wurden in Grossbritannien sieben Personen im Alter zwischen 16 und 21 Jahren, potenzielle Mitglieder der Gruppe, festgenommen. Zwei von ihnen wurden Anfang April 2022 angeklagt. Die Aktivitäten der Gruppe liessen daraufhin nach und bis Ende des ersten Halbjahres 2022 gingen keine weiteren Meldungen mehr ein. Lapsus$ wurde zu Beginn seiner Aktivität für eine Gruppe gehalten, die mit Ransomware operierte. Die Gruppe exfiltrierte jedoch nur Daten, manchmal löschte sie diese auch, und erpresste ihre Opfer dann mit der Drohung, sie zu veröffentlichen. Um einen Zugriff auf die Systeme ihrer Opfer zu erlangen,

106 Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes (zdnet.com)
107 Lapsus$ ransomware gang hits SIC, Portugal's largest TV channel (therecord.media)
108 NVIDIA confirms data was stolen in recent cyberattack (bleepingcomputer.com)
109 Hackers leak 190GB of alleged Samsung data, source code (bleepingcomputer.com)
110 Vodafone Investigating Source Code Theft Claims (securityweek.com)
111 Ubisoft Cyber Security Incident Update (ubisoft.com)
112 DEV-0537 criminal actor targeting organizations for data exfiltration and destruction (microsoft.com)
113 Updated Okta Statement on LAPSUS$ (okta.com)
114 vx-underground on Twitter (twitter.com)

setzte Lapsus$ häufig Techniken des Social Engineering ein, mit denen sie an Anmeldeinformationen gelangten[115]. Einige ihrer Angriffe wurden möglicherweise auch durch Mitarbeiter der Zielunternehmen ermöglicht, die mit ihnen kooperiert hatten (Insider, interne Bedrohung). Die Gruppe hatte eine entsprechende Ankündigung auf ihrem Telegram-Kanal veröffentlicht, in der sie anbot, Mitarbeitern von Unternehmen in den für sie interessanten Branchen im Austausch für VPN-Fernzugriff eine hohe Summe zu zahlen.[116] Dieser Telegram-Kanal war auch die einzige öffentliche Plattform der Gruppe, auf der ihre Mitglieder zum Teil in Echtzeit über ihre Aktivitäten berichteten und die von mehr als 60'000 Zuschauern verfolgt wurde. Zusammenfassend lässt sich sagen, dass Lapsus$ zwar nicht sehr lange bestand, es aber in kurzer Zeit geschafft hat, mit bescheidenen Mitteln und wenig anspruchsvollen Techniken zahlreiche renommierte Unternehmen erfolgreich anzugreifen und Daten zu exfiltrieren.

115 LAPSUS$: Recent techniques, tactics and procedures (nccgroup.com)

116 Lapsus$ Ransomware Group Announced Recruitment of Insiders (securityaffairs.co)