11. Mai 2023 | Nationales Zentrum für Cybersicherheit NCSC

Halbjahresbericht 2022/II (Juli – Dezember)

Informationssicherung

Lage in der Schweiz und International

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

1 Übersicht / Inhalt

1 Übersicht / Inhalt 2
Management Summary 4
Editorial 5
2 Fokus: Cybersicherheit bei KMU 6
2.1 Digitalisierung schreitet voran 6
2.2 Kerngeschäft und unterstützende Werkzeuge 6
2.3 IT-Betrieb und Cybersicherheit 6
2.4 Auslagerung an externe Dienstleister 7
2.5 Prävention und Vorbereitung auf Vorfälle 7
3 Gastbeiträge: Erlebte Cyberangriffe 8
3.1 Cyberangriff bei den Verkehrsbetrieben Luzern 8
3.2 Ein Ransomwarevorfall aus Sicht der Polizei 9
4 Meldungen von Unternehmen und aus der Bevölkerung 10
4.1 Eingegangene Meldungen zu Cybervorfällen – Überblick 10
4.2 Am häufigsten gemeldet: Betrug 12
4.2.1 Drohmails von der Polizei in zahlreichen Varianten 12
4.2.2 Web-Administratoren im Fokus 13
4.2.3 Investitionsbetrug 14
4.3 Meldungen zu Phishing 14
4.3.1 Wie Phisher die Wahrscheinlichkeit ausnutzen 15
4.3.2 Immer professionelleres Office365-Phishing: Mitarbeitende im Visier 16
4.4 Meldungen zu Schadsoftware und Hacking 17
4.4.1 Ransomware auf gleichem Niveau 17
4.4.2 Meldungen zu Hacking weiterhin stark steigend 18
4.4.3 Gefälschte Erpressungen mit richtigen Angriffen 18
4.5 Diverse Meldungen 19
4.5.1 Die Ohnmacht bei Spoofing-Anrufen 19
5 Lage 19
5.1 Initialer Zugang 19
5.1.1 Nutzername / Passwort 20
5.1.2 Schadsoftware (Trojaner) 20
5.1.3 Ausnutzen von Schwachstellen 21
5.2 Schadsoftware / Malware 22
5.2.1 Schadsoftware-Verbreitung 22
5.2.2 Ransomware 23

5.3 Industrielle Kontrollsysteme (ICS) & operative Technologie (OT) 27
5.3.1 Sabotageversuche im Rahmen von Konflikten 27
5.3.2 Angespannte Energieversorgung im Fokus 28
5.4 Schwachstellen 29
5.4.1 Systeme mit öffentlich einsehbaren Konfigurationsdateien 29
5.4.2 ProxyNotShell 30
5.4.3 Retbleed 31
5.5 Datenabflüsse 31
5.5.1 Metadaten bei veröffentlichten Dateien 32
5.5.2 Entsorgung von IT-Mitteln und Datenträgern 32
5.6 Update Ukraine 33
5.6.1 Fortsetzung der Aktivitäten im Cyberraum ohne nennenswerte Erfolge 33
5.6.2 Unterschiedliche Cyberangriffe mit unterschiedlichen Folgen 34
5.6.3 Zukünftige Entwicklungen 35

Management Summary

Fokus: Cybersicherheit bei KMU

Die Digitalisierung schreitet auch in kleinen und mittleren Unternehmen voran. Zahlreiche Computer sind über Netzwerkschnittstellen miteinander verbunden. Prozesse wie Bestellungsabwicklung, Planung, Produktion und Logistik greifen immer mehr ineinander und werden digital gesteuert. Dadurch steigt die Anzahl Systeme, die aus dem Internet zugänglich sind und somit bestmöglich geschützt werden sollten. Doch oftmals wird gerade bei KMU der Cybersicherheit noch zu wenig Beachtung geschenkt. Aus diesem Grund wird im aktuellen Halbjahresbericht der Fokus auf die Cybersicherheit bei KMU gelegt und die wichtigsten Punkte zum Schutz vor Cyberbedrohungen aufgezeigt.

Am häufigsten gemeldet: Betrug

Im zweiten Halbjahr 2022 blieb der Meldeeingang beim NCSC sehr hoch und war mit 17'341 Meldungen praktisch identisch mit dem ersten Halbjahr 2022. Insgesamt erhielt das NCSC im vergangen Jahr 34'527 Meldungen. Davon stammen 85 Prozent aus der Bevölkerung und die restlichen 15 Prozent von Unternehmen, Vereinen und Behörden. Die Meldungen betreffen verschiedenste Betrugsformen. Dabei machen gefälschte Drohmails im Namen von Strafverfolgungsbehörden, sogenannte Fake-Extortion-E-Mails, fast einen Drittel der Meldungen aus. Weitere häufig gemeldete Betrugsformen sind CEO-Betrug sowie Rechnungsmanipulationsbetrug.

Ransomware auf gleichem Niveau

Die Meldungen zu Ransomware sind konstant geblieben und machen fast die Hälfte aller Meldungen in der Kategorie Schadsoftware aus. Etwa ein Drittel der 76 Meldungen betrifft Privatpersonen, zwei Drittel Unternehmen. Bei den Angriffen gegen Unternehmen ist besonders die Ransomware «Lockbit» aktiv. Diese Schadsoftware ist bekannt dafür, dass neben der Verschlüsselung die Daten auch gestohlen und ins Netz gestellt werden, falls die Lösegeldsumme nicht bezahlt wird. Solche Double-Extortions (Zweifach-Erpressungen) werden immer häufiger beobachtet. Weil viele Firmen die Bedrohung durch Ransomware erkannt haben und über Backups verfügen, ist die reine Verschlüsselung für die Angreifer mittlerweile nicht mehr lukrativ genug. Die initiale Infektion bei Ransomware-Vorfällen ist neben E-Mails mit schädlichen Anhängen oder Links häufig auf eine Schwachstelle oder eine schlechte Konfiguration zurückzuführen.

Meldungen zu Hacking weiterhin stark ansteigend

Im Vergleich zur Vorhalbjahresperiode haben sich die Meldungen bezüglich Hacking im zweiten Halbjahr mit 276 Meldungen nahezu verdoppelt. Insbesondere Social Media-Accounts sind bei Hackern ein beliebtes Ziel, um beispielsweise die Nutzerinnen und Nutzer zu erpressen oder die gehackten Accounts für das Vertreiben von Werbung für Investitions-Betrug zu verwenden.

Editorial

Oft werde ich gefragt: «Sind KMU weniger sicher als Grossunternehmen?». Um dies zu erörtern, stellt sich die Frage: Wie sieht denn ein typisches KMU aus? Ein marktwirtschaftliches Unternehmen gilt dann als KMU, wenn es weniger als 250 Arbeitskräfte beschäftigt. In diese Kategorie fallen in der Schweiz 99,7% aller Unternehmen. Die meisten Beschäftigten bei KMU finden sich in der Herstellung von Waren, dem Handel, der Instandhaltung und Reparatur von Motorfahrzeugen und dem Gesundheits- und Sozialwesen.

Alleine diese Fakten lassen es schon erahnen: Das typische KMU gibt es nicht. Es gibt also auch nicht «die» Cybersicherheit für KMU. Wie bei grossen Unternehmen auch, können die Rahmenbedingungen bei KMU, um sich vor Cyberangriffen zu schützen, ganz unterschiedlich sein. So trifft eine hochtechnisierte Unternehmung in der Pharmabranche ganz andere Voraussetzungen als ein regionales Handelsunternehmen. Erhebliche Faktoren sind dabei die zur Verfügung stehenden Finanzen, der Grad der Technologisierung der Unternehmung, das Geschäftsmodell, die Zusammensetzung der Belegschaft, Unternehmensstrukturen und -kultur und nicht zuletzt das wirtschaftliche und politische Umfeld.

Die Eingangs gestellte Frage lässt sich also gar nicht einfach so beantworten. Was dieser Halbjahresbericht mit dem Fokus KMU jedoch klar aufzeigt ist, dass KMU durchaus auch Ziele von Cyberangriffen sind. Dies können opportunistische Angriffe nach dem Giesskannenprinzip sein, oder gezielte Angriffe auf KMU mit zum Beispiel interessantem geistigem Eigentum.

Der vorliegende Halbjahresbericht soll gerade auch für KMU die Gefährdungslage aufzeigen und darlegen, wie man – je nach Beschaffenheit der Unternehmung – diese schützen kann. Als NCSC sehen wir es als unsere Aufgabe, Rahmenbedingungen zu schaffen, um die KMU in der Schweiz noch besser zu unterstützen, sich selber zu schützen. Nehmen Sie also unbedingt die Chance wahr, uns auch zu diesem Bericht Feedback zu geben und allfällige Ideen bezüglich KMU und Cyberrisiken mitzuteilen.

So unterschiedlich KMU auch sind, eines verbindet sie: Die oft kleine Anzahl Beschäftigte erlaubt keine riesigen Sicherheitsabteilungen. Cybersicherheit muss jedoch integral und geschäftsorientiert angegangen werden. Das bedeutet in letzter Konsequenz, dass sowohl die Unternehmensführung wie auch die Mitarbeitenden im Rahmen ihres Verantwortungsbereiches Cyberwissen brauchen. Gelingt es, dieses Wissen aufzubauen ohne an Wirtschaftskraft zu verlieren, könnten die KMU bald einen nicht unerheblichen Vorteil in einer zunehmend digitalen Wirtschaft haben. Damit wir diese Chance für das KMU-Land Schweiz realisieren können, braucht es jedoch die Zusammenarbeit von Behörden, Wirtschaft, Wissenschaft und Gesellschaft. Gehen wir es also gemeinsam an!

Florian Schütz, Delegierter des Bundes für Cybersicherheit

2 Fokus: Cybersicherheit bei KMU

2.1 Digitalisierung schreitet voran

Kaum jemand kann sich der Digitalisierung entziehen. Ein Leben ohne Internet ist für viele Menschen nicht mehr vorstellbar. Computer haben mittlerweile in fast allen Bereichen von Wirtschaft und Gesellschaft Einzug gehalten, zumindest für Kommunikation und Administration. Aber auch die Produktion kommt vielfach nicht mehr ohne Computer aus. Viele dieser Geräte sind durch Netzwerkschnittstellen untereinander und auch mit den administrativen Büronetzwerken in der einen oder anderen Form verbunden. Bestellungen, Planung, Produktion, Logistik und Abrechnung greifen in teil- oder vollautomatisierten Prozessen immer mehr ineinander.

Empfehlungen:

Digitalisieren Sie umsichtig: Beachten Sie nicht nur Chancen und Vorteile sondern auch neue Abhängigkeiten und Risiken. Planen Sie Cybersicherheit von Anfang an bei jedem Digitalisierungsschritt mit ein.

2.2 Kerngeschäft und unterstützende Werkzeuge

Für Unternehmen, die ausschliesslich digitale Dienste anbieten, sollte Cybersicherheit eine Selbstverständlichkeit sein – schliesslich können sie nur arbeiten, wenn ihre Systeme ordnungsgemäss funktionieren. Bei den meisten Unternehmen wird IT jedoch vornehmlich unterstützend eingesetzt. Die Priorität liegt auf dem Kerngeschäft, sei dies das Herstellen von Produkten oder das Erbringen von Dienstleistungen. Solange die IT funktioniert, wird ihr wenig Aufmerksamkeit geschenkt, und wenn sich etwas nicht wie gewünscht verhält, kann man häufig noch darum herum organisieren. Dennoch können insbesondere Totalausfälle massive Konsequenzen nach sich ziehen: Wenn Planungen und Abrechnungen nicht mehr verarbeitet werden können, ist auch hier mit Arbeitsausfällen und Verzögerungen zu rechnen, die sich gegebenenfalls in der Bilanz niederschlagen. Auf der anderen Seite können auch Diebstahl von geistigem Eigentum (Wirtschaftsspionage) oder eine falsch ausgelöste Zahlung grosse finanzielle Schäden anrichten.

Schlussfolgerung / Empfehlung:

Informatikmittel sind Arbeitswerkzeuge, die unterhalten und gepflegt werden müssen. Lassen Sie sich durch Fachpersonen beraten und unterstützen. Die vom Bundesamt für wirtschaftliche Landesversorgung (BWL) in Zusammenarbeit mit der Wirtschaft erarbeiteten IKT-Minimalstandards und IKT-Branchenstandards dienen als Empfehlungen und Orientierungspunkte.

2.3 IT-Betrieb und Cybersicherheit

Der Betrieb der Firmen-IT beinhaltet in KMU häufig auch die Zuständigkeit für Cybersicherheit. Vielfach wird dies im Nebenamt gemacht. Da aber nur schon der Unterhalt der IT aufwendig ist, besteht die Gefahr, dass die Cybersicherheit dabei vernachlässigt wird. Typischerweise

können sich Unternehmen erst ab einer gewissen Grösse Cybersicherheit als eigenständige Funktion leisten. Während bei der IT klare Anforderungen an die Funktionalitäten gesetzt werden und diese auch messbar sind, gehört die Cybersicherheit zum Risikomanagement und muss in diesem Rahmen von der Geschäftsleitung gesteuert werden. Es empfiehlt sich insbesondere, die Cybersicherheit als eigenständigen Budgetposten zu behandeln, damit Ressourcen explizit für entsprechende Massnahmen zur Verfügung stehen.

Schlussfolgerung / Empfehlung:

Betrieb und Sicherheit von IT-Infrastruktur hängen zwar zusammen, sind jedoch verschiedene Handlungsfelder. Die Zuweisung von Ressourcen an Cybersicherheitsmassnahmen muss im Rahmen des Risikomanagements entschieden werden.

2.4 Auslagerung an externe Dienstleister

In jedem Büro stehen Computer. Doch nicht alle Unternehmen haben ein eigenes Firmennetzwerk. Wenn Arbeiten dennoch über mehrere Geräte hinweg ausgeführt werden müssen, bietet sich heutzutage die Auslagerung von Datenhaltung und auch der Betrieb von Programmen in der Cloud an. Eine solche Auslagerung kann natürlich auch zur Entlastung des Firmennetzwerks oder zur Flexibilitätssteigerung sinnvoll sein. Nicht zuletzt dürften Cloud-Dienstleister auch bezüglich Cybersicherheit gute Kenntnisse haben, sind sie doch spezialisierte IT-Dienstleister. Eine weitere Möglichkeit besteht darin, einen externen Cybersicherheitsdienstleister zu engagieren, der sich spezifisch um Sicherheitsbelange kümmert.

Schlussfolgerungen / Empfehlungen:

Bei Verträgen mit externen Dienstleistern gilt es zu beachten, dass auch die Sicherheit angemessen geregelt wird. Neben allfälligen spezifischen Massnahmen zum Schutz vor und der Abwehr von Cyberangriffen (z. B. DDoS, Datenabfluss und Ransomware) sollten auch Datensicherung (Backups) und Meldepflichten bei Vorfällen thematisiert werden.

2.5 Prävention und Vorbereitung auf Vorfälle

Neben technischen Schutzmassnahmen ist die Schulung von Mitarbeiterinnen und Mitarbeitern bezüglich Cyberrisiken eine wichtige Massnahme, denn sie sind ein wichtiges Glied in der Abwehrkette. Auch wenn das zuverlässige, eigenständige Erkennen von bösartigen E-Mails durch die Mitarbeitenden nicht garantiert werden kann, hilft bereits die Sensibilisierung auf die Gefahr. Wenn Empfängerinnen und Empfänger bei Verdacht oder Unsicherheiten bezüglich einem E-Mail nicht direkt die in der Nachricht aufgeführte Handlungsanweisung ausführen, respektive nicht auf den Link klicken oder die angehängte Datei öffnen, sondern das E-Mail intern überprüfen oder beim (vermeintlichen) Absender die Echtheit der Nachricht bestätigen lassen, wird das Risiko für einen erfolgreichen Angriff reduziert.

Auch bei bester Prävention und Sensibilisierung kann nie ausgeschlossen werden, dass etwas passiert. Um auf solche Eventualitäten vorbereitet zu sein, sollten im Unternehmen Pläne für den Ernstfall erstellt werden: Prozesse und Eskalationspfade sind zu definieren und zu testen.

Vorgängige Überlegungen zur Krisenkommunikation, gegen intern wie extern, nehmen im Ereignisfall Druck weg, helfen Fehler zu vermeiden und unterstützen damit bei der erfolgreichen Bewältigung eines Angriffs. Ebenfalls empfehlenswert ist es, Kontakte zu möglichen Dienstleistern zu etablieren, die bei einem Vorfall unterstützen könnten (Incident Response), damit man diese im Ernstfall nicht erst suchen muss.

Schlussfolgerungen / Empfehlungen:

Cybersicherheit ist kein Zustand, der erreicht werden kann. Sie ist vielmehr ein Prozess, der aus technischen, organisatorischen und personellen Massnahmen besteht und gepflegt werden muss.[1] Die Schulung von Mitarbeitenden ist dabei ein zentraler Punkt.

Auch wenn intensiv in die Prävention investiert wird, kann nie ganz ausgeschlossen werden, dass sich ein Cybervorfall ereignet. Neben Plänen für die Vorfallsbewältigung sollten auch im Vorfeld Überlegungen zu entsprechender interner wie externer Kommunikation gemacht werden.[2]

3 Gastbeiträge: Erlebte Cyberangriffe

3.1 Cyberangriff bei den Verkehrsbetrieben Luzern

Beitrag von Franz Theiler, Leiter Informatik VBL AG

In der Nacht auf Samstag, 14. Mai 2022, wurden die Verkehrsbetriebe Luzern Opfer eines gezielten Cyberangriffs. Mitarbeitende der Leitstelle informierten früh morgens das IT-Pikett infolge einer Störung. Die IT-Abteilung konnte schnell das Ausmass erkennen und als einen ausserordentlichen Vorfall einstufen. Daraufhin wurden die IT-Systeme offline genommen und das IT-Netzwerk der VBL vom Internet getrennt.

Über den Leiter Notfall und Krisenmanagement (NKM) wurde der Notfallstab einberufen. Aufgrund der inzwischen erhärteten Fakten wurde die Luzerner Polizei informiert sowie der Vorfall dem Nationalen Zentrum für Cybersicherheit (NCSC) gemeldet. Die wichtigsten Stakeholder wie Behörden, Transport- und Branchenunternehmen, Mitarbeitende sowie die Medien wurden noch am selben Morgen vom NKM und der Geschäftsleitung über den erfolgten Cyberangriff informiert.

Bereits am Samstagmittag hatten sich das IT-Team der VBL und weitere Mitarbeitende ihres externen IT-Dienstleisters zur Abstimmung und Aufnahme der Arbeiten in den Räumlichkeiten der VBL eingefunden. Die VBL-Informatik betreibt betriebskritische und hochverfügbare öV-Systeme für interne sowie auch externe Kunden in der ganzen Schweiz. Sie weist eine sehr anspruchsvolle IT-Systemlandschaft in einem Windows- und Linux-Umfeld auf. Unmittelbar wurde mit der Eindämmung und Analyse der Krise begonnen. Die Schadsoftware konnte eruiert und beseitigt werden. Nötige Grundsysteme wurden neu aufgebaut und isoliert. Die Sys-

1 Schützen Sie Ihr KMU (ncsc.admin.ch)
2 Vorfall - Was nun? (ncsc.admin.ch)

teme konnten vom letzten Backup wieder schrittweise hergestellt, geprüft und mit einem kontrollierten und bewährten Prozess in den produktiven Betrieb überführt werden. Das perfekte Zusammenspiel zwischen Mitarbeitenden, Lieferanten und spezialisierten Experten konnten die schnelle Eindämmung der Krise und das erfolgreiche Recovery erst ermöglichen. Für die Forensik stand die Luzerner Polizei kompetent zur Seite. Im Rahmen des Wiederaufbaus wurde punktuell die Sicherheit durch gezielte Massnahmen erhöht.

Die Fahrgäste waren vom Cyberangriff nicht betroffen. Einzig die Abfahrtsmonitore wurden aus Sicherheitsgründen abgeschaltet. Rückblickend war die Unternehmung auf die Krisensituation gut vorbereitet. Die Geschäftsbereiche waren stets in der Lage den Betrieb in einer gut organisierten, aber eingeschränkten Form aufrechtzuerhalten. Über einige Wochen traf sich das interne Notfall- und Krisenmanagement täglich inklusive eines Abgleiches im Anschluss mit der Geschäftsleitung. Die GL nahm im Besonderen die Brückenfunktion in die Fachabteilungen wahr.

Das NCSC unterstützte die VBL in der schwierigen Situation zeit- und kundennah. Die Informationen gaben der VBL wertvolle Aufschlüsse und Sicherheit hinsichtlich Täterschaft und mögliche Vorgehensmuster. Auch danken wir dem NCSC für die beiden eindrucksvollen Vorträge anlässlich der Kader- und Personalinfo, bei welchen das NCSC die VBL-Mitarbeitenden mit viel Herzblut und Leidenschaft rund um Cyberattacken sensibilisieren konnte. VBL ist ein öV-Betreiber mit kritischen Infrastrukturen und kann daher an den vom NCSC organisierten Austauschmeetings partizipieren und profitiert von den regelmässigen Neuigkeiten im Bereich der Security.

3.2 Ein Ransomwarevorfall aus Sicht der Polizei

Beitrag vom Dezernat Digitale Kriminalität, Kantonspolizei Bern

Ein Ransomware-Angriff beinhaltet die Verschlüsselung von Daten und eine Lösegeldforderung, die in aller Regel in Kryptowährung verlangt wird. Der Angriff ist automatisiert und wird von einer organisierten Tätergruppierung initiiert. Geht das geschädigte Unternehmen nicht auf die Lösegeldforderung ein, wird damit gedroht, sensible Kundeninformationen im Darkweb bekanntzugeben bzw. sie dort zu verkaufen. Somit erfolgt direkt auch ein Angriff auf die Reputation des Unternehmens.

In einem aktuellen Fall wurde der Angriff vom betroffenen Unternehmen über die Telefonzentrale der Polizei gemeldet und an das zuständige Dezernat Digitale Kriminalität übermittelt. Dieses bestimmte nachfolgend die verantwortlichen Ermittelnden und zog Spezialistinnen und Spezialisten des Fachbereichs Digitale Forensik bei, mit denen die ersten Massnahmen geplant wurden. Ein Ransomware-Fall bedingt immer interdisziplinäre Zusammenarbeit von verschiedenen Akteurinnen und Akteuren und wie auch im aktuellen Fall, ist der Austausch mit dem betroffenen Unternehmen wichtig, um die notwendigen Informationen zu erheben und daraus Handlungsanweisungen abzuleiten. Eine gute Kooperation ist in vielen Aspekten ausschlaggebend. Denn bei einem Ransomware-Fall stehen für das Unternehmen nicht die Erhebungen und Ermittlungen im Vordergrund, sondern die Rekonstruktion der Daten und die Wiederaufnahme der Geschäftstätigkeit.

Im vorliegenden Fall wurde schon sehr früh neben der Polizei ein privater Sicherheitsdienstleister beigezogen, um zu helfen, die Infrastruktur wieder aufzubauen. Die Zusammenarbeit

mit diesem war gut; meistens hängt dies aber vom Unternehmen ab, wie viel sie zu den Ermittlungen beisteuern möchten und welche Priorität diese haben.

Da ein Ransomware-Angriff technisch anspruchsvoll ist, folgen Gespräche und Sitzungen, um den Schwachstellen nachzugehen, die überhaupt ein unbefugtes Eindringen ermöglichten.

Neben den Ermittlungen hat das betroffene Unternehmen eine Beratung über das weitere Vorgehen und vor allem rechtliche Auskünfte von uns erwartet, denn ein solcher Angriff kann weitere geschädigte Parteien zum Vorschein bringen und sensible Daten tangieren.

Generell hat das Unternehmen im vorliegenden Fall vorbildlich reagiert, indem der Vorfall so schnell wie möglich polizeilich gemeldet und ein Sicherheitsdienstleister beigezogen wurde, was einen reibungslosen Ablauf zwischen den Spezialistinnen und Spezialisten vom Dezernat Digitale Kriminalität und dem Fachbereich Digitale Forensik ermöglicht hat. Wir raten in jedem Fall davon ab, eine Lösegeldzahlung in Betracht zu ziehen, da das die organisierte Kriminalität mitfinanziert. Die Bereitschaft zu einer Zahlung hängt oftmals vom Grad der verschlüsselten Daten und von der Wahrscheinlichkeit ab, diese wieder herstellen zu können, aber auch von der Höhe der Lösegeldforderung. Das Unternehmen hat auch hier vorbildlich gehandelt und zu keinem Zeitpunkt in Betracht gezogen, das Lösegeld zu bezahlen. Um zu vermeiden, in eine ähnliche Situation zu geraten, ist es ratsam, Mitarbeitende auf Risiken im digitalen Raum zu sensibilisieren und in Schulungen, aber auch in eine sichere Infrastruktur zu investieren. Die betroffene Firma konnte nach kurzer Zeit ihre Geschäftstätigkeit wieder aufnehmen, die vollständige Bewältigung des Vorfalles dauerte jedoch einige Wochen.

4 Meldungen von Unternehmen und aus der Bevölkerung

4.1 Eingegangene Meldungen zu Cybervorfällen – Überblick

Auch in diesem Jahr erhöhte sich die Gesamtzahl der Meldungen deutlich. Mit insgesamt 34’527 Meldungen fand im Vergleich zum Vorjahr mit 21’714 Meldungen zwar keine Verdoppelung mehr statt, die Zunahme in absoluten Zahlen ist mit 12’813 Meldungen aber immer noch deutlich höher als im letzten Jahr (Zunahme 2020/21 +10’881). Dies ist einerseits der steigenden Bekanntheit des NCSC und seinem Meldeformular zuzuschreiben. Andererseits hat die erneute Zunahme auch andere Ursachen und ist vor allem auf die Zunahme bei den Meldungen in den Phänomenen «Gefälschte Drohmails der Polizei» (siehe Kapitel 4.2.1) und «Spoofing von Telefonnummern» (siehe Kapitel 4.5.1) zurückzuführen. Dass im zweiten Halbjahr 2022 mit insgesamt 17’341 Meldungen praktisch gleich viele Meldungen wie im ersten Halbjahr eingegangen sind, deutet aber darauf hin, dass zukünftig der Meldeeingang nicht mehr in dem Umfang wie in den letzten drei Jahren steigen wird.

85% der Meldungen stammen aus der Bevölkerung, die restlichen Meldungen teilen sich in Meldungen von Unternehmen, Vereinen und Behörden auf. Typische Phänomene, welche von Unternehmen gemeldet werden, sind CEO-Betrug (190 Meldungen im zweiten Halbjahr 2022), Rechnungsmanipulationsbetrug (45 Meldungen), Angriffe mit Verschlüsselungsschadsoftware (54 Meldungen) und Angriffe auf die Verfügbarkeit (DDoS) (13 Meldungen). Zudem werden sogenannte Fake-Erpressungsversuche (Fake Extortion) nicht nur gegen Privatpersonen beobachtet. Es existieren ebenfalls Varianten, die sich direkt gegen Firmen richten, wie die Fake-Extortion-Versuche gegen Web-Administratoren in Kapitel 4.4.2 exemplarisch zeigen. Auch Phishing-Versuche zielen längst nicht mehr nur auf Privatpersonen, immer häufiger werden

auch Firmenmitarbeitende gezielt angegriffen. Dabei stehen vor allem Office-365-Zugangsdaten im Fokus, wie Kapitel 4.3.2 zeigt.

Meldungen an das NCSC im zweiten Halbjahr 2022 (pro Woche)

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

Meldungen an das NCSC im zweiten Halbjahr 2022 (nach Kategorie)

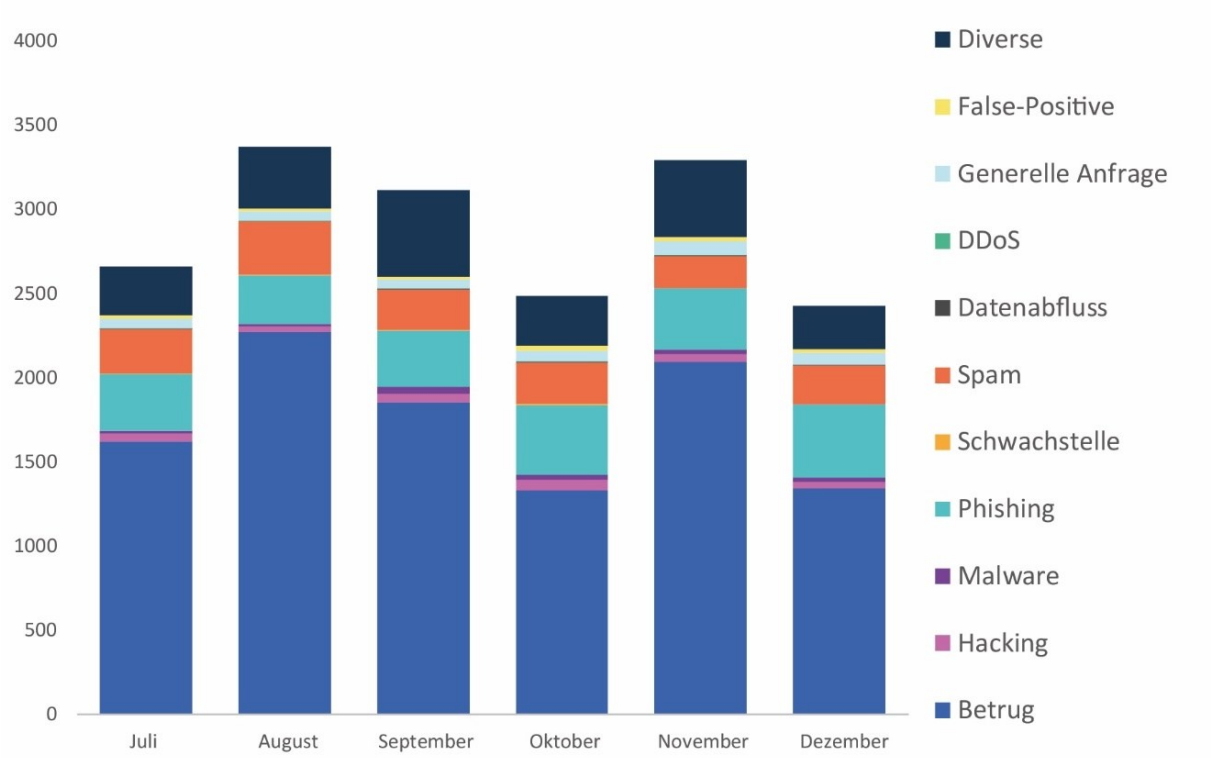

Abb. 2: Meldungen an das NCSC im zweiten Halbjahr 2022 nach Kategorien, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

4.2 Am häufigsten gemeldet: Betrug

4.2.1 Drohmails von der Polizei in zahlreichen Varianten

Auch im zweiten Halbjahr 2022 gehörten mit 5’179 Meldungen die gefälschten Drohmails, die vermeintlich von Strafverfolgungsbehörden verschickt wurden, zum Phänomen mit dem höchsten Meldeeingang. So erstaunt es wenig, dass auch für die Rekordwoche 36, in der mit 954 Meldungen der höchste Eingang im Jahr 2022 verzeichnet wurde, die angeblichen Drohmails der Polizei mit insgesamt 418 Meldungen den grössten Anteil ausmachten. In diesen Drohmails wird behauptet, 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. Insgesamt fielen im Jahr 2022 über 11’051 Meldungen in diese Kategorie, davon 5’179 Meldungen im zweiten Halbjahr. Dies entspricht etwa einem Drittel des Gesamtmeldeeingangs.

Abb. 3: Verschiedene Varianten von haltlosen Drohmails im Namen von Strafverfolgungsbehörden mit zusammengewürfelten Absendern und Logos. Unten rechts missbrauchen die Betrüger den Namen des NCSC, allerdings mit dem falschen Logo.

Um den Erpresserschreiben einen offiziellen Anstrich zu verleihen, werden von den Betrügern die Namen und Logos von verschiedensten Strafverfolgungsbehörden aus dem In- und Ausland mehr oder weniger zufällig zusammengesetzt. Als Absender verwendet wurden im zweiten Halbjahr 2022 beispielsweise die Namen von Kantonspolizeibehörden der Kantone Wallis, Waadt und Genf. International werden unter anderem die Namen von Europol und Interpol, sowie der Polizei in Frankreich, Belgien oder den Niederlanden verwendet. Auch das NCSC blieb nicht verschont und wurde als Absender dieser Erpresserschreiben missbraucht. Allerdings vergriffen sich die Angreifer beim Logo und verwendeten das Logo der gleichnamigen britischen Cybersicherheitsbehörde. Nach wie vor die häufigste Variante bleiben die E-Mails, die vorgeben, vom Bundesamt für Polizei (Fedpol) zu stammen. Die angehängten Dokumente geben dabei vor, dass sie von dessen Direktorin, Nicoletta della Valle, oder von der ehemaligen Vorsteherin des Eidgenössischen Justiz und Polizeidepartementes (EJPD), Bundesrätin Karin Keller-Sutter, unterschrieben sind.

4.2.2 Web-Administratoren im Fokus

Fake-Erpressungen wurden im zweiten Halbjahr 2022 auch gegen Web-Administratoren beobachtet. Insgesamt 114 Meldungen gingen beim NCSC zu dieser Betrugsart ein. Im Erpresserschreiben, das meist über das Kontaktformular auf der Website abgesetzt wird – jedoch auch per E-Mail eingehen kann – wird behauptet, dass die Website gehackt und dahinterliegende Datenbanken gestohlen worden seien. Schliesslich wird mit der Veröffentlichung dieser Daten gedroht. Die Forderungen haben alle einen ähnlichen Wortlaut und sind ähnlich aufgebaut, wie die sogenannten Fake-Sextortion-E-Mails. Typisch an diesen Erpressungen ist die Verwendung gleicher Bitcoin-Adressen in den E-Mails, die an die Firmen versendet werden. Wenn jemand also einzahlen würde, wäre es den Erpressern gar nicht möglich herauszufinden, welches Opfer das Lösegeld bezahlt hat. Es handelt sich um einen klassischen Bluff.

Eine Untervariante dieser Betrugsart wurde in der Berichtsperiode zum ersten Mal beobachtet: Sicherheitsverantwortliche wurden von angeblichen Forschern kontaktiert und auf vermeintliche Schwachstellen ihrer Systeme hingewiesen. Das E-Mail schloss jeweils mit den Worten, dass im Rahmen des «Responsible Disclosure»-Prozesses für Schwachstellen eine entsprechende Belohnung erwartet werde. Bei den Hinweisen handelte es sich aber nicht um eine eigentliche Sicherheitslücke, sondern es wurde lediglich darauf hingewiesen, dass auf der Unternehmens-Website die Funktion «HTTP Strict Transport Security (HSTS)»[3] nicht aktiviert sei. Auch wenn es sehr empfehlenswert ist, HSTS zu implementieren, kann ihr Fehlen kaum als klassische Sicherheitslücke bezeichnet werden. Im Internet gibt es zahlreiche Seiten, mit denen auch Personen ohne spezielle IT-Kenntnisse Webseiten auf die gängigen Sicherheitsmerkmale hin überprüfen können. Die Betrüger nutzen diese Seiten und die Unsicherheit von Web-Administratoren aus und hoffen, so an eine Belohnung zu kommen.

[3] Ist HSTS für eine Website aktiviert, wird ein zusätzlicher Header im HTTPS-Protokoll verwendet, der den Browser strikt anweist, ab dem ersten Aufruf ausschliesslich die Verschlüsselung zu benutzen.

Hi Team,I am a security researcher and found a vulnerability on your website.

Vulnerability : Non - secure requests are not automatically upgraded to HTTPS | HSTS missing

I am hoping to receive a reward for the responsible disclosure of vulnerability.

Looking forward to hearing from you soon.
Kind Regards,

Abb. 4: E-Mail betreffend eine angebliche Sicherheitslücke des Web-Servers und die Frage nach einer Belohnung

4.2.3 Investitionsbetrug

Investitionsbetrug gehört mit 219 Meldungen und einer Schadensumme von über 4 Millionen Franken auch im zweiten Halbjahr 2022 zu den ans NCSC gemeldeten Phänomenen mit dem grössten finanziellen Schaden. Es handelt sich bei diesem Betrag lediglich um die von den Meldenden mitgeteilten Beträge. Da nicht alle Fälle dem NCSC zur Kenntnis gebracht werden und von einer erheblichen Dunkelziffer ausgegangen werden muss, dürfte die reale Schadenssumme weit höher liegen. Mit verschiedenen Maschen werden die Opfer dabei verleitet, ihr Geld auf dubiosen Seiten zu investieren. Die bekannteste Masche ist über fiktive Werbeversprechen, in denen bekannte Persönlichkeiten erzählen, wie man schnell an das grosse Geld kommt. Während vor ein paar Jahren gefälschte Interviews mit Roger Federer kursierten, folgten dann fiktive Werbeseiten, welche Bezug auf die Fernsehsendung «Höhle der Löwen» nahmen. Mittlerweile werden auch die Namen von Bundesrätinnen und Bundesräten regelmässig für solche Werbung missbraucht. Insgesamt 469 Mal erhielt das NCSC im zweiten Halbjahr Meldungen zu betrügerischer Werbung, die verspricht, schnell an das grosse Geld zu kommen. Im Vergleich zur Vorhalbjahresperiode mit 619 Meldungen haben diese Meldungen jedoch leicht abgenommen. Obschon das NCSC auch Meldungen von Opfern erhält, welche auf solche Werbung hereingefallen sind, dürfte die Erfolgsrate solch betrügerischer Werbung gering sein. Die Angreifer suchen sich deshalb vermehrt andere Tricks, um Opfer zu überzeugen, ihr Geld zu investieren. Eine häufig beobachtete Methode geht über unverfängliche Kontaktaufnahmen auf Social-Media oder Partnervermittlungsseiten. Die Betrüger investieren dabei viel Zeit, um das Vertrauen des Opfers zu erlangen und es dann in einem zweiten Schritt zu einer vermeintlich lukrativen Investition zu überreden. Dabei behaupten die Betrüger, eigene Erfahrungen gemacht zu haben und durch diese Investitionen reich geworden zu sein.

4.3 Meldungen zu Phishing

Im zweiten Halbjahr 2022 erhielt das NCSC über sein Meldeportal insgesamt 2'177 Meldungen zu Phishing. Die Meldungen haben dabei im Vergleich mit der Vorhalbjahresperiode leicht abgenommen. Damals gingen 2’544 Meldungen ein. Es dominieren immer noch Phishing-E-Mails, welche auf Kreditkartendaten abzielen. Allerdings haben es die Angreifer auch häufig auf andere Daten, wie beispielsweise E-Mail-Logins abgesehen. Gerade E-Mail-Konten von Firmen haben für die Angreifer einen grossen Wert, wie in Kapitel 4.3.2 beschrieben wird. Doch auch E-Mail-Konten von Privatpersonen sind für die Angreifer wertvoll. Das E-Mail-Konto ist mittlerweile Dreh- und Angelpunkt von sämtlichen Internetshops und -dienstleistungen. Hat man das Passwort eines Internetdienstleisters vergessen, kann man dies über das E-Mail-

Konto in den meisten Fällen zurücksetzen. Das heisst, dass die Angreifer Zugriff auf zahlreiche Konten erhalten können, wenn sie im Besitz des E-Mail-Passworts sind. Werden auf diese Weise Webshop-Konten gehackt, lassen sich Waren und Dienstleistungen erschleichen. Betrüger benutzen aber gehackte E-Mail- und Social-Media-Konten mittlerweile auch, um ihren Fake-Erpressungen Nachdruck zu verleihen (siehe Kapitel 4.4.2).

Anzahl Phishing-Sites pro Woche

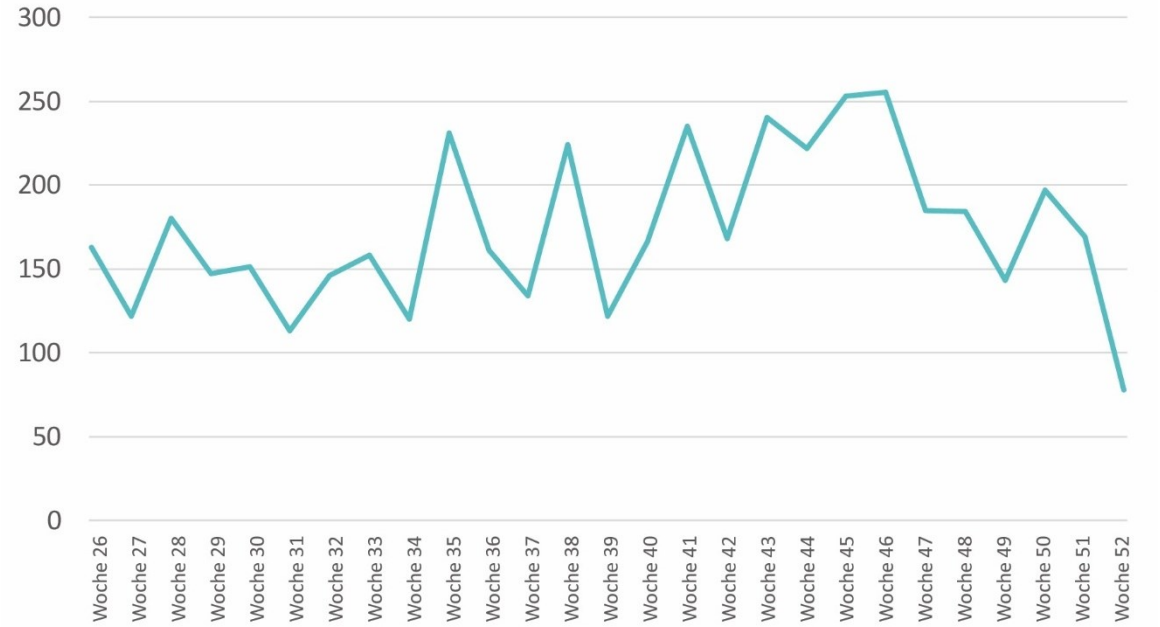

Abb. 5: Anzahl durch das NCSC überprüfte und bestätigte Phishing-URLs pro Woche im zweiten Halbjahr 2022. Aktuelle Daten finden Sie unter: https://www.govcert.admin.ch/statistics/phishing/

4.3.1 Wie Phisher die Wahrscheinlichkeit ausnutzen

E-Mails mit angeblich doppelt bezahlten Swisscom- oder Sunrise-Rechnungen, SMS mit angeblichen Ticket-Rückerstattungen der Schweizerischen Bundesbahnen AG (SBB) oder fiktive Paketzustellungen: All diesen Nachrichten ist gemein, dass die Wahrscheinlichkeit relativ hoch ist, dass die von den Angreifern erfundene Geschichte dem Opfer plausibel erscheint. So warten viele tatsächlich auf ein Paket, haben Lastschriftverfahren bei Sunrise oder Swisscom, oder haben bei den SBB tatsächlich einen Erstattungsantrag gestellt. Die Angreifer nutzen in diesen Fällen die Wahrscheinlichkeitsrechnung zu ihren Gunsten und nehmen Vorgänge, die von Bürgerinnen und Bürgern häufig durchgeführt werden, als Vorlage für ihre Geschichte. Klassisches Beispiel sind die falschen Benachrichtigungen der diversen Paketdienstleister, die das Opfer verleiten, eine Seite zu öffnen, auf der dann Kreditkartendaten eingegeben werden sollen. Mit 532 Meldungen gehen fast ein Viertel aller Phishing-Meldungen auf das Konto von falschen Paketbenachrichtigungen. Seit der Corona-Pandemie haben die Online-Bestellungen stark zugenommen. Die Wahrscheinlichkeit, dass jemand tatsächlich auf ein Paket wartet, ist gross. Angenommen 10% der Bevölkerung machen pro Woche eine Online-Bestellung, dann passt die Geschichte bei 10’000 Personen, wenn die Angreifer pro Woche 100’000 E-Mails versenden. Auch bei den Phishing-Versuchen unter dem Vorwand doppelt bezahlter Telekom-Rechnungen nutzen die Angreifer die Wahrscheinlichkeit. Wenn angeblich doppelt bezahlte Swisscom-Rechnungen an «bluewin.ch»-Adressen, respektive doppelt bezahlte Sunrise-Rechnungen an «sunrise.ch»-Adressen gesendet werden, ist die Wahrscheinlichkeit gross,

dass die erfundene Story passen könnte und die Empfänger auf den Phishing-Versuch hereinfallen. Am Ende des Jahres 2022 haben sich die Angreifer auf angebliche Rückerstattungen der SBB konzentriert. Auch hier scheint die Geschichte in vielen Fällen zu passen, wie zahlreiche Rückmeldungen von Melderinnen und Meldern zeigen, die tatsächlich auf eine Rückerstattung bei den SBB warteten.

Abb. 6: Phishing-Versuch mit angeblicher Rückerstattung eines SBB-Tickets

4.3.2 Immer professionelleres Office-365-Phishing: Mitarbeitende im Visier

Office-365-Zugangsdaten sind für Angreifer besonders interessant, da solche Konten als Ausgangspunkt für weitere Angriffe, wie beispielsweise den Rechnungsmanipulationsbetrug, missbraucht werden können. Mit 45 Meldungen und einem beim NCSC gemeldeten Schaden von fast einer halben Million Franken in der Berichtsperiode gehört dieser Betrugstyp zu den Phänomenen mit einem hohen Schadenspotential. Auch hier ist von einer erheblichen Dunkelziffer auszugehen. Dabei werden die gehackten Konten nach gestellten Rechnungen durchforstet. Die Betrüger ändern dann die IBAN-Nummer auf der Rechnung zu ihren Gunsten. Anschliessend wird die Rechnung unter einem Vorwand noch einmal an den Auftragnehmer gesendet mit der Bitte, die neue IBAN zu verwenden. Mit dem Zugriff auf Office-365-Firmen-Konten erhalten die Angreifer aber auch Daten zu Firmeninterna, die für Social-Engineering-Angriffe gegen andere Mitarbeitende verwendet können oder mit denen sich die Firma erpressen lässt. Oft erstellen die Angreifer auch eine E-Mail-Weiterleitungsregel, die eine Kopie aller empfangenen E-Mails des Opfers an die Angreifer sendet. Wenn das Opfer bemerkt, dass es gephisht worden ist und die Zugangsdaten geändert werden, erhalten die Angreifer so weiterhin alle E-Mails. Daher ist es nicht verwunderlich, dass Phisher alle Register ziehen, um an die Zugangsdaten der Mitarbeitenden zu gelangen. Die Versuche werden immer professioneller und demnach auch schwieriger zu erkennen. Mitarbeitende sollten deshalb regelmässig geschult werden und es ist ratsam, wenn immer möglich, eine Zwei-Faktor-Authentifizierung zu implementieren. Dies bietet eine zusätzliche Schutzebene, um zu verhindern, dass Office-365-Konten gehackt werden.

Abb. 7: Angeblicher Projektvorschlag, der von einem Server heruntergeladen werden soll. Im Hintergrund wird ein Dokument verschwommen angezeigt. Um dieses zu öffnen, müsse allerdings zuerst das Office-365-Passwort eingegeben werden.

4.4 Meldungen zu Schadsoftware und Hacking

4.4.1 Ransomware auf gleichem Niveau

Im zweiten Halbjahr 2022 wurden insgesamt 155 Meldungen im Zusammenhang mit Schadsoftware registriert. Im Vergleich zur Vorhalbjahresperiode ist dies ein starker Rückgang. In der Vorhalbjahresperiode war der Meldeeingang mit 592 fast viermal so hoch. Grund dafür ist das Ausbleiben grosser Wellen. So gingen vor einem Jahr allein 405 Meldungen auf das Konto der Schadsoftware «Flubot». In der aktuellen Berichtsperiode wurde kein einziger «Flubot»-Fall mehr gemeldet.

Konstant geblieben sind die Meldungen zu Ransomware. Mit 76 Meldungen machen sie fast die Hälfte aller Meldungen in der Kategorie Schadsoftware aus. Etwa ein Drittel der Meldungen betreffen Privatpersonen, zwei Drittel Unternehmen. Bei den Angriffen gegen Unternehmen ist besonders die Ransomware «Lockbit» aktiv. Gerade diese Schadsoftware ist bekannt dafür, dass neben der Verschlüsselung die Daten auch gestohlen und ins Netz gestellt werden, falls die Lösegeldsumme nicht bezahlt wird. Solche Double-Extortion (Zweifach-Erpressungen) werden immer häufiger beobachtet. Dieser Trend wird sich vermutlich auch 2023 fortsetzen. Viele Firmen haben die Bedrohung durch Ransomware erkannt und mit einer angepassten Backup-Strategie reagiert. Die reine Verschlüsselung ist deshalb für die Angreifer mittlerweile nicht mehr lukrativ genug. Mit der Androhung, die Daten zu veröffentlichen, versuchen die

Angreifer, an Lösegeld zu kommen. Weitere gemeldete Ransomware-Familien, die sich im letzten Halbjahr gegen Firmen gerichtet haben, sind «Play», «Medusalocker», «Blackcat», «Magniber» und «Makop». Der Infektionsvektor ist in den meisten Fällen zur Zeit der Meldung noch nicht bekannt. Meist ist die initiale Infektion aber auf eine Schwachstelle oder eine schlechte Konfiguration zurückzuführen. Dies geht auch aus einer Studie von Microsoft hervor, wonach die Ursache für 80% der Ransomware-Angriffe in allgemeinen Konfigurationsfehlern bei Software und Geräten liegt.[4] Mit einem zeitnahen Patch-Management, einer regelmässigen Überprüfung der Systemkonfiguration, sowie dem konsequenten Verwenden von Zwei-Faktor-Authentifizierung für den Zugriff, kann das Risiko eines Ransomware-Angriffs effizient gesenkt werden.

Bei den Angriffen gegen Privatpersonen stehen weiterhin vor allem Netzspeichergeräte (NAS) im Visier der Angreifer. Mit siben Meldungen fällt hier vor allem die Schadsoftware «Deadbolt» auf. Geräte, die direkt vom Internet her erreichbar sind, sind besonders exponiert. Es wird systematisch nach Schwachstellen gescannt oder nach schlechten Konfigurationen z. B. schwachen Passwörtern gesucht. Es ist deshalb besonders wichtig, diese Systeme immer auf dem neuesten Stand zu halten und die Zugriffe angemessen zu schützen.

Bei den Schadsoftware-Familien ist weiterhin vor allem «Qakbot» aktiv. Insgesamt 20 Meldungen sind dem NCSC im zweiten Halbjahr 2022 gemeldet worden. Diese Schadsoftware wird über E-Mails verbreitet. Eine Spezialität von «Qakbot» ist die Verwendung und Anknüpfung an bestehende E-Mail-Konversationen, die durch frühere Angriffe in deren Hände gelangt sind. So versuchen die Angreifer Vertrauen aufzubauen, da die Empfänger die Kommunikation und die angeblichen Absender kennen. Ziel ist es, das Opfer zu verleiten, auf den Link zu klicken.

4.4.2 Meldungen zu Hacking weiterhin stark steigend

Meldungen in der Kategorie Hacking nahmen stark zu. Mit 276 Meldungen hat sich die Zahl, verglichen mit der Vorhalbjahresperiode, fast verdoppelt. Im Visier sind dabei mit 108 Meldungen vor allem Social-Media-Konten. Mittlerweile werden gehackte Social-Media-Konten im Zusammenhang mit Fake-Sextortion verwendet, um der Fake-Erpressung Nachdruck zu verleihen (siehe unten). Eine andere häufige Verwendung von gehackten Social-Media-Konten ist das Schalten von Werbung für Investment-Betrug. Gerade bei Social-Media-Konten mit vielen Followern ist dies eine beliebte Masche, um die Informationen zu dubiosen Geschäften an möglichst viele potentielle Opfer zu bringen.

4.4.3 Gefälschte Erpressungen mit richtigen Angriffen

Bislang wurde bei sogenannten Fake-Sextortion-E-Mails ausschliesslich geblufft. Die Täter behaupten jeweils in einem E-Mail, dass sie Foto- oder Videomaterial gesammelt haben, welches den E-Mail-Empfänger während eines angeblichen Besuchs auf pornografischen Websites zeigen soll. Die Erpresser drohen mit der Veröffentlichung des Bild- oder Videomaterials, wenn die geforderte Lösegeldzahlung nicht innerhalb einer bestimmten Frist erfolgt. In der Berichtsperiode wurden dem NCSC 1’138 E-Mails des Typs Fake-Sextortion gemeldet. Normalerweise bluffen die Betrüger. Sie haben keinen Zugriff auf den Computer des Opfers und hoffen, dass dieses eingeschüchtert und die Lösegeldsumme bezahlt wird. Im letzten Halbjahr

[4] Cyber Signals (microsoft.com)

gab es aber auch Meldungen, dass kurz vor oder nach dem Erpresser-Schreiben, sowohl das E-Mail-Konto als auch diverse Social-Media-Konten des Opfers gehackt wurden. In insgesamt 33 Fällen luden die Betrüger pornographisches Material hoch, was zu einer sofortigen Sperre der Social-Media-Konten und einer entsprechenden Benachrichtigung führte. Die Angreifer versuchten so, das Opfer zu verängstigen und zu einer Zahlung zu bewegen. Die Zugangsdaten dürften entweder von alten Datenabflüssen oder von alten Phishing-Angriffen stammen. Gemessen an der Gesamtzahl der gemeldeten Fake-Sextortion-E-Mails ist die Variante mit gehackten Konten aber immer noch sehr klein. Dies weist darauf hin, dass die verwendeten Login/Passwort-Kombinationen nicht sehr aktuell sind und demnach nicht bei jedem Opfer funktionieren. Es dürfte sich um eine Zweitverwendung von Login/Passwort Daten handeln, die im Darknet billig zu kaufen sind.

4.5 Diverse Meldungen

4.5.1 Die Ohnmacht bei Spoofing-Anrufen

Auch Meldungen zu gespooften Telefonnummern sind geradezu explodiert. Dabei manipulieren die Angreifer die angezeigte Telefonnummer so, dass anstelle ihrer Rufnummer eine andere Telefonnummer angezeigt wird mit dem Ziel, beim Opfer Vertrauen zu erwecken. Während im ganzen Jahr 2021 gerade einmal 26 Meldungen dazu eingegangen sind, hat das NCSC allein im zweiten Halbjahr 2022 insgesamt 781 entsprechende Meldungen erhalten. Der Grund liegt in einer neuen Vorgehensweise von dubiosen ausländischen Callcentern. Damit die Angerufenen möglichst viele ihrer Werbeanrufe auch entgegennehmen, verwenden die Angreifer unscheinbare Schweizer Telefonnummern. Diese auf den ersten Blick harmlose Vorgehensweise hat weitreichende Folgen für diejenige Person, der die Nummer gehört. Wird der Anruf verpasst und die Nummer im Display angezeigt, rufen viele darauf zurück und der Inhaber der Nummer wird mit Anrufen überhäuft. Da die Callcenter über Wochen oder sogar Monate die gleiche Nummer verwenden, ist dies für die Opfer sehr nervenaufreibend.

Leider kann gegen solche Anrufe nur wenig unternommen werden. Da die Callcenter-Anrufe aus dem Ausland stammen, ist die Prüfpflicht betreffend Nummernnutzung, welche die Schweizer Telefonanbieterinnen durchführen müssen, nicht anwendbar. Diese gilt nur, wenn der Anruf aus ihrem Netz stammt. Hören die Anrufe nicht auf, bleibt am Schluss nur der Ausweg, die Rufnummer zu wechseln.

5 Lage

5.1 Initialer Zugang

Cyberakteure sind arbeitsteilig organisiert und spezialisieren sich auf einzelne Etappen von Cyberangriffen. Die Erlangung von Fernzugriffen auf Computersysteme oder Zugang zu Nutzerkonten ist bei den meisten Arten von Cyberangriffen der erste Schritt. Ein solcher initialer Zugang kann auf verschiedene Weise erlangt und nach der Etablierung auch an andere Akteure zur Ausnützung weitergegeben werden.

5.1.1 Nutzername / Passwort

Die Beschaffung von Login-Daten geschieht meistens via Phishing (siehe auch Kapitel 4.3). Das heisst, sie werden von den Nutzern selbst unbewusst an die Angreifer weitergegeben. Daneben können Login-Daten auch mithilfe von Schadsoftware (Keylogger) bei der Eingabe auf einem infizierten Gerät abgegriffen werden.

Für das Eindringen in Firmennetzwerke werden häufig Zugangsdaten für Fernzugriffe via Remote Desktop Protocol (RDP) oder Virtual Private Network (VPN) missbraucht.

Empfehlung:

Schutz vor dieser Bedrohung bietet zum Beispiel eine Zwei- oder Mehrfaktor-Authentisierung. Dann reicht die Kombination von Nutzername und Passwort nämlich nicht aus, um auf das gesicherte System oder Nutzerkonto zuzugreifen, sondern es wird noch eine weitere Information benötigt, wie zum Beispiel ein einmaliger Code, der auf das Mobiltelefon gesendet wird oder der Zugang muss via eine Authentisierungs-App freigegeben werden.

5.1.2 Schadsoftware (Trojaner)

Schadsoftware, die nach ihrer Installation eine Hintertür zum System einrichtet, ist weiterhin eine häufig verwendete Methode, um einen initialen Zugang zu etablieren.

Der beliebteste Verbreitungsvektor für solche 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 dem Krieg in der Ukraine, Naturkatastrophen oder Sportanlässen in Aussicht gestellt, um Neugier zu wecken. Häufig wird Dringlichkeit vorgetäuscht, um Empfängerinnen und Empfänger zu unbedachten Aktionen zu verleiten. Solche E-Mails werden zum einen massenweise an eine Vielzahl von Empfängern geschickt (Malspam). Zum anderen werden alte E-Mail-Konversationen genutzt, die zu einem früheren Zeitpunkt von kompromittierten E-Mail-Nutzerkonten oder gehackten E-Mail-Servern beschafft worden sind, um gezielt Teilnehmer an diesen Konversationen anzuschreiben (Thread-Hijacking) und ihnen einen Trojaner unterzujubeln.

Eine andere Variante, wie Nutzer dazu gebracht werden, eine Schadsoftware zu installieren, ist der Kauf von Online-Werbefläche respektive das Aufschalten von gesponserten Suchmaschinentreffern (Malvertising). Darin wird vorgetäuscht, dass eine gesuchte Software – sei dies z. B. ein Browser, eine Kommunikations-App oder ein Videoplayer – über das entsprechende Inserat erhältlich sei. Zusammen mit der gewünschten (Gratis-)Software wird dann jedoch auch ein Trojaner installiert. Eine ähnliche Methode besteht darin, dass Nutzer via Werbelink auf eine Seite gelockt werden, die vorgibt, dass der Browser nicht mehr aktuell sei und ein Update brauche. Da die Webseite erkennt, mit was für einem Browser man sie aufruft, wird die Seite dynamisch an den verwendeten Browser angepasst. Beim Klick auf die Update-Schaltfläche wird dann eine Datei heruntergeladen, die beim Ausführen den Trojaner installiert. Solche Fake-Updates können auch via gehackte Webseiten verbreitet werden.

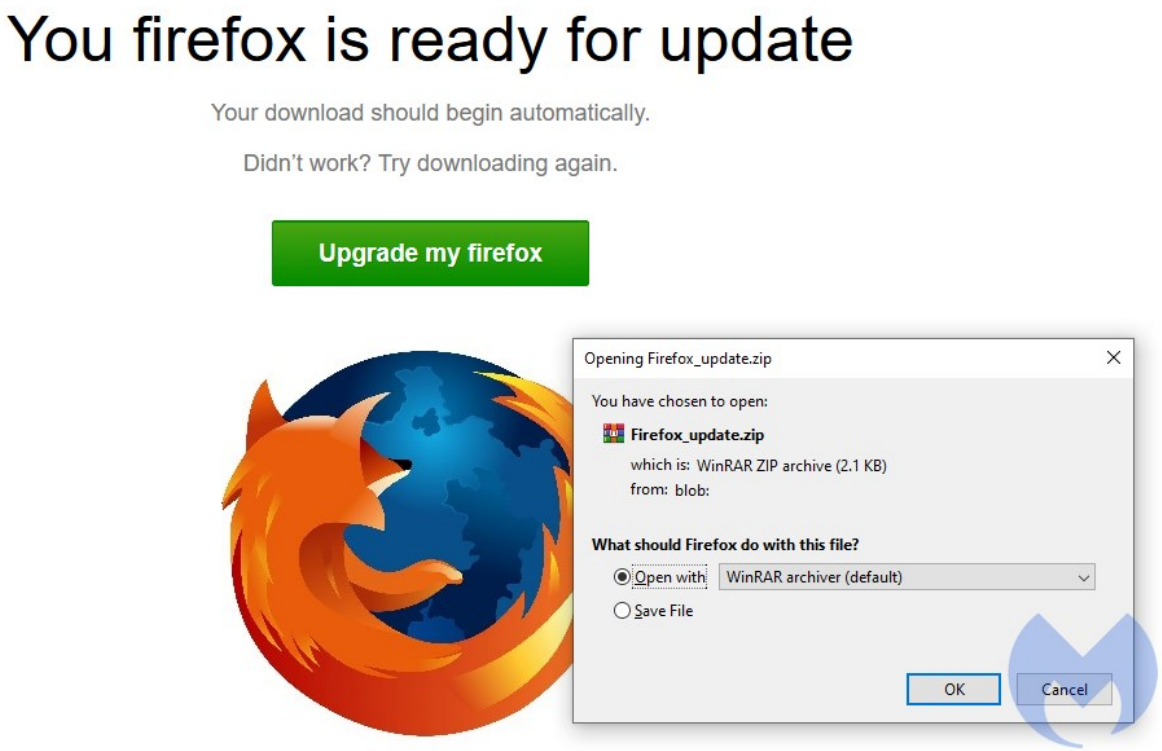

Abb. 8: Fake-Update (Quelle: Malwarebytes.com)

Schlussfolgerung / Empfehlung:

Klicken Sie in verdächtigen E-Mails nicht auf Links und öffnen Sie keine angehängten Dateien. Fragen Sie im Zweifelsfall beim vermeintlichen Absender nach, ob das E-Mail tatsächlich von ihm versendet worden ist.

Verifizieren Sie bei der Suche nach Software im Internet vor dem Download, dass Sie sich auf der Website der Herstellerin oder einer anderen vertrauenswürdigen Website (z. B. einer bekannten Computerzeitschrift) befinden. Seien Sie vorsichtig, wenn immer sich ein Download-Fenster öffnet. Lassen Sie Programme wenn möglich automatisch aktualisieren. Ansonsten verwenden Sie immer die integrierte Update-Funktion oder laden die neueste Version direkt beim Hersteller herunter.

5.1.3 Ausnutzen von Schwachstellen

Sobald eine Schwachstelle in einem Produkt bekannt wird, beginnen verschiedene Akteure, das Internet nach verwundbaren Systemen abzusuchen. Nach einigen Stunden oder Tagen beginnt das Ausnutzen dieser Schwachstelle. Es werden jedoch auch regelmässig Schwachstellen ausgenutzt, die schon länger bekannt sind und für die ein Patch verfügbar wäre. Im Katalog der aktuell ausgenutzten Verwundbarkeiten der US-amerikanischen Cybersicherheitsbehörde CISA[5] werden regelmässig alte Schwachstellen neu eingefügt, die von den Anwendern mit effektivem Update-Management bereits hätten behoben werden können.[6]

---

5 Known Exploited Vulnerabilities Catalog (cisa.gov)

6 Adobe, Apple, Cisco, Microsoft Flaws Make Up Half of KEV Catalog (darkreading.com)

Neben Programmierfehlern der Entwickler, die mittels Patch behoben werden, können auch die bei der Implementierung von Produkten gewählten Konfigurationen zu Schwachstellen führen. Verschiedene Hersteller geben Konfigurationsanleitungen zur Härtung ihrer Produkte.

Empfehlungen:

Prüfen Sie beim Einsatz neuer Produkte deren Konfiguration bezüglich Sicherheit und Datenschutz. Stellen Sie sicher, dass nur diejenigen Funktionalitäten aktiviert sind, die Sie auch benötigen.

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

Software, die am Ende ihres Lebenszyklus (End-of-Life) angelangt ist und vom Hersteller nicht mehr mit Updates versorgt wird, sollte ersetzt werden.

Das NCSC informiert regelmässig Organisationen, die über veraltete Systeme angreifbar sind.[7] Es erhält entsprechende Hinweise von Sicherheitsforschern, die das Internet nach solchen Systemen absuchen. In gleicher Weise können auch Kriminelle verwundbare Systeme suchen und angreifen. Systembetreiberinnen sollten deshalb nicht darauf warten, vom NCSC benachrichtigt zu werden. Ein eigenes, effektives Software-Management mit Inventar und Update-Prozessen ist dringend empfohlen.[8] Spätestens jedoch wenn ein eingeschriebener Brief des NCSC bei der Organisation eintrifft, ist rascher Handlungsbedarf gegeben.

5.2 Schadsoftware / Malware

5.2.1 Schadsoftware-Verbreitung

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 KMU. 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.

---

[7] Höchste Zeit, die Sicherheitslücken bei Microsoft Exchange-Server zu schliessen (ncsc.admin.ch);
MS Exchange-Lücken werden noch immer nicht geschlossen (ncsc.admin.ch);
Erneut über 2'800 verwundbare Microsoft Exchange Server in der Schweiz («ProxyNotShell») (ncsc.admin.ch);
Weiterhin verwundbare Microsoft Exchange Server in der Schweiz («ProxyNotShell») trotz Warnung des NCSC (ncsc.admin.ch)

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

Analysen von Malware-Familien durch das NCSC

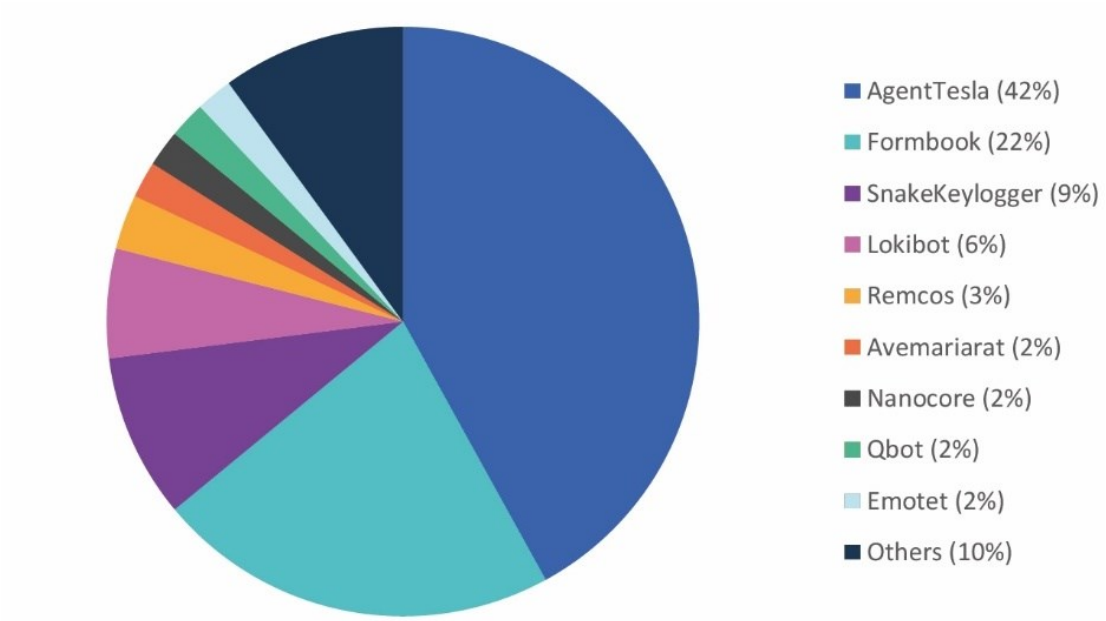

Abb. 9: Analysen des NCSC von Malware-Familien, die in der Schweiz im zweiten Semester 2022 verbreitet wurden.

5.2.2 Ransomware

Angriffe mit Ransomware sind nach wie vor eine häufige und die wahrscheinlich konsequenzenreichste Cyberbedrohung, mit der Organisationen in der Schweiz konfrontiert sind. In der zweiten Jahreshälfte waren vorwiegend kleine und mittelgrosse Industriebetriebe und IT-Dienstleister davon betroffen. Ransomware-Entwickler verfolgen neue Strategien und Methoden, um Systeme zu infiltrieren und ihre Opfer zu erpressen: neue Version der Ransomware, Code in der für Windows und Linux anwendbaren Programmiersprache Rust, Veröffentlichung der Daten auf regulären Webseiten (nicht nur im Darkweb) usw. Zur Gewinnmaximierung setzen sie häufig auf doppelte Erpressung: Daten werden vor der Verschlüsselung aus dem kompromittierten Netzwerk exfiltriert, damit die Opfer auch mit der drohenden Publikation der Daten erpresst werden können. Angesichts der steigenden Zahl von Ransomware-Fällen, der Verfügbarkeit dieser Malware als Dienstleistung (Ransomware-as-a-Service, RaaS) und der immer grösseren Anzahl von Ransomware-Stämmen und -Familien arbeiten Cybersecurity-Firmen und staatliche Stellen enger zusammen, um die Schlüssel für die Dechiffrierung zu finden und Entschlüsselungsprogramme zu entwickeln.

5.2.2.1 Beispiele von Vorfällen in der Schweiz

Play: Wenn ein Vorfall Dritte betrifft

Ende November musste ein Berner Anbieter von Cloud-Computing-Dienstleistungen seine Rechenzentren infolge eines Ransomware-Angriffs, der vermutlich von der Gruppierung Play ausging, herunterfahren. Die vier Tage zuvor durchgeführten Backups ermöglichten die Rettung eines Teils der Daten. Dieser Vorfall hatte Folgen für alle Kunden des Anbieters, da einige nicht mehr auf ihren Cloud-Service zugreifen konnten. Sie konnten unter anderem keine Rechnungen mehr ausstellen oder Gehälter berechnen und auszahlen. Allerdings wurden beim Angriff keine Daten exfiltriert. Auch aus anderen Kantonen wurden im Laufe dieses Jahres vergleichbare Vorfälle gemeldet, die die Handschrift von Play trugen.

Doppelte Erpressung – Angriff mit Verschlüsselung und Datenverlust

Am 5. September 2022 erlitt eine Schokoladenfabrik einen Ransomware-Angriff, der die Produktion, die Logistik und die Verwaltung in Mitleidenschaft zog. Zwei Wochen nach dem Angriff waren diese Abteilungen wieder voll funktionsfähig. Allerdings bestätigte das Unternehmen, dass der Cyberangriff wahrscheinlich zu einem Datenabfluss geführt hatte. Einen Monat später veröffentlichte die Ransomware-Gruppe BianLian im Darknet Dateien über die Geschäfte des Unternehmens.

Die BianLian-Gruppe verwendet eine massgeschneiderte Malware, die in der Programmiersprache Go geschrieben ist.[9] Die Gruppe begann mit ihren Online-Aktivitäten im Dezember 2021, intensivierte sie im Juli 2022 und baute ihre Command-and-Control-Infrastruktur (C2) im August 2022 massiv aus.

5.2.2.2 Vorfälle im Ausland: Angriffe auf den Energiesektor

Im Halbjahresbericht 2022/1 stellte das NCSC einige Beispiele für Wirtschaftszweige vor, die von Ransomware betroffen sind, und wies darauf hin, dass es Kriminelle offenbar besonders auf Regierungen, Behörden und Energieinfrastrukturen abgesehen haben. Diese Tendenz bestätigte sich in der zweiten Jahreshälfte, und es wurde viel über den Energiesektor geschrieben. Das erhöhte Interesse an dieser Branche liegt möglicherweise auch daran, dass der Energiesektor als kritische Infrastruktur permanent betriebsbereit sein muss und im aktuellen geopolitischen Kontext besonders unter Druck steht. Mehrere europäische Energieversorger waren von Ransomware-Angriffen betroffen.[10] Es überrascht nicht, dass die Täter, die sich zu diesen Angriffen bekannt haben, wie im Fall von BlackCat und Everest, russlandaffine Gruppen sind. Bisher sind die Energieversorger in der Schweiz von solchen Angriffen verschont geblieben, und es ist zurzeit auch eher unwahrscheinlich, dass die Schweiz gezielt angegriffen wird. Nicht ausgeschlossen werden können jedoch opportunistische Angriffe auf verwundbare Systeme oder Kollateralschäden durch Angriffe auf europäische Versorger.

5.2.2.3 Überblick über die aktivsten Akteure und meist genutzten Infektionsvektoren

Im Jahr 2022 wurde in der Schweiz am häufigsten die Ransomware «Lockbit» (in den Versionen 2.0 oder 3.0 alias Black) eingesetzt, gefolgt von «Deadbolt» und «Play» (siehe Kapitel 4.4.1). Weltweit führte die Lockbit-Gruppe weiterhin das Feld an, gefolgt von BlackBasta und BlackCat. Einige Monate rangierten andere Gruppen unerwartet an der Spitze der Rangliste, konnten sich dort aber nicht lange halten. Beispiele hierfür sind Hive, Sparta, Cuba, Royal und BianLian.

Lockbit Black: Mit Versions-Update bleibt Lockbit auf Platz 1

Im Juli 2022 gab die Lockbit-Gruppe die Entwicklung der Version 3.0 ihrer Ransomware bekannt. Dieses Upgrade machte sich ab November 2022 in der Schweiz bemerkbar: Die Polizei registrierte einen Anstieg der Fälle, die im Zusammenhang mit dieser Malware auftraten.

---

9 MalwareHunterTeam on Twitter: "A BianLian x64 ransomware sample (twitter.com)

10 2022 waren wichtige Gasunternehmen in Italien, wie GSE SpA und Amalfitana Gas Srl, das Erdölunternehmen Eni, der Betreiber von Strom- und Erdgasnetzen in Luxemburg Creos Luxembourg SA, und der nationale griechische Erdgasbetreiber DESFA von Ransomware-Angriffen betroffen.

Allerdings sind einige Bereiche verschont geblieben, denn der Ehrenkodex von Lockbit (respektive die allgemeinen Geschäftsbedingungen der Ransomware-as-a-Service-Gruppe) verbietet die Verschlüsselung von Daten in Schulen und Spitälern. Trotzdem wurde ein kanadisches Kinderspital Opfer eines solchen Angriffs. Es stellte sich heraus, dass die Täter Partner (so genannte Affiliates) der Lockbit-Gruppe waren. Die Gruppe entschuldigte sich via Social Media und teilte mit, dass sie diesen Partner ausgeschlossen habe. Ausserdem stellte Lockbit dem Spital einen kostenlosen Dechiffrierer zur Entschlüsselung seiner Daten zur Verfügung.

Im Rahmen von Ermittlungen gegen Lockbit konnten französische und kanadische Behörden gemeinsam mit dem FBI rund 1'800 tatsächliche oder mutmassliche Opfer von Lockbit identifizieren.[11] Die befallenen Systeme wiesen eine Sicherheitslücke in ihren FortiGate- oder SonicWall-Firewalls auf. Betroffene Organisationen in der Schweiz wurden von der Polizei benachrichtigt.

Agenda & Hive: Rust bringt frischen Wind in alte Ransomware

Viele Akteure der Ransomware-Szene haben eine überarbeitete Version ihrer Software in der plattformübergreifenden Sprache Rust entwickelt, mit der die Malware auf Windows wie auch Linux eingesetzt werden kann. Ein Beispiel hierfür ist «Agenda» (auch bekannt als «Qilin»), das ursprünglich in der Programmiersprache Go geschrieben wurde. Derzeit scheinen die Autoren von «Agenda» damit beschäftigt zu sein, den Code ihrer Ransomware in Rust zu migrieren, da den neuesten Ausgaben der Software einige Funktionen fehlen, die im Originalcode enthalten waren. «Agenda», wie auch die Ransomware «Royal», arbeitet mit Teilverschlüsselung (auch intermittierende Verschlüsselung genannt). Dabei wird der Prozentsatz des zu verschlüsselnden Dateiinhalts durch gesetzte Parameter bestimmt. Auf diese Weise können Verschlüsselungen schneller durchgeführt und Erkennungen vermieden werden, die weitgehend auf den Lese-/Schreibfunktionen der Dateien beruhen. Die Urheber von Angriffen verwenden immer häufiger die Programmiersprache Rust, da sie schwieriger zu analysieren ist und in Rust geschriebene Malware von vielen Antivirenprogrammen bislang nicht sehr gut erkannt wird. In der Schweiz wurde eine Gemeindeverwaltung im Kanton Zürich von der Ransomware «Agenda» verschlüsselt. Die Wiederherstellung der Daten war dank Backups möglich.

BlackCat & IceFire: Veröffentlichung geleakter Daten im Internet

Eine neue Erpressungstechnik der Ransomware-Gruppe ALPHV/BlackCat besteht darin, eine Kopie der Website des Opfers zu erstellen und dort die gestohlenen Daten zu veröffentlichen, um den Druck auf die Geschädigten zu erhöhen. Auf der kopierten Website ersetzt BlackCat die ursprünglichen Rubriken und Unterseiten, um die geleakten Daten zu sortieren. Die nachgebildete Website wird ins Internet gestellt, damit die gestohlenen Dateien leichter verfügbar sind als im Darkweb. Die Erpressungs-Website wird häufig auf einer Tippfehler-Domain[12] aufgeschaltet. Dies ist für das geschädigte Unternehmen problematischer als die Freigabe von Daten über eine Website im Tor-Netzwerk im Darkweb, da auf normalen Webseiten bereitgestellte Daten einfacher eingesehen werden können. Dies erhöht den Druck auf das Opfer, Lösegeld zu zahlen. Denn sie wollen vermeiden, dass ihre Kunden oder andere Personen die Daten sehen können.

---

11 Police arrest suspected LockBit operator as the ransomware gang spills new data (techcrunch.com)

12 So genannte Typo-Domain, z. B. adimn.ch, adnim.ch oder adrnin.ch statt admin.ch

Diese Idee wurde von der Ransomware-Gruppe IceFire aufgegriffen, die Mitte August 2022 ein Schweizer Unternehmen angriff. IceFire trat im März 2022 in Erscheinung und wählte die gleiche Technik wie BlackCat, um ihre Opfer stärker unter Druck zu setzen.

Play alias PlayCrypt: Fokus auf regierungsnahe Opfer

Schon bei ihrem Debüt im Sommer 2022 interessierte sich die Play-Gruppe für staatliche Stellen. Dies ist angesichts der repressiven Strafverfolgung, die solche Angriffe nach sich ziehen, eher eine Seltenheit. Play greift vor allem in Lateinamerika an. Es gab jedoch auch Opfer auf anderen Kontinenten und in anderen Sektoren als in der Verwaltung.

Play ist bekannt für seine «Big Game Hunting»-Strategie, also Angriffen auf grosse finanzkräftige Organisationen. Zum Einsatz kommen dabei z. B. «Cobalt Strike» für die Post-Breach-Phase und «SystemBC RAT» für die Persistenz. Erst kürzlich haben die Hacker von Play damit begonnen, die ProxyNotShell-Schwachstellen in Microsoft Exchange auszunutzen. Analysen zeigten Parallelen zwischen den Ransomware-Varianten «Play», «Hive» und «Nokoyawa».

BianLian & MegaCortex: Entschlüsselung mit Dechiffrierern ...

Im Januar 2023 wurde ein kostenloser Dechiffrierer (Programm zum Entschlüsseln von mit Ransomware verschlüsselten Dateien) für den Ransomware-Stamm «BianLian» veröffentlicht, und das nur sechs Monate nach dessen Hochphase im Sommer 2022.[13] In einer Gemeinschaftsaktion von Europol und der Kantonspolizei Zürich wurde auch ein Entwickler der Ransomware «MegaCortex» festgenommen, woraufhin eine Entschlüsselungs-Software für diesen Stamm entwickelt werden konnte. Im Internet gibt es jetzt viele kostenlose Entschlüsselungsprogramme.[14] Cybersecurity-Unternehmen bemühen sich, diese schnell zu entwickeln, um gegen die stetig wachsende Anzahl und Vielfalt von Ransomware-Stämmen vorzugehen.

… und mit Dechiffrierschlüsseln (Deadbolt)

Die niederländischen Polizei konnte im Oktober 2022 mit einem Trick bei der Bitcoin-Zahlung 150 Dechiffrierschlüssel von der Ransomware-Gruppe Deadbolt erlangen.[15] Deadbolt, die vorrangig von der Firma QNAP hergestellte NAS-Geräte verschlüsselt, sind auch in der Schweiz mehrere Geräte zum Opfer gefallen. Die Beschaffung dieser Schlüssel war ein grosser Erfolg, weil dadurch mehrere Opfer ihre Datenträger entschlüsseln konnten. Es ist jetzt möglich, online nachzusehen, ob ein Schlüssel für ein von Deadbolt infiziertes Gerät verfügbar ist.[16]

Schlussfolgerungen, Ausblick und Empfehlungen:

Bei Ransomware-Angriffen kommt es immer öfter vor, dass (teilweise sensible) Daten verschlüsselt und abgezogen werden, was als doppelte Erpressung bezeichnet wird. Manche Angreifer machen sich gar nicht mehr die Mühe, die Systeme zu verschlüsseln, sondern drohen ihren Opfern nur noch mit der Veröffentlichung ihrer Daten.

---

13 Decrypted: BianLian Ransomware (avast.io)

14 Siehe z. B. The No More Ransom Project (nomoreransom.org)

15 Police tricked a ransomware gang into handing over its decryption keys. Here's how they did it (zdnet.com)

16 Deadbolt Decryption (responders.nu)

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) sowie Datenabfluss - Was nun? (ncsc.admin.ch)

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

Wie zuletzt im Rahmen des Krieges in der Ukraine demonstriert, werden im Umfeld von geopolitischen Konflikten sporadisch auch zerstörerische Cybersabotageangriffe beobachtet.[17] Um Wirkung auf physische Prozesse zu erzielen, braucht es fast zwangsläufig eine Manipulation der operativen Technologie, respektive deren Steuerungssysteme. Dabei wird nur in den seltensten Fällen direkt auf die gesteuerten physischen Prozesse eingewirkt, sondern in weitaus mehr Fällen, die Server- und Netzwerkinfrastruktur angegriffen, um dadurch den operativen Betrieb zu stören.[18]

5.3.1 Sabotageversuche im Rahmen von Konflikten

Zu Beginn des Krieges[19] wurden gezielte Sabotageangriffsversuche mit Schadsoftware spezifisch für Systeme der Elektrizitätsversorgung[20] abgewehrt, Angriffsinfrastruktur[21] derselben Akteure exponiert und eine ganze Sammlung von Angriffswerkzeugen[22] vor deren Einsatz veröffentlicht. Im zweiten Halbjahr beschränkten sich die Sabotageversuche auf den Einsatz von destruktiven Wipern[23] und als Ransomware[24] getarnte zerstörerische Angriffe. Dabei wurden keine spezifischen Fähigkeiten zur Manipulation von industriellen Systemen mehr beobachtet, sondern die Angriffe richteten sich gegen IT-Systeme beispielsweise von Transportorganisationen[25] in der Ukraine und Polen.

Behauptungen von Hacktivisten-Gruppierungen wie OneFist[26] und Ghostsec[27], sie seien an Störfällen bei industriellen Anlagen beteiligt, wurden weder bestätigt noch konnten sie unabhängig verifiziert werden. Die präsentierten Ausschnitte der Gruppen deuten auf simple Manipulationsversuche aus dem Internet erreichbarer und schlecht geschützter Anzeige- oder Bedienoberflächen industrieller Steuerungen hin.

---

17 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.

18 How Many ICS-OT Directed Attacks In 2022? (linkedin.com)

19 NCSC Halbjahresbericht 2022/1, Kapitel 3 und 5.4

20 Industroyer2: Industroyer reloaded (welivesecurity.com)

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

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

23 Russian APT groups continue their attacks against Ukraine with wipers and ransomware (eset.com)

24 RansomBoggs: New ransomware targeting Ukraine (welivesecurity.com)

25 New “Prestige” ransomware impacts organizations in Ukraine and Poland (microsoft.com)

26 The Increasing Threat Posed by Hacktivist Attacks (forescout.com)

27 Country-Specific ICS Targeting: Shining a Light on GhostSec (otorio.com)

5.3.2 Angespannte Energieversorgung im Fokus

Als Nebenwirkung des Krieges in der Ukraine wurde die Versorgungssicherheit mit Energieträgern in Europa und damit auch der Schweiz beeinträchtigt. In der Schweiz wirkt sich dies besonders auf die Gas- und Stromversorgung aus. Um die Eintretenswahrscheinlichkeit einer Mangellage zu verringern, wurde beispielsweise in einer Kampagne zum Energiesparen aufgerufen.[28]

In einer solch angespannten Lage könnte ein erfolgreicher Cyberangriff auf die Steuerungen der Versorgungssysteme schwerwiegendere Auswirkungen haben, als wenn genügend Kompensationsmöglichkeiten verfügbar wären. Ohne Eskalation des Krieges auf weitere europäische Gebiete bleibt ein gezielter staatlicher Cybersabotageversuch[29] gegen Schweizer Energieversorgungssysteme unwahrscheinlich. Die weitaus grössere Gefahr geht hier von Ransomware-Angriffen aus.[30] Legen daraus resultierende Verschlüsselungen Systeme lahm, welche am Betrieb der Energieversorgung beteiligt sind, kann dies Einschränkungen und Unterbrüche im produktiven Betrieb verursachen.[31]

Auch die physische Sicherheit der Systeme spielt in diesem Kontext eine Rolle. Das Beispiel der mechanischen Durchtrennung von Steuerungskabeln der Deutschen Bahn,[32] zeigt einerseits die reale Gefahr von Sabotage-Angriffen vor Ort auf.[33] Andererseits betont sie die Wichtigkeit der Vorbereitung von Massnahmen zur Wiederherstellung der Betriebsbereitschaft, um die Resilienz des Gesamtsystems zu stärken.

Schlussfolgerung / Empfehlungen:

Überlegungen zur Resilienz der Systeme und Organisationen spielen eine zentrale Rolle, um den Betrieb industrieller Anlagen auch in angespannten Situationen aufrecht zu erhalten. Dazu gehört auch die ständige Aus- und Weiterbildung des Personals.

Geeignete Massnahmen finden sich in den IKT-Minimalstandards des Bundesamtes für wirtschaftliche Landesversorgung (BWL) oder in den jeweiligen Branchenstandards:

IKT-Minimalstandards (ncsc.admin.ch)

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

28 Energie: Bundesrat startet Sparkampagne (admin.ch)
29 Sicherheit Schweiz 2022: Der Nachrichtendienst des Bundes publiziert seinen neuen Lagebericht (admin.ch)
30 Dragos Industrial Ransomware Analysis: Q4 2022 (dragos.com)
31 Cybersecurity Research Report January 2023 (nozominetworks.com)
32 Sabotage bei der Bahn: Viele vertrauliche Infos sind offen zugänglich (heise.de)
33 BfV-Sicherheitshinweis für die Wirtschaft 04/2022 (wirtschaftsschutz.info)

5.4 Schwachstellen

5.4.1 Systeme mit öffentlich einsehbaren Konfigurationsdateien

Dem NCSC werden regelmässig Schwachstellen von Sicherheitsforschenden über den «Coordinated Vulnerability Disclosure»-Prozess[34] mitgeteilt. In diesem Halbjahr wurden verschiedene Schwachstellen gemeldet, welche auf eine schlechte Software-Konfiguration zurückzuführen waren: Die Konfigurationsdateien liegen in einem Verzeichnis auf einem Webserver und sind ohne Restriktionen zugreifbar.

Ein verbreitetes Beispiel sind die Dateien, welche von der Versionierung-Software «Git» erstellt werden. Diese Software erstellt einen Ordner mit der Bezeichnung «.git», darin wird der gesamte Quellcode gespeichert. Ist dieser Ordner über einen Webserver zugänglich und einsehbar, so kann ein Angreifer mit technischem Verständnis auf potenziell sensible Daten wie Zugangsdaten oder Passwörter zugreifen.

Das NCSC konnte 1'300 betroffene Systeme in der Schweiz identifizieren und hat deren Betreiber benachrichtigt.

«Git» ist nicht die einzige Software, welche solche Konfigurationsdateien und versteckte Ordner anlegt; ein weiteres Beispiel sind PHP-Profiler-Seiten, eine Komponente des Symfony Frameworks.[35] Auch Textdateien wie «.env» werden häufig verwendet, um Zugangsschlüssel und Passwörter, welche ein System verwendet, zu speichern. Sind diese nicht mit den korrekten Zugriffsrechten versehen, können auch diese von einem Angreifer gelesen und missbraucht werden.

Das NCSC arbeitet aktiv mit Sicherheitsforschenden zusammen, um betroffene Betreiber zu informieren und bezüglich der Risiken und Gefahren solcher Konfigurationsfehler zu sensibilisieren.[36]

Schlussfolgerung / Empfehlungen:

Konfigurationsdateien wie der «.git»-Ordner sollten niemals öffentlich im Internet zugänglich sein. Ist eine Entfernung des Ordners kurzfristig nicht möglich, sollte mindestens der Zugriff auf den Ordner eingeschränkt und entsprechend geschützt werden (beispielsweise durch .htaccess Regeln oder je nach eingesetzter Technologie ähnliche technische Zugriffsbeschränkungen).

Noch zielführender sind präventive Massnahmen wie die Überprüfung und Anpassung des Entwicklungsprozesses. Dabei soll sichergestellt werden, dass nur die gewünschten und die dafür vorgesehenen Daten («build files») überhaupt abgelegt werden. Sensitive oder geheime Daten wie Passwörter, API-Keys, usw. sollten niemals im Quellcode oder in der Applikation selbst abgelegt sein («hardcoded») oder zumindest sichergestellt werden, dass diese nicht im «Git»-Verzeichnis abgelegt, sondern ignoriert werden («gitignore file»). Diese grundlegenden Sicherheitsmassnahmen und «best practices» sollten auf jeden Fall eingehalten werden.

---

34 Melden einer Schwachstelle (Coordinated Vulnerability Disclosure, CVD) (ncsc.admin.ch)

35 Covid-Center & andere Webseiten: Bedienen Sie sich! (dnip.ch)

36 Ungeschützte Git-Verzeichnisse im Internet als Sicherheitsrisiko (ncsc.admin.ch)

5.4.2 ProxyNotShell

Ende September 2022 berichtete ein vietnamesisches Cybersicherheitsunternehmen[37] über Angriffe, welche im August 2022 auf kritische Infrastrukturen weltweit stattgefunden hatten. In deren Untersuchung konnten zwei Zero-Day-Schwachstellen in Microsoft Exchange-Server identifiziert werden, welche für den Angriff verwendet wurden. Die erste Schwachstelle (CVE-2022-41040) ist eine «Server-side request forgery» (SSRF) Schwachstelle, welche es einem authentisierten Angreifer erlaubt, die zweite Schwachstelle (CVE-2022-41082) zu starten, welche eine «Remote Code Execution» (RCE) Schwachstelle ist. Diese ermöglicht, Schadcode aus der Ferne über das Internet auszuführen. Beide Schwachstellen in Kombination können genutzt werden, um beispielsweise Zugang zu verwundbaren Systemen zu erhalten.

Microsoft hat kurz darauf die Schwachstellen in Microsoft Exchange-Server 2013, Microsoft Exchange-Server 2016 und Microsoft Exchange-Server 2019 bestätigt und empfohlen, Sofortmassnahmen einzuleiten. Die Schwachstelle wurde als «ProxyNotShell» bezeichnet, da sie sich auf eine im 2021 aufgetauchte Exchange-Schwachstelle mit der Bezeichnung «ProxyShell» (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) bezieht, welche gewisse Ähnlichkeiten mit der neuen Schwachstelle aufwies.

Am 10. November 2022 wurden Software-Updates durch Microsoft veröffentlicht, welche die Schwachstellen geschlossen haben. Am 18. November 2022 konnte das NCSC immer noch 2'800 Server in der Schweiz identifizieren, welche die aktuellen Sicherheits-Updates nicht eingespielt hatten und zu diesem Zeitpunkt verwundbar waren.[38] Anfang Dezember 2022 wurden die Betroffenen per eingeschriebenen Brief durch das NCSC benachrichtigt.

Schlussfolgerung / Empfehlungen:

Die «ProxyNotShell»-Schwachstelle wurde bereits aktiv ausgenutzt, noch bevor ein offizieller Patch verfügbar war. In diesen Fällen ist es wichtig, schnell zu reagieren und den Empfehlungen – die bis zur Abschaltung des anfälligen Systems gehen können – zu folgen, bis beispielsweise 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, Zugriffsliste autorisierter IPs für die Wartung usw.). Falls für eine aktiv ausgenutzte Schwachstelle noch kein Patch verfügbar ist, kann durch eine gute Verwaltung externer Zugriffe allenfalls zusätzliche Reaktionszeit für Verteidigungsmassnahmen geschaffen werden. Dies ersetzt jedoch nicht die Aktualisierung des Systems und Installation von Patches, sobald diese verfügbar werden.

[37] Two Microsoft Exchange zero-days exploited by attackers (helpnetsecurity.com)

[38] Erneut über 2'800 verwundbare Microsoft Exchange Server in der Schweiz («ProxyNotShell») (ncsc.admin.ch)

5.4.3 Retbleed

Am 12. Juli 2022 hat die ETH Zürich[39] eine Schwachstelle in Mikroprozessoren von Intel und AMD veröffentlicht. Die als «Retbleed» benannte Schwachstelle ermöglicht einem Angreifer, potentiell auf beliebige Speicherbereiche zuzugreifen. Der Name «Retbleed» ist ein Kunstwort, das sich aus «RET» und «Bleed» (Englisch für bluten) zusammensetzt. Dies in Analogie zu früheren Schwachstellenbezeichnungen wie «Heartbleed», bei denen ebenfalls Daten aus dem Speicher gelesen werden konnten. RET ist die Bezeichnung für RETURN, eine Programm-Instruktion bei Prozessoren. Insbesondere bei geteilten Infrastrukturen (shared infrastructure) ist Vorsicht geboten und bei der Ausführung nicht vertrauenswürdiger Software.

Das NCSC hat die Forschenden der ETH Zürich in der Koordination der Veröffentlichung und bei der Vergabe der CVE-Nummern unterstützt. Für «Retbleed» wurden die CVE-Nummern CVE-2022-29900 (für Prozessoren des Herstellers AMD) und CVE-2022-29901 (für Prozessoren des Herstellers Intel) vergeben.

Schlussfolgerung / Empfehlungen:

«Retbleed» ist eine sehr komplexe Schwachstelle, welche bis jetzt nicht aktiv ausgenutzt worden oder zumindest eine Ausnutzung nicht bekannt ist.

Die Schwachstelle erfordert aber bestimmte Bedingungen, um erfolgreich ausgenutzt werden zu können, weshalb das Risiko für Benutzer sehr eingeschränkt ist.

Intel sowie AMD arbeiten an Patches, um die Schwachstelle zu minimieren und zu schliessen. Es ist und bleibt wichtig, nur vertrauenswürdige Software auf einem System zu betreiben und skeptisch gegenüber Fremdsoftware zu sein. Zudem ist es essenziell, Updates und Patches von Herstellern zeitnah zu installieren und auf deren Empfehlungen zu achten.

5.5 Datenabflüsse

Die Datensicherheit ist eine der zentralen Herausforderungen der Digitalisierung, sowohl für Dateneigentümer als auch für Personen und Unternehmen, die ihre eigenen Informationen in den Datensätzen wiederfinden. Trotz eines kontinuierlich steigenden Bewusstseins für Datensicherheit und Datenschutz im digitalen Raum, bleiben Datenabflüsse aufgrund vielfältiger Gründe auch in der zweiten Hälfte des Jahres 2022 Thema. Nebst ungenügend geschützten oder gewarteten Systemen führten menschliches Versagen und Cyberangriffe zur Veröffentlichung sensitiver Daten. Bei Cyberangriffen kann der Datendiebstahl – häufig gekoppelt mit einer Verschlüsselung der Daten (vgl. Kapitel 5.2.2 Ransomware) – genutzt werden, um die Dateneigentümer zu erpressen und/oder die Daten an den Meistbietenden zu verkaufen.

Obwohl Ransomware-Angriffe medial dominant sind, muss klar unterstrichen werden, dass ein beträchtlicher Teil der Veröffentlichungen sensitiver Daten mit einem bewussteren Datenmanagement verhindert werden könnte. Im Folgenden werden zwei Fälle beleuchtet, bei denen Informationen unbewusst publiziert, oder Dritten anvertraute Daten unbefugt weitergegeben wurden.

39 Spekulative Berechnungen öffnen eine Hintertür zum Informationsklau (ethz.ch)

5.5.1 Metadaten bei veröffentlichten Dateien

Webseiten sind zentrale Plattformen für Unternehmen und Institutionen, um Informationen gegen aussen zu kommunizieren und verfügbar zu machen. Dabei können ungewollt interne Informationen in den Metadaten von Dateien[40] ebenfalls publik werden. Rückschlüsse auf Namen der Beschäftigten, Nutzernamen, E-Mail-Adressen, Ordnerstrukturen, die eingesetzte Software und deren Versionsnummern können so beispielweise für Aussenstehende ersichtlich werden. In Bezug auf Cyberangriffe ist besonders die Information zu Versionen und die verwendete Applikation für Angreifer interessant, da es ihnen Hinweise auf mögliche Angriffsvektoren geben kann.

Dieses Problem im Zusammenhang mit Metadaten wurde auch in der Bundesverwaltung erkannt und entsprechende Massnahmen zur Sensibilisierung der Mitarbeitenden wurden eingeleitet.

Schlussfolgerung / Empfehlung:

In einem ersten Schritt sollten Organisationen eine Bestandesaufnahme durchführen und alle publizierten Dateien auf enthaltene Metadaten überprüfen. Nach einer allfälligen Bereinigung der Dateien können diese erneut publiziert werden. Weiter ist zu empfehlen, dass Dateien vor der Weitergabe respektive der Publikation gemäss einem vorgeschriebenen Prozess gesäubert werden. Nutzerinnen und Nutzer sind entsprechend zu sensibilisieren und zu schulen.

5.5.2 Entsorgung von IT-Mitteln und Datenträgern

Im Dezember 2022 wurde medial bekannt, dass die Justizdirektion des Kantons Zürich während mehreren Jahren Speichergeräte nicht fachgerecht entsorgt hatte. Damit gerieten sensitive, unverschlüsselte Daten mindestens zwischen 2006 und 2012 ins kriminelle Milieu. Die Datenträger beinhalteten unter anderem Telefonnummern und geheime Adressen von Staatsanwälten und Richtern, Strafakten, psychologische Gutachten sowie Gebäudepläne.[41]

Gemäss einem externen Untersuchungsbericht zu den Vorfällen wurde zudem festgestellt, dass Angestellte für eine effizientere Fallbearbeitung aufgrund eines unzuverlässigen Rechtsinformationssystems Schattendossiers auf lokalen Laufwerken anlegten. Diese Laufwerke waren jedoch nur ungenügend geschützt, da die Daten darauf nicht konsequent verschlüsselt worden seien.[42]

Schlussfolgerung / Empfehlung:

Der Vorfall zeigt exemplarisch, dass mit der fortschreitenden Digitalisierung der Datensicherheit eine besondere Aufmerksamkeit gewidmet werden muss. Dabei sollten die Prozesse der sicheren Datenaufbewahrung benutzerfreundlich gestaltet sein, damit die Vorgaben auch von allen Angestellten eingehalten werden.

---

40 Metadaten (Dateiinformationen und -eigenschaften) sind in allen Arten von Dateien enthalten. Während bei Dokumenten wie Word- oder PDF-Dateien z. B. die Autorenschaft hinterlegt sein kann, sind bei Fotodateien u. a. Ortsangaben (GPS) als Datenfelder in den Metadaten vorgesehen.

41 Schweiz aktuell - Datenleck bei Justizdirektion Kanton Zürich: GPK stellt Antrag auf PUK (srf.ch)

42 Datenskandal Justizdirektion: Zürich setzt die Prioritäten falsch (nzz.ch)

Es gibt verschiedene Wege, um Datenträger sachgerecht zu vernichten: Das Überschreiben der Daten, die Entmagnetisierung oder das physische Schreddern der Datenträger. Wenn Sie die Datenlöschung extern vergeben, wählen Sie den Dienstleister sorgfältig aus, wählen Sie ein angemessenes Verfahren und stellen Sie sicher, dass der Daten(träger)-Vernichtungsprozess protokolliert wird.

Das NCSC stellt einen Ratgeber für Unternehmen zum Thema Datenabfluss zur Verfügung.

5.6 Update Ukraine

5.6.1 Fortsetzung der Aktivitäten im Cyberraum ohne nennenswerte Erfolge

In der zweiten Hälfte des Jahres 2022 war der Krieg in der Ukraine weiterhin eines der Hauptereignisse des geopolitischen Geschehens. Im letzten Halbjahresbericht wurden die wichtigsten Vorfälle im Cyberraum im Zusammenhang mit dem aktuellen Krieg in der Ukraine und im Vorfeld des Krieges beleuchtet.[43] Seitdem gab es keine wesentlichen Veränderungen bei den Arten von Cybervorfällen, aber sie sollen an Intensität zugenommen haben.[44] So berichtete der Sicherheitsdienst der Ukraine, dass im Jahr 2022 4'500 Cyberangriffe neutralisiert worden waren, dreimal so viel wie im Jahr zuvor.[45] Russland übt also weiterhin über den Cyberraum Druck auf die Ukraine aus, bislang jedoch ohne offensichtliche Erfolge. Im letzten Halbjahresbericht wurden drei Hypothesen vorgeschlagen, um das Ausbleiben von erkennbaren zerstörerischen russischen Cyberangriffen zu erklären:

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.

Die seither verfügbaren Informationen über die Aktivitäten im Cyberraum im Zusammenhang mit dem Krieg in der Ukraine deuten darauf hin, dass die zweite Hypothese der Realität am nächsten kommt. Russland soll sehr aktiv sein und seit Oktober 2022 besonders intensiv die Infrastrukturen des Energiesektors in der Ukraine ins Visier genommen haben, konnte aber im Cyberraum keine Erfolge erzielen, da sich die Ukraine erfolgreich verteidigt.[46] Diese Cyberangriffe werden offenbar nicht als Alternative zu konventionellen militärischen Mitteln betrachtet,

---

43 Halbjahresbericht 2022/1 (ncsc.admin.ch), Kapitel 3

44 The number of cyberattacks on Ukraine keeps increasing (cip.gov.ua)

45 SSU neutralized over 4,500 cyberattacks on Ukraine in 2022 (ssu.gov.ua)

46 SSU neutralized hundreds of cyberattacks on Ukrainian cogeneration plants and energy companies in 2022 (ssu.gov.ua)

sondern werden oft gleichzeitig eingesetzt, auch in Verbindung mit Beeinflussung. Die Kampagne gegen die ukrainischen Elektrizitätswerke im Oktober/November 2022 ist ein Beispiel für diese Multidimensionalität einer Operation. Raketenangriffe wurden von Cyberangriffen und Propaganda begleitet. Die Cyberangriffe sollten den Druck auf einen Sektor erhöhen, der bereits mit begrenzten Ressourcen auskommen muss, welche zum Teil durch konventionelle militärische Mittel zerstört worden sind. Die Propaganda sollte die Verantwortung für die Folgen der Angriffe (einschliesslich Stromausfälle) auf den ukrainischen Staat, die lokalen Regierungen oder grosse ukrainische Unternehmen abwälzen.[47] Da die Ukraine mit dieser Vorgehensweise gerechnet hatte, konnten die Cyberoperationen jedoch nicht den beabsichtigten Erfolg erzielen. Dies unterstreicht einen Faktor, der den fehlenden Erfolg Russlands im Cyberraum erklären könnte: Es gab keine neuen Arten von Angriffen im Cyberraum. Die beobachteten Cyberangriffe wurden nach bereits bekannten Mustern durchgeführt, die durch Einsatz bewährter Abwehrstrategien vereitelt werden konnten.[48]

5.6.2 Unterschiedliche Cyberangriffe mit unterschiedlichen Folgen

Im Zusammenhang mit dem Krieg in der Ukraine wurde über zahlreiche Cyberangriffe berichtet, auch in der nicht fachspezifischen Presse. Leider werden in einigen dieser Artikel die Art oder die Auswirkungen dieser Angriffe nicht näher erläutert, was eine differenzierte Betrachtung der Ereignisse verhindert. Die Beschreibung einiger Cyberangriffe in den folgenden Abschnitten soll als Beispiel für die unterschiedlichen Auswirkungen dienen und die Vorsicht beim Lesen von Artikeln, die unspezifische Begriffe verwenden, unterstreichen.

5.6.2.1 Angriffe auf die Verfügbarkeit (Distributed Denial of Service, DDoS-Angriffe)

DDoS-Angriffe waren eine der sichtbarsten Arten von Cyberangriffen während des Berichtszeitraums.[49] Diese Angriffe zielen darauf ab, Websites oder andere Online-Dienste unzugänglich zu machen, hauptsächlich durch Überlastung mit einer hohen Anzahl von Anfragen. Diese Angriffe wurden hauptsächlich von Hacktivisten-Gruppen durchgeführt, die sich auf die Seite einer der Kriegsparteien geschlagen haben. Pro-russische Hacktivisten-Gruppen wie KillNet wählen die Zielobjekte und -länder auf der Grundlage der Unterstützung, die sie der Ukraine gewähren, oder der Sanktionen, die sie gegen Russland verhängen, aus. Im Zusammenhang mit dem Krieg in der Ukraine war der Schaden dieser Angriffe bislang marginal und bestand hauptsächlich aus Reputationsschäden.

So führten beispielsweise die DDoS-Angriffe auf die Websites von Flughäfen in den USA durch KillNet im Oktober 2022[50] zu einer vorübergehenden Unterbrechung der Verfügbarkeit mehrerer Flughafen-Websites, so dass sich Passagiere beispielsweise nicht dort über den aktuellen Status ihres Fluges informieren konnten. Die Angriffe hatten jedoch keine Auswirkungen auf die operativen Tätigkeiten der betroffenen Flughäfen.

---

47 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua); Preparing for a Russian cyber offensive against Ukraine this winter (microsoft.com)

48 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua)

49 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

50 Coverage of Killnet DDoS attacks plays into attackers' hands, experts say (therecord.media)

5.6.2.2 Verbreitung von Schadsoftware

Während des Berichtszeitraums wurde über zahlreiche Kampagnen zur Verbreitung von Schadsoftware berichtet, die sich hauptsächlich gegen ukrainische Institutionen richteten.[51] Diese Kampagnen zielen darauf ab, einen Zugriff auf Systeme zu erlangen, indem sie diese mit Schadsoftware infizieren. Im Krieg wird dieser Zugriff dann vor allem für Spionage (Diebstahl von Informationen) oder Sabotage (Störung der Systemfunktion) genutzt. Die Schadsoftware wird oft über ein E-Mail zugestellt, welches die Identität offizieller Stellen vortäuscht. Dies, verbunden mit einem aktuellen Thema, soll die Empfänger zu einer Handlung verleiten, die notwendig ist, um das Zielsystem zu infizieren. Eine weitere beobachtete Vorgehensweise ist die Erstellung von gefälschten Webseiten, die die Identität offizieller Stellen annehmen und auf denen die Schadsoftware in einem Programm versteckt ist, das der Benutzer installieren soll. Schliesslich kann Schadsoftware auch durch die Ausnutzung von Schwachstellen in einem System verbreitet werden. In diesem Fall ist die Interaktion eines Nutzers des Zielsystems in der Regel nicht erforderlich. Die Auswirkungen solcher Kampagnen sind sehr unterschiedlich und hängen vom Schadsoftware-Typ und dem infizierten System ab. In einem vereinfachten Beispiel wird eine Schadsoftware, die Informationen vom Computer eines Studenten in einer Schule stiehlt, höchstwahrscheinlich weniger gravierende Auswirkungen haben als eine Schadsoftware, welche auf dem System eines Spitals den Betrieb stört.

So wurde beispielsweise im Juli 2022 die Schadsoftware «GammaLoad» an ukrainische Behörden verteilt. Diese Kampagne wird der russischen Advanced Persistent Threat (APT) Gruppe Gamaredon zugeschrieben.[52] Bei dieser Kampagne wurde die Schadsoftware «GammaLoad» als vermeintliches Informationsblatt im Anhang von E-Mails verbreitet, die die Identität der Nationalen Akademie für Sicherheitsdienste der Ukraine vortäuschten. Sobald das Zielsystem mit «GammaLoad» infiziert ist, kann die Gamaredon-Gruppe Informationen extrahieren oder zusätzliche Schadsoftware mit weiteren Funktionen, z. B. für Sabotagezwecke, auf das System laden.

In einem weiteren Fall wurden im Oktober 2022 drei Transport- und Logistikunternehmen in der Ukraine und Polen innerhalb weniger Stunden mit der Ransomware «Prestige» infiziert.[53] Diese Ransomware wird der russischen Advanced Persistent Threat (APT) Gruppe Sandworm zugeschrieben. Ein Ransomware-Vorfall kann den Betrieb der betroffenen Unternehmen beeinträchtigen, was sich z. B. vorliegend auf den Transport von Gütern hätte auswirken können. Der Erfolg dieses Angriffs konnte jedoch durch eine schnelle Reaktion eingegrenzt werden.

5.6.3 Zukünftige Entwicklungen

Es gibt derzeit keine Anzeichen dafür, dass die Aktivitäten im Cyberraum im Zusammenhang mit dem Krieg in der Ukraine abnehmen würden. Solange der Krieg andauert, wird Russland höchstwahrscheinlich weiterhin Angriffe in dieser Dimension durchführen und jede Gelegenheit nutzen, um gewünschte Effekte zu erzielen, ob in Kombination mit Aktivitäten in anderen Operationssphären oder nicht.

---

51 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

52 Кібератаки групи UAC-0010 (Armageddon) з використанням шкідливої програми GammaLoad.PS1_v2 (CERT-UA#5003,5013,5069,5071) (cert.gov.ua)

53 New “Prestige” ransomware impacts organizations in Ukraine and Poland (microsoft.com)