6. Mai 2024 | Bundesamt für Cybersicherheit BACS

Halbjahresbericht 2023/II (Juli – Dezember)

Informationssicherung

Lage in der Schweiz und International

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Übersicht / Inhalt

Management Summary

Das Nationale Zentrum für Cybersicherheit (NCSC) wurde per 1. Januar 2024 ins Bundesamt für Cybersicherheit (BACS) überführt. Das BACS nimmt diese Transformation zum Anlass, im Fokusthema die verschiedenen Tätigkeitsfelder des Bundes im Bereich Cybersicherheit aufzuzeigen. In zwei Gastbeiträgen werden die Herausforderungen in der Strafverfolgung und bei der Zertifizierung der Cybersicherheit von Gemeinden beleuchtet.

Zunahme der Meldungen im zweiten Halbjahr 2023

Im zweiten Halbjahr 2023 sind beim damaligen NCSC 30’331 Meldungen zu Cybervorfällen eingegangen. Dies entspricht nahezu einer Verdoppelung im Vergleich zum zweiten Halbjahr 2022 (16’951 Meldungen). Zurückzuführen ist diese Zunahme in erster Linie auf betrügerische Stellenangebote und auf vermeintliche Anrufe der Polizei.

Meldungen zu Betrug gehörten auch im zweiten Halbjahr zu den meistgemeldeten Cybervorfällen beim NCSC. Die von Unternehmen gemeldeten Betrugsversuche fallen meist in die Kategorie «CEO-Betrug» mit 253 Meldungen (Vorjahresperiode: 190 Meldungen) und die Kategorie «Rechnungsmanipulationsbetrug» mit 63 Meldungen (Vorjahresperiode: 45 Meldungen) und erlebten eine kleine Zunahme. Rückläufig waren hingegen die gemeldeten Ransomware-Angriffe auf Unternehmen. Im zweiten Halbjahr 2022 gingen beim NCSC 54 Meldungen ein, in der aktuellen Berichtsperiode waren es 42 Meldungen.

Betrugsversuche mit Künstlicher Intelligenz

In der Berichtsperiode hat das NCSC vermehrt Meldungen zu Betrugsversuchen erhalten, bei denen Künstliche Intelligenz (KI) zum Einsatz kam. Bei den Meldungen handelte es sich u. a. um Sextortion mit KI-generierten Bildern, um Telefonanrufe und um Investitionsbetrug im Namen von prominenten Persönlichkeiten. Aufgrund der vergleichsweise geringen Zahl von Meldungen in diesem Bereich dürfte es sich nach Einschätzung des NCSC um erste Versuche der Cyberkriminellen handeln, mit denen sie ausloten wollen, wie sich KI künftig gewinnbringend für Cyberangriffe einsetzen lässt.

Phishing nach wie vor das am zweithäufigsten gemeldete Phänomen

Im Vergleich zur Vorjahresperiode kam es bei den Meldungen zu Phishing zu mehr als einer Verdoppelung, von 2'179 Meldungen auf 5'536 Meldungen. Besonders erwähnenswert ist das so genannte «Chain Phishing»: Über gehackte E-Mail-Postfächer versenden Phisher E-Mails an alle in diesem Postfach gespeicherten Adressen. Da der Absender den Empfängern bekannt sein dürfte, ist die Wahrscheinlichkeit gross, dass diese auf das Phishing hereinfallen. Danach werden über das gephishte E-Mail-Konto wiederum alle darin vorhandenen Kontakte angeschrieben.

Editorial

Das Bundesamt für Cybersicherheit: Stärkung der Schweizer Cybersicherheit

Seit dem 1. Januar 2024 ist die Überführung des Nationalen Zentrums für Cybersicherheit (NCSC) im Eidgenössischen Finanzdepartement (EFD) in das Bundesamt für Cybersicherheit (BACS) im Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) vollzogen.

Der Kernauftrag bleibt auch als Bundesamt unverändert: Es schützt die Schweiz präventiv vor Cyberrisiken, unterstützt bei Cybervorfällen und identifiziert Chancen, um die Schweiz strategisch im Cyberraum gut zu positionieren. Oberstes Ziel dabei ist es, Organisationen und Personen zu befähigen, Cyberrisiken zu verstehen und nach der eigenen Risikobereitschaft die Cybersicherheit zu gestalten. Dafür etabliert das BACS mit seinen Partnern ökonomische und zivilgesellschaftliche Mechanismen, die einerseits systemische Risiken senken und andererseits die Kosten, um Cyberrisiken zu adressieren, möglichst tief halten. Dadurch wird die Schweiz für Unternehmen, die sich im digitalen Raum bewegen ein attraktiver Standort.

Einige der aktuellen Herausforderungen in der Schweizer Cybersicherheit sind die hohe Verwundbarkeit von IT-Systemen, eine noch schwach ausgeprägte Reaktionsfähigkeit bei systemrelevanten Cybervorfällen und -krisen sowie eine oft mangelnde Transparenz und fehlende Daten, um Aussagen von Experten und Organisationen zur Cybersicherheit einzuordnen und kritisch zu hinterfragen. Diese Risikofaktoren führen dazu, dass Cyberangriffe zu oft erfolgreich sind, was sich wiederum in hohen wirtschaftlichen Schäden und einem hohen Risiko von Ausfällen bei kritischen Infrastrukturen niederschlägt. Die Meldungen zu Cybervorfällen mit Schadensfolge steigern sich im Schnitt jährlich um ca. 30%. Während die Situation dramatisch klingt, muss man aber auch einordnen, dass in Anbetracht der immer stärkeren Nutzung des digitalen Raums diese Zahlen durchaus nachvollziehbar sind. Im internationalen Vergleich befindet sich die Schweiz im Mittelfeld. Man muss die Lage aber ernst nehmen und verbessern. Dafür fokussiert sich das BACS auf vier strategische Bereiche. Diese sind: Cyberbedrohungen verständlich machen, Mittel zu Verhinderung von Cyberangriffen zur Verfügung stellen, Schäden aus Vorfällen reduzieren und die Sicherheit von digitalen Produkten und Dienstleistungen erhöhen. Was dies konkret heisst, können Sie in der neu publizierten Strategie des BACS nachlesen.

Ein zentraler Erfolgsfaktor für das BACS sind seine Mitarbeitenden. Das BACS möchte ein attraktiver Arbeitgeber sein, um Mitarbeitende zu haben und neue Talente zu gewinnen, welche die Leistungen und Produkte des BACS möglichst effizient und qualitativ hochwertig auf die Bedürfnisse von Politik, Wirtschaft und Zivilgesellschaft ausrichten. Um dies zu erreichen, muss das BACS flexibel sein und seine Organisation rasch auf neue Anforderungen und ökonomische Realitäten ausrichten. Dies geht nur, wenn seine Teams möglichst autonom agieren können und Entscheidungen von den Mitarbeitenden, welche das notwendige Fachwissen haben, möglichst selbständig getroffen oder zumindest signifikant beeinflusst werden können. Oft müssen solche Entscheide schnell getroffen werden, was wiederum eine offene und sachliche Fehlerkultur ermöglicht. Es ist mir lieber, wir machen kontrolliert Fehler und sind innovativ, als wenn wir keine Fehler machen und uns nicht bewegen. Umso wichtiger ist es aber auch, die «Operational Excellence» hoch zu halten und verlässliche und konsistente Ergebnisse zu liefern. Der Kern all dessen ist eine möglichst diverse Belegschaft, die sich selber und

die Amtsleitung immer wieder konstruktiv hinterfragt. Wir sind noch nicht ganz bei diesem Idealbild. Wir haben aber wichtige Schritte in diese Richtung gemacht, was sich auch darin niederschlägt, dass unsere Mitarbeitenden meiner Einschätzung nach gute Arbeit leisten.

Es ist uns wichtig, dass Sie uns, liebe Leserinnen und Leser, Feedback geben und insbesondere auch konstruktive Kritik üben, wenn das BACS Ihre Erwartungen nicht erfüllt. In dieser wichtigen Phase der Entwicklung des Bundesamtes sind wir mehr denn je darauf angewiesen. Schliesslich wollen wir gemeinsam mit Ihnen einen freien, sicheren Cyberraum zum Wohle aller gestalten.

Florian Schütz, Direktor Bundesamt für Cybersicherheit

1 Fokus: Herausforderungen in der Cybersicherheit

Die Cybersicherheit und damit der Schutz der Schweiz vor Cyberrisiken ist eine gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat. Alle Beteiligten sind gefordert, in ihrem Zuständigkeits- und Einflussbereich angemessene Massnahmen zu ergreifen.

Wie in vielen Bereichen gilt auch bei der Cybersicherheit in erster Linie das Prinzip der Selbstverantwortung. Es gibt jedoch Herausforderungen, die die Fähigkeiten und Möglichkeiten von Privatpersonen und Organisationen übersteigen und bei denen der Staat unterstützen soll oder gewisse Aufgaben übernehmen muss.

Mit dem Nationalen Zentrum für Cybersicherheit (NCSC[1]), dem heutigen Bundesamt für Cybersicherheit (BACS), das als Kompetenzzentrum des Bundes für Cybersicherheit fungiert, hat der Bundesrat eine Struktur geschaffen, mit der verschiedene Herausforderungen in der Cybersicherheit von staatlicher Seite angegangen werden können.

1.1 Cyberbedrohungen (er)kennen und darüber informieren

Um zu wissen, worauf geachtet werden muss und was für Massnahmen getroffen werden sollen, ist es wichtig, aktuelle Phänomene zu kennen. Informationen darüber, was gerade passiert und was für Entwicklungen im Gange sind, helfen bei der Einschätzung von Risiken und beim Treffen von Entscheidungen. Das BACS hat aufgrund von Meldungen aus der Bevölkerung und von Unternehmen (vgl. Kap. 1.5 und Kap. 2), den Kontakten zu Betreiberinnen kritischer Infrastrukturen (vgl. Kap. 1.6) und einem nationalen wie auch internationalen Netzwerk von Partnerorganisationen eine gute Übersicht auf aktuelle Ereignisse und Bedrohungsformen.

Diese Lageinformationen bereitet das BACS zielgruppengerecht auf und versorgt entsprechend verschiedene Empfängerkreise mit den für sie relevanten Informationen zur Sensibilisierung (vgl. Kap. 1.2) und für das Ergreifen von Massnahmen zu ihrem Schutz (vgl. Kap. 1.3 und 1.5).

Empfehlungen:

Lesen Sie bisherige Halbjahresberichte und besuchen Sie regelmässig die BACS-Website.

Auch auf anderen Websites wie cybercrimepolice.ch und eBanking – aber sicher! (ebas.ch) finden Sie Informationen über aktuelle Phänomene, Bedrohungen und Schutzmassnahmen.

[1] National Cyber Security Centre, vgl. Finnland: NCSC-FI (kyberturvallisuuskeskus.fi); Irland: National Cyber Security Centre (ncsc.gov.ie); Lettland: National Cyber Security Centre (nksc.lt); Niederlande: National Cyber Security Centre (ncsc.nl), Norwegen: Norwegian National Cyber Security Centre (nsm.no) und Vereinigtes Königreich: National Cyber Security Centre (ncsc.gov.uk). Einige Länder haben eigene spezifische Bezeichnungen für entsprechende Einheiten, wie Deutschland: BSI - Bundesamt für Sicherheit in der Informationstechnik (bsi.bund.de); Frankreich: ANSSI - Agence nationale de la sécurité des systèmes d'information (cyber.gouv.fr) oder die USA: Cybersecurity & Infrastructure Security Agency – America's Cyber Defense Agency (cisa.gov). Australien und Kanada betonen derweil ihr Land im Titel: Australian Cyber Security Centre ACSC (cyber.gov.au) beziehungsweise Canadian Centre for Cyber Security CCCS (cyber.gc.ca). Siehe auch Centre for Cyber security Belgium (belgium.be) sowie Cyber Security Agency of Singapore (csa.gov.sg).

1.2 Sensibilisierung

Sensibilisierungs- und Präventionsmassnahmen sind in der Cybersicherheit elementar, da die Bewältigung eines Cybervorfalls viel aufwändiger ist als etwa die Umsetzung weniger und einfach anzuwendender Massnahmen, mit denen sich jede und jeder sicher im digitalen Raum bewegen kann. Deshalb veröffentlicht das BACS Informationen zur Cybersicherheit sowie Empfehlungen präventiver Massnahmen gegen Cyberangriffe. Für die Nationale Cyberstrategie (NCS) wurden mit Vertretern aus Wirtschaft, Behörden, Bevölkerung und Bildungsinstitutionen Ansätze erarbeitet, mit denen einerseits über die Thematik informiert und sensibilisiert wird. Andererseits werden zielgruppenorientiert Handlungsempfehlungen erarbeitet, wonach Personen und Organisationen selbst Massnahmen zu ihrem Schutz ergreifen können.

Zur bedarfsgerechten Erfüllung dieser Aufgabe kann das BACS zum einen auf eigene Erkenntnisse aus seinen operativen Tätigkeiten zurückgreifen. Zum andern koordiniert es die Anstrengungen zur Verbesserung der Cyberresilienz schweizweit. Es konzipiert in enger Zusammenarbeit mit externen Partnern wie der Schweizerischen Kriminalprävention, der Plattform «e-banking – aber sicher!» der Hochschule Luzern, der Swiss Internet Security Alliance und weiteren bestehenden Gremien und Organisationen Massnahmen. Diese Massnahmen und Empfehlungen können durch die einzelnen definierten Zielgruppen, die in ihrer Gesamtheit die Öffentlichkeit ausmachen, in Eigenverantwortung und gemäss ihrer Betroffenheit umgesetzt werden.

So werden beispielsweise in der Wirtschaft Pilotprojekte durchgeführt, etwa in der Logistikbranche, der metallverarbeitenden Industrie oder in Familienunternehmen. Die daraus resultierenden Erkenntnisse werden in der Folge idealerweise mit den entsprechenden Branchenverbänden diskutiert, weiterentwickelt und den jeweiligen Wirtschaftssektoren zur Verfügung gestellt. Für die Bevölkerung realisiert das BACS zusammen mit externen Partnern landesweite Kampagnen. Diese bringen cybersicherheitsrelevante Inhalte der breiten Bevölkerung näher und sollen jeder Nutzerin und jedem Nutzer des Internets und digitaler Geräte einfach anzuwendende Hilfsmittel zur Verfügung stellen, mit deren Anwendung sie vor Cyberkriminalität geschützt online unterwegs sind. Alle Anstrengungen werden laufend ausgewertet und überprüft, damit sie hinsichtlich ihrer Realisierung und Wirksamkeit optimiert werden können.

Empfehlungen:

Erkundigen Sie sich regelmässig über aktuelle Ereignisse, die Ihre Cybersicherheit oder diejenige Ihres Unternehmens beeinträchtigen können. Auf den Websites des BACS, der Schweizerischen Kriminalprävention SKP, «eBanking – aber sicher!», der Plattform für Internetsicherheit iBarry oder der Präventionskampagne s-u-p-e-r.ch finden Sie zahlreiche Informationen für Privatpersonen, Unternehmen, Behörden und IT-Spezialisten.

Sprechen Sie mit Mitarbeitenden, Verwandten und Bekannten über Cybersicherheit, den Umgang mit Daten und Cyberkriminalität.

1.3 Anleitung zum Schutz und zur Erhöhung der Resilienz geben

Das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat in Zusammenarbeit mit dem BACS und der Wirtschaft den IKT-Minimalstandard entwickelt, um Unternehmen systematische Anleitungen zur Verfügung zu stellen, wie sie ihre Cybersicherheit ausgestalten können. Der IKT-Minimalstandard fasst verschiedene international anerkannte Standards zusammen und soll als Empfehlung zur Verbesserung der IKT-Resilienz beitragen. Der Standard sowie das dazugehörige Assessment-Tool werden regelmässig aktualisiert.

Für verschiedene kritische Sektoren wurden zusammen mit Branchenverbänden und Sektorvertretenden Branchenstandards erarbeitet und publiziert, um sektorspezifischen Anforderungen besser gerecht zu werden. Auch diese haben grundsätzlich empfehlenden Charakter.

Bei gewissen Sektoren wurden Aspekte des IKT-Minimalstandards vorgeschrieben. So hat zum Beispiel das Bundesamt für Energie (BFE) die IKT-Minimalstandards für die Strom- und Gasversorgung als verpflichtend erklärt. Die Verpflichtung gilt bei Strom ab 2024 und bei Gas ab 2025. Ähnlich hat das Bundesamt für Verkehr (BAV) im Herbst 2023 die Richtlinie Cybersicherheit Eisenbahn (RL CySec-Rail) publiziert. Die neue Richtlinie beschreibt die minimalen Anforderungen an ein Managementsystem für Informationssicherheit (ISMS), welches die Eisenbahnunternehmen aufzubauen und zu pflegen haben. Die RL CySec-Rail, die am 1. Juli 2024 in Kraft gesetzt wird, nimmt Bezug zum «IKT-Minimalstandard öffentlicher Verkehr», welcher seit 2020 publiziert ist.[2]

Das BACS unterstützt seinerseits mit Anleitungen und Empfehlungen zu verschiedenen Themen wie beispielsweise Webseitensicherheit[3], Schutz von industriellen Kontrollsystemen[4] und Geräten des «Internet of Things»[5] oder zur Zusammenarbeit mit IT-Providern[6].

Schlussfolgerung / Empfehlung:

Auf der Website des BACS finden Sie zahlreiche Informationen zu Cybersicherheit.

Die vom Bundesamt für wirtschaftliche Landesversorgung (BWL) in Zusammenarbeit mit der Wirtschaft erarbeiteten IKT-Minimalstandards und IKT-Branchenstandards dienen als Empfehlung und Orientierungspunkte, um sich gegen Bedrohungen von Cyberrisiken zu schützen.

1.4 Label cyber-safe.ch – Erfahrungen einer Waadtländer Gemeinde

Gastbeitrag von Kilian Cuche, Gemeinderat in Pomy/VD

Die 900 Einwohnerinnen und Einwohner zählende Gemeinde Pomy im Bezirk Waadtländer Jura-Nord hat Ende 2023 nach rund zweieinhalb Jahren Arbeit das Schweizer Cybersicherheitslabel cyber-safe.ch erlangt. Dieser Artikel soll den Prozess von der Aufnahme des Ist-

---

2 Richtlinie zur Cybersicherheit (bav.admin.ch)

3 Massnahmen zum Schutz von CMS (ncsc.admin.ch);
Massnahmen zum Schutz vor DDoS-Angriffen (ncsc.admin.ch)

4 Massnahmen zum Schutz von ICS (ncsc.admin.ch)

5 Massnahmen zum Schutz von IOT Geräten (ncsc.admin.ch)

6 Empfehlungen für die Zusammenarbeit mit IT-Providern (ncsc.admin.ch)

Zustands bis zum Nutzen der Umsetzung aufzeigen sowie die Herausforderungen und Chancen für Gemeinden beleuchten.

1.4.1 Weg zur Awareness für Cybersicherheit

2021, nach einem Anlass des Waadtländer Gemeindeverbandes (UCV) zum Thema Cybersicherheit, entstand die Idee, den Ist-Zustand der Cybersicherheit der Gemeinde Pomy zu ermitteln und Verbesserungen einzuführen. An der Konferenz wurde das Label cyber-safe.ch vorgestellt, was uns als Ausgangspunkt diente. Natürlich musste zuerst der ganze Gemeinderat davon überzeugt werden, in die Cybersicherheit zu investieren. Dazu zeigte uns der Verband cyber-safe.ch auf Grundlage eines ersten Fragebogens auf, welche Kosten uns unter Berücksichtigung des Umfangs unserer Infrastruktur und unserer Daten bei einem Cyberangriff entstehen könnten. Dieser Bericht war sehr nützlich, da er das Kosten-Nutzen-Verhältnis einer Investition in die Cybersicherheit deutlich machte. Die Gemeinde Pomy war schnell von der Notwendigkeit der Investitionen überzeugt und startete den Prozess zur Erlangung des Labels im Frühling 2021. Der Cyberangriff auf die Gemeinde Rolle einige Monate später bewirkte, dass unser Wille zur Verbesserung der Cybersicherheit der Gemeinde noch stärker wurde.

1.4.2 Prozess zur Erlangung des Labels cyber-safe.ch

Der erste Schritt zur Erlangung des Labels cyber-safe.ch bestand in einem Bericht, der auf der Grundlage von Fragebögen, Phishing-Tests sowie einer Analyse unserer Informatikinfrastruktur (Scan zum Aufspüren von Sicherheitslücken) erstellt wurde. Mit diesem Bericht wurde der Ist-Zustand der Cybersicherheit der Gemeinde ermittelt und es wurden prioritäre Massnahmen identifiziert, die als Voraussetzungen für das Label umzusetzen waren. Anders ausgedrückt, erhielten wir eine Liste der erfüllten und nicht erfüllten Punkte, anhand der wir einen Aktionsplan für die Vorbereitung der Zertifizierung erstellen konnten. Danach erfolgte der wichtigste Teil der Arbeit: die Umsetzung der Korrekturmassnahmen. Von der Verwaltung der Updates über die Kontrolle der Backups, die Schulung der Benutzerinnen und Benutzer bis hin zur physischen Sicherung unserer Infrastruktur wurden alle wesentlichen Elemente der Cybersicherheit unter die Lupe genommen, überprüft, angepasst und korrigiert. Zwei Jahre später durchliefen wir ein erstes Audit, bei dem noch einige nicht erfüllte Punkte gefunden wurden. Wir arbeiteten anschliessend an deren Behebung und erlangten schliesslich, nach einem zweiten Audit, die Zertifizierung cyber-safe.ch.

1.4.3 Nutzen, Herausforderungen und Chancen für Gemeinden

Das Label cyber-safe.ch war für uns ein ausgezeichnetes Instrument zur Verbesserung der Cybersicherheit. Ein von unserer Verwaltung und unserem Informatikdienstleister unabhängiger Blick auf unsere Infrastruktur ermöglichte es, das Verbesserungspotenzial umfassend und vollständig zu erkennen. Wir wurden professionell und auch mit einem Verständnis für die Herausforderungen kleiner Gemeinden begleitet. Dazu gehört insbesondere die Tatsache, dass unser Gemeinderat ausschliesslich aus Milizpolitikern besteht, die hinsichtlich Zeit, Kompetenzen, aber auch Kenntnissen im Bereich der Cybersicherheit ihre Grenzen haben. Das alles konnte berücksichtigt werden und so wurde eine auf unseren besonderen Kontext zugeschnittene Lösung gefunden. Es ist auch erfreulich zu sehen, dass mehrere Kantone den Ge-

meinden zunehmend Mittel zur Verfügung stellen, um sie bei der Verbesserung der Cybersicherheit zu unterstützen. Diese Bemühungen sollten auf gesamtschweizerischer Ebene ausgebaut und koordiniert werden.

1.4.4 Fazit

Obwohl unsere Infrastruktur mit zwei Arbeitsplätzen, einem Server und einigen BYOD[7]-Geräten sehr klein ist, ist der Arbeitsaufwand für die Erlangung eines Cybersicherheitslabels wie cyber-safe.ch nicht zu unterschätzen. Der grösste Teil der Massnahmen ist nämlich vom Umfang der Infrastruktur unabhängig. Die Verantwortlichen für das Label konnten uns jedoch pragmatisch begleiten, sich unseren Bedürfnissen sowie den verschiedenen Realitäten vor Ort anpassen. Das Label zu erlangen, ist also keine «Mission Impossible». Mit einer guten Begleitung, einem Change-Management gegenüber den Mitarbeitenden sowie der Unterstützung der Informatikdienstleister ist eine Verbesserung der Cybersicherheit für alle Schweizer Gemeinden möglich und sollte Teil einer jeden kommunalen Informatikplanung sein. Schliesslich geht es um die Sicherheit der Daten unserer Bürgerinnen und Bürger sowie um den Schutz der kritischen Infrastrukturen in der Verantwortung der Gemeinden.

1.5 Vorfälle registrieren und Empfehlungen an Betroffene abgeben

Das BACS nimmt Meldungen zu Cybervorfällen und Cyberbedrohungen entgegen. Es betreibt zu diesem Zweck eine nationale Anlaufstelle für Cyberbedrohungen. Diese kategorisiert die eingegangenen Meldungen und führt eine erste Analyse durch, auf deren Grundlage Massnahmen ergriffen und weitere vertiefende Untersuchungen durchgeführt werden können. Melderinnen und Melder sollen möglichst rasch, unkompliziert und kompetent unterstützt werden, indem ihre Fragen direkt beantwortet werden. Sie erhalten ausserdem Empfehlungen für die weitere Vorgehensweise und/oder werden an die zuständigen Stellen verwiesen. Als nationaler und zentraler Ansprechpartner für Meldungen und Fragen im Bereich Cyber arbeitet das BACS eng mit Akteuren aus Bund, Kantonen, Strafverfolgung aber auch privaten Partnern wie beispielsweise Internetanbietern sowie mit internationalen Partnern und Organisationen zusammen. Darüber hinaus stellt das BACS sicher, dass betrügerische Websites, E-Mail-Adressen, Telefonnummern usw. an die zuständigen Stellen weitergeleitet werden, damit diese ihrerseits Massnahmen ergreifen können.

Anhand der eingegangenen Meldungen erkennt das BACS neue Trends und Vorgehensweisen im Cyberbereich. Die aus den Meldungen erhaltene Fallübersicht vervollständigt den Überblick über die aktuelle Cyberlage (vgl. Kap. 1.1). Die Entwicklung dieser Phänomene wird laufend analysiert, damit Bevölkerung und Unternehmen bei zunehmender Bedrohung gewarnt werden können. Die erhobenen Zahlen sind eine wichtige Grundlage für die Prävention und für die Sensibilisierung der Öffentlichkeit im Umgang mit Cyberrisiken (vgl. Kap. 1.2). Durch die daraus gewonnenen Erkenntnisse können mitunter zukünftige Delikte verhindert und weitere Geschädigte vermieden werden.

[7] BYOD steht für «bring your own device», vgl. Bring your own device (wikipedia.org)

Empfehlungen:

Helfen Sie mit, Gefahren im Internet zu erkennen und melden Sie Vorfälle und Cyberbedrohungen beim BACS über das Meldeformular: NCSC Report (ncsc.admin.ch)

1.6 Kritische Infrastrukturen schützen und unterstützen

Kritische Infrastrukturen sind Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind. Das BACS unterstützt Betreiberinnen kritischer Infrastrukturen in der Schweiz beim Schutz vor Cyberbedrohungen und damit bei der Minimierung von Cyberrisiken. Dazu betreibt es ein nationales Einsatzteam für Computersicherheit (Computer Emergency Response Team [CERT]), das als nationale Fachstelle für die technische Bewältigung von Cybervorfällen und die technische Analyse von Cyberbedrohungen fungiert.

Das BACS stellt den Betreiberinnen kritischer Infrastrukturen Werkzeuge und Datensätze zur Verfügung, welche die Cybersicherheit der Infrastruktur sowie ihrer Nutzerinnen und Nutzer erhöht. Dazu zählen beispielsweise technische Informationen zu IT-Infrastrukturen, welche für die Verbreitung von Schadsoftware (sogenannter «Malware») oder das Betreiben von Phishing-Webseiten missbraucht werden.

1.7 Verwundbarkeiten reduzieren

Software und/oder Konfigurationen von Systemen können Schwachstellen aufweisen, die von Angreifern ausgenützt werden, um sich unbefugt Zugriff zu verschaffen. Um die Angriffsfläche zu reduzieren und Vorfällen vorzubeugen, müssen solche Verwundbarkeiten gefunden und rasch behoben werden.

Das BACS erhält von Partnern und über verschiedene interne und externe Quellen täglich Hinweise zu Schwachstellen im Bereich von IT-Systemen. Diese Informationen prüft es sorgfältig und leitet aus den einzelnen Meldungen nach erfolgter Analyse die erforderlichen Massnahmen für die bundeseigenen Systeme sowie für externe Stellen ab. Das BACS verfügt beispielsweise über die Möglichkeit, Betreiber kritischer Infrastrukturen über die eigene Informationsplattform vor bestimmten Sicherheitslücken zu warnen und relevante Sicherheitshinweise zu publizieren. Oftmals informiert das BACS zudem betroffene Unternehmen auch direkt per E-Mail, per Telefon oder auch via eingeschriebenen Brief. In vielen Fällen gelingt es so, in Zusammenarbeit mit den betroffenen Unternehmen Schwachstellen rechtzeitig zu schliessen.

Das BACS ist zudem die offizielle Anlaufstelle zum Melden von Sicherheitslücken in der Schweiz und von MITRE[8] als Autorisierungsstelle für die Vergabe von CVE-Nummern aner-

[8] Solving Problems for a Safer World (mitre.org)

kannt. In dieser Funktion stellt das BACS für die ihm gemeldeten Schwachstellen die koordinierte Veröffentlichung sicher und leistet damit einen wichtigen Beitrag, damit das Ausnutzen dieser Schwachstellen möglichst vermieden werden kann.[9]

Sensibilisierungsmassnahmen tragen ebenfalls dazu bei, die Angriffsfläche zu reduzieren. Das BACS ermutigt beispielsweise Unternehmen, Organisationen und Verwaltungen in der Schweiz, den Sicherheitsstandard des security.txt umzusetzen[10] und so einen wesentlichen Beitrag zur Cybersicherheit zu leisten.

Um die Cybersicherheit der bundeseigenen IT-Infrastruktur zu erhöhen sowie Cyberrisiken zu senken, ist das BACS auch zuständig für den Betrieb des eigenen Bug-Bounty-Programms. Bug-Bounty-Programme dienen ergänzend zu anderen Sicherheitsmassnahmen dazu, allfällige Verwundbarkeiten in IT-Systemen und in Anwendungen in Zusammenarbeit mit ethischen Hackern zu identifizieren, zu dokumentieren und zu beheben.

Empfehlungen:

Aktualisieren Sie Ihre installierten Apps und Programme umgehend, wenn Updates zur Verfügung stehen. Aktivieren Sie wo möglich die automatische Update-Funktion.

Beachten Sie den Lebenszyklus von Geräten und Software und ersetzen Sie diese, wenn sie vom Hersteller nicht mehr mit Sicherheits-Updates versorgt werden.

Für Unternehmen: Führen Sie ein aktuelles Inventar der installierten Hard- und Software und stellen Sie sicher, dass Sie Informationen über Schwachstellen und Updates erhalten.

1.8 Strafverfolgung von Cybercrime

Gastbeitrag von Serdar Günal Rütsche, Leiter Netzwerk Ermittlungsunterstützung in der digitalen Kriminalitätsbekämpfung (NEDIK)

Ransomware stellt derzeit die mit Abstand grösste Bedrohung im Bereich der Cyberkriminalität in der Schweiz dar. Obwohl wir in der Schweiz eigentlich sehr gut geschützt sind, bieten alle Unternehmen und Privatpersonen, die Internetdienste nutzen, eine Angriffsfläche für solche Angriffe. Die Digitalisierung eröffnet der Wirtschaft neue Wachstumschancen und Beschäftigungsmöglichkeiten. Gleichzeitig erfordert sie neue Prozesse und führt zu einer grösseren Abhängigkeit von einer funktionierenden Informations- und Kommunikationstechnik. Diese Abhängigkeiten machen sich auch Kriminelle zunutze. Um sich Zugang zu Netzwerken zu verschaffen, Daten zu stehlen oder ganze Systeme lahm zu legen, wenden Kriminelle immer raffiniertere Methoden an. Vom kleinen Handwerksbetrieb bis zur Grossfirma: Ein Cyberangriff kann für Unternehmen zur existenziellen Bedrohung werden.

Die Anzahl gemeldeter Straftaten im Bereich Cybercrime und digitalisierte Kriminalität stieg im Jahr 2023 stark an. Vor allem der Bereich der Cyberwirtschaftskriminalität ist von diesem signifikanten Wachstum betroffen. Bedrohungen im Cyberspace gehören zu den bedeutendsten

[9] Das NCSC ist neu Teil des weltweiten Netzwerks zur Verwaltung von Schwachstellen in Informatiksystemen (ncsc.admin.ch)

[10] Security.txt - Hinterlegen Sie Ihren Sicherheitskontakt auf Ihrer Webseite (ncsc.admin.ch)

Gefahren für Unternehmen, Behörden, Privatpersonen und kritische Infrastrukturen. Der technologische Fortschritt im Bereich der künstlichen Intelligenz eröffnet Kriminellen neue Angriffsvektoren, die für eine Vielzahl von Anwendungen genutzt werden können und somit ihr Handwerk erleichtern. Das Netzwerk Ermittlungsunterstützung in der digitalen Kriminalitätsbekämpfung (NEDIK) bekämpft als Zusammenschluss der Schweizer Polizeikorps gemeinsam die digitalisierte Kriminalität und Cybercrime. NEDIK koordiniert dabei die Fallbearbeitung, tauscht zeitnah Informationen aus, erstellt aktuelle und nationale Cyberfallübersichten, teilt Wissensgrundlagen, erarbeitet interkantonale Projekte und kooperiert dafür mit relevanten nationalen und internationalen Partnern. Dazu leisten alle Polizeikorps ihren Beitrag. Durch die Schaffung einer solchen interdisziplinären Plattform können Phänomene und Bedrohungen frühzeitig erkannt und entgegengewirkt werden. Durch die aktive Zusammenarbeit, den Aufbau neuer Kooperationspartnerschaften und die operative Präventionsarbeit soll die Kriminalität im digitalen Raum eingedämmt und die Schweizer Bevölkerung geschützt werden. NEDIK unterstützte 2023 Projekte in Schwerpunktbereichen wie beispielsweise im Online-Anlagebetrug, der Pädokriminalität und den Ausbau der Zusammenarbeit mit zivilen Marktführern.

In den kommenden Jahren wird sich im Bereich Cybercrime viel verändern. Ransomware bleibt eine zentrale Bedrohung für die Schweiz. Daher müssen wir weiterhin daran arbeiten, die Bevölkerung zu sensibilisieren. Die künstliche Intelligenz (KI) wird die Bedrohungslage signifikant verändern. Mit neuen Angriffsmöglichkeiten wie Voice Cloning oder Deepfakes erweitert KI die Fähigkeiten der Cyberkriminellen massiv. Eine KI kann allein aus einer bestehenden Malware keine völlig neue Cyberbedrohung schaffen. In Kombination mit einem Menschen ist dies jedoch möglich. Zudem werden Betrugsdelikte durch den Einsatz von KI raffinierter und massgeschneiderter. Um uns vor diesen Bedrohungen zu schützen, müssen wir weiterhin auf hochspezialisierte Sicherheitsteams und einen bewussten Umgang mit Daten setzen. Dafür müssen entsprechende Budgets bereitgestellt, Ausbildungsplätze in der Schweiz geschaffen und rechtliche Rahmenbedingungen verbessert werden. IT-Sicherheit ist keine Frage der Technik allein, sondern eine Gemeinschaftsaufgabe mit verbindlichen Kooperationen.

2 Meldungen von Unternehmen und aus der Bevölkerung

2.1 Eingegangene Meldungen zu Cybervorfällen – Überblick

Im 2023 hat die Gesamtzahl der beim NCSC und heutigem BACS eingegangenen Meldungen wiederum zugenommen. Mit 49'380 Meldungen ist die Zahl im Vergleich zum Vorjahr (34'527 Meldungen) signifikant gestiegen. Die Zunahme im zweiten Halbjahr 2023 ist verglichen mit dem Vorjahr sogar noch deutlicher. Während im zweiten Halbjahr 2022 noch 16'951 Meldungen eingegangen sind, waren es in der Berichtsperiode 30'331. Diese beinahe Verdoppelung ist vor allem auf die Zunahme der beiden Phänomene «betrügerische Stellenangebote»[11] und «gefälschte Anrufe im Namen der Polizei»[12] zurückzuführen.

Das Verhältnis der Meldungen aus der Bevölkerung (88%) zu denjenigen von Unternehmen, Vereinen und Behörden (12%) blieb weiterhin stabil. Bei den typischen von Unternehmen gemeldeten Betrugsdelikten CEO-Betrug[13] und Rechnungsmanipulationsbetrug[14] ist in der zweiten Jahreshälfte ein leichter Anstieg zu verzeichnen. Bei CEO-Betrug stieg der Meldeeingang im zweiten Halbjahr 2023 verglichen mit 2022 von 190 auf 253, beim Rechnungsmanipulationsbetrug von 45 auf 63 Meldungen. Leicht rückläufig im letzten Halbjahr war die Zahl der Meldungen über Ransomware-Angriffe[15] auf Unternehmen. Während im zweiten Halbjahr 2022 beim NCSC 54 Meldungen eingingen, waren es in der aktuellen Berichtsperiode noch 42. Stark zurückgegangen sind Meldungen über Ransomware-Angriffe auf Privatpersonen. Im zweiten Halbjahr 2023 gab es noch gerade 3 Meldungen verglichen mit 22 Meldungen in der Vorhalbjahresperiode.

11 Betrügerische Jobangebote (ncsc.admin.ch)
12 Anrufe im Namen von Fake-Behörden (Polizei, Zoll) (ncsc.admin.ch)
13 CEO-Betrug (ncsc.admin.ch)
14 Rechnungsmanipulationsbetrug (BEC-Betrug) (ncsc.admin.ch)
15 Ransomware (ncsc.admin.ch)

Meldungen an das NCSC im zweiten Halbjahr 2023 (pro Woche)

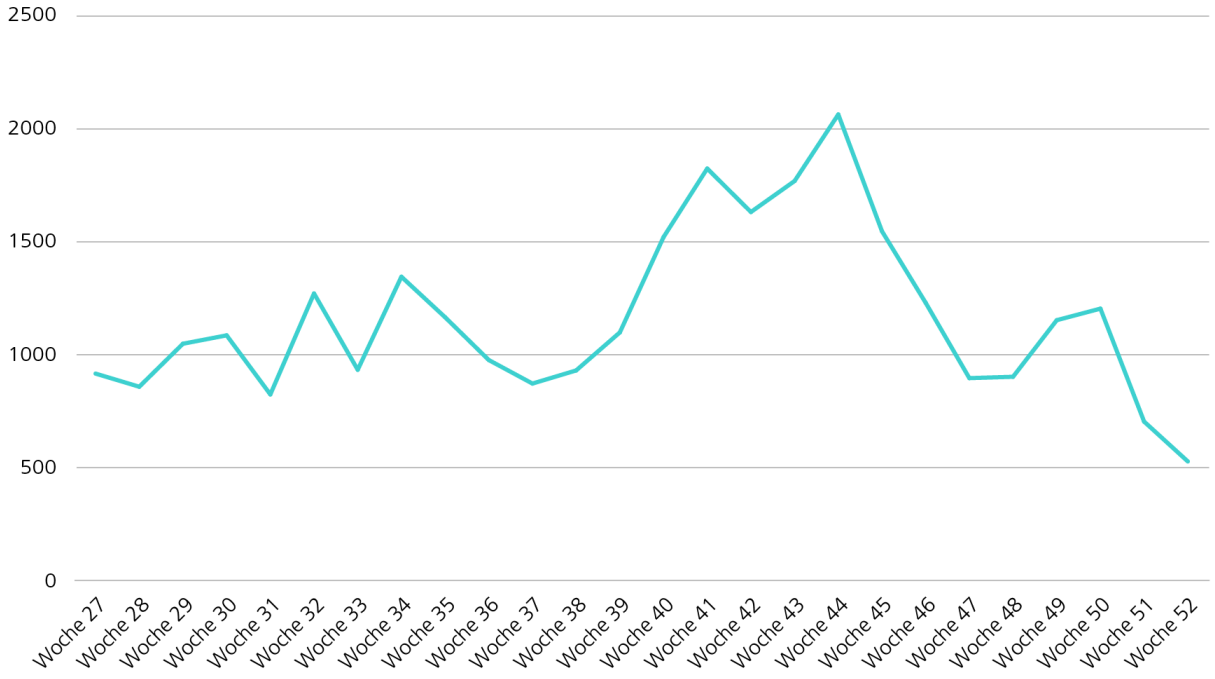

Abb. 1: Anzahl Meldungen pro Woche beim NCSC vom Juli bis Dezember 2023, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

Meldungen an das NCSC im zweiten Halbjahr 2023 (nach Kategorie)

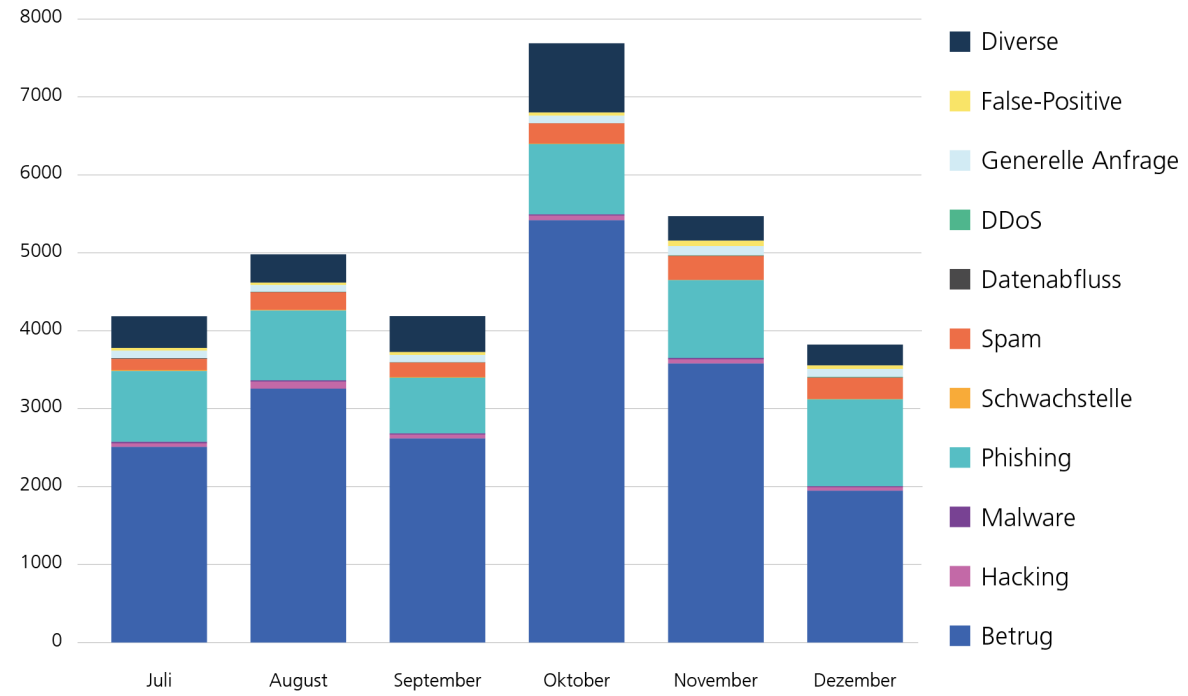

Abb. 2: Meldungen an das NCSC im zweiten Halbjahr 2023 nach Kategorien, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

2.2 Betrug

2.2.1 Betrug verursacht weiterhin die meisten Meldungen

Betrugsmeldungen sind im Jahr 2023 mit über 30’000 Meldungen nach wie vor das mit Abstand am häufigsten gemeldete Phänomen. Der Anstieg ist im zweiten Halbjahr besonders eindrücklich. Verglichen mit dem zweiten Halbjahr 2022 verdoppelte sich die Zahl der Betrugsmeldungen beinahe von 10’503 auf 19’323. Einen grossen Anteil an den Betrugsmeldungen machen wie bereits im Vorjahr Droh-E-Mails im Namen von Strafverfolgungsbehörden aus. 4’461 Meldungen gingen im zweiten Halbjahr 2023 zu diesem Thema ein. In diesen Droh-E-Mails wird behauptet, die angeschriebene Person sei eines massiven Fehlverhaltens (meist im Zusammenhang mit Kinderpornografie) überführt worden und die Anklage könne nur durch eine Geldüberweisung fallen gelassen werden.[16]

In der zweiten Jahreshälfte trat eine angepasste Vorgehensweise in den Vordergrund, die den Meldeeingang in die Höhe trieb. Die Variante startet mit einem Anruf von einer vermeintlichen Polizeibehörde. Eine computergenerierte Stimme informiert dabei die Betroffenen darüber, dass z. B. ihre persönlichen Bankkontodaten im Zusammenhang mit einer Straftat aufgetaucht seien. Für weitere Informationen soll die Ziffer 1 gedrückt werden. Drückt das Opfer die 1, wird es mit einem «Mitarbeiter» verbunden und aufgefordert, ein Fernzugriffs-Tool herunterzuladen und dem Angreifer Zugriff auf den Computer oder das Mobiltelefon zu gewähren. Die Angreifer versuchen so, Zugang zum E-Banking-Konto des Opfers zu erhalten und lösen über das Fernzugriffs-Tool im Hintergrund Zahlungen aus. Die Meldungen zu diesem Phänomen haben in der zweiten Jahreshälfte 2023 extrem zugenommen. Höhepunkt war die Kalenderwoche 44, in der das NCSC mit insgesamt 2’059 Meldungen einen Melderekord verzeichnete, wovon rund die Hälfte, 914 Meldungen, Drohanrufe betrafen.[17]

In der zweiten Jahreshälfte häuften sich auch die Meldungen über gefälschte Stellenangebote. Die Angebote vermeintlicher Personalvermittler wurden vor allem über WhatsApp verschickt. Die Kandidatinnen und Kandidaten wurden dabei mit aussergewöhnlichen Verdienstversprechen gelockt. Dazu erhielten die «Mitarbeitenden» über eine Online-Plattform eine Liste mit Aufträgen, z. B. zur Erstellung von Online-Bewertungen. Für jede Bewertung gab es dann eine bestimmte Vergütung, die über die Plattform dem Konto des Mitarbeitenden gutgeschrieben wurde. Die Anzahl der verfügbaren Aufträge sank jedoch schnell auf null. Um das Geschäft zu beschleunigen und nicht auf neue Aufträge warten zu müssen, bot die Plattform die Möglichkeit, gegen Bezahlung neue Aufträge zu generieren. So konnten für wenige Dollar 50 neue Bewertungsaufträge erworben werden. Der damit in Aussicht gestellte Gewinn, der wiederum der Plattform gutgeschrieben werden sollte, überstieg die Kosten bei weitem, so dass sich dieses Modell für den Geschädigten vermeintlich lohnte. Das böse Erwachen kam dann, als man sich den angehäuften Gewinn auszahlen lassen wollte. Um an den Gewinn zu gelangen, wurden vom Plattformbetreiber Gebühren verlangt, und zwar so lange, bis das Opfer merkte, dass es sich um einen Betrug handelte.[18]

---

16 Gefälschte Drohmails von Behörden (ncsc.admin.ch)

17 Woche 43: Firmenähnliche Strukturen bei den Fake-Support-Betrügern (ncsc.admin.ch)

18 Woche 35: Fake-Jobangebote 2.0 (ncsc.admin.ch)

2.2.2 Erste Betrugsversuche mit künstlicher Intelligenz (KI)

Künstliche Intelligenz (KI) ist im letzten Jahr zum Trendthema geworden. Spätestens mit ChatGPT ist das Thema auch bei der breiten Masse angekommen. Wie jede Technologie kann sie einerseits nutzbringend eingesetzt werden, andererseits aber auch Schaden anrichten. So ist es nicht erstaunlich, dass auch Cyberkriminelle KI für ihre Zwecke zu nutzen versuchen. Aufgrund der gemeldeten Fälle geht das BACS jedoch davon aus, dass KI noch nicht systematisch von Cyberkriminellen eingesetzt wird. Vielmehr handelt es sich immer noch um Versuchsballone, mit denen die Betrüger ausloten, was möglich, respektive gewinnbringend ist.[19]

2.2.2.1 Sextortion mit Bildern, die mit KI erzeugt wurden

Sextortion bezeichnet eine Erpressungsmethode, bei der eine Person mit Bild- und Videomaterial erpresst wird, welches sie beim Vornehmen sexueller Handlungen und/oder nackt zeigt. Opfer werden im Vorfeld durch eine attraktive Frau oder einen attraktiven Mann in Sozialen Medien kontaktiert und danach verführt, sich vor der Kamera auszuziehen. Alle diese Handlungen werden heimlich aufgenommen. Die Täter drohen dann, die Aufnahmen unter Angabe des Namens auf YouTube zu veröffentlichen oder die Aufnahmen per E-Mail an Familienangehörige, Freunde oder den Arbeitgeber zu schicken.[20]

Dem BACS sind auch einige Fälle bekannt, in denen Betrüger mithilfe von KI kompromittierende Fotos oder Videos erstellten, um die Opfer zu erpressen. Dazu reicht es aus, wenn die Täter im Besitz eines unverfänglichen Videos oder Fotos sind, das sie zuvor selbst aufgenommen haben oder das sogar im Internet für jedermann zugänglich ist. Die KI erstellt aus diesen unverfänglichen Videos pornografische Videos oder Nacktbilder. Was damit möglich ist, ist spätestens seit den Taylor Swift Deep-Fake-Pornos bekannt.[21] Das BACS geht davon aus, dass diese Form der Erpressung in den nächsten Jahren stark zunehmen wird. Neben diesen düsteren Aussichten gibt es aber auch einen positiven Aspekt. Da solche Fake-Videos von praktisch jeder Person erstellt werden können, die mit Fotos und Videos im Internet präsent ist, dürfte dies zu einer Abstumpfung führen. Damit könnte die Drohkulisse auch für diejenigen verpuffen, von denen tatsächlich kompromittierende Videos existieren.

2.2.2.2 Telefonanrufe

Die meisten Betrugsversuche erfolgen nach wie vor schriftlich über E-Mail oder Messenger-Dienste. Nur ein kleiner Teil erfolgt über das Telefon. Der Grund dafür liegt auf der Hand. Während die Angreifer bei der schriftlichen Kommunikation genügend Zeit haben, ihre Sätze mittels Deepl und vergleichbare Hilfsmittel in die jeweilige Landessprache zu übersetzen, muss der Angreifer bei einem Telefonat die Landessprache beherrschen und auf den Gesprächspartner unmittelbar reagieren können. KI dürfte in Zukunft auch hier Einzug halten, indem Telefongespräche mit einer vorgegebenen Stimme und Sprache simultan übersetzt werden. Erste Anzeichen für den Einsatz von KI bei Telefongesprächen gibt es bereits. So meldeten dem BACS schon mehrere Unternehmen, dass vermeintliche Mitarbeitenden mit passender Stimme bei ihnen angerufen hätten, um sich nach Firmeninterna zu erkundigen

---

19 Woche 49: Einsatz von künstlicher Intelligenz für Betrugsversuche (ncsc.admin.ch)

20 Sextortion (ncsc.admin.ch); Schweizerische Kriminalprävention | Sextortion (skppsc.ch)

21 Deepfake-Pornos: Ein manipuliertes Video kann ein Leben ruinieren (srf.ch)

oder Zahlungen auszulösen. Der betroffene Mitarbeiter hatte jedoch keine Ahnung von diesen Anrufen. Diese Anrufe werden wahrscheinlich mit Deep Fake erzeugt. Auch bei Schockanrufen bei Eltern, deren Kinder angeblich einen Unfall hatten, werden Stimmen verwendet, die denjenigen der Kindern sehr ähnlich sind. Inwieweit hier KI bereits eine Rolle spielt, ist allerdings unklar.

2.2.2.3 Kommunikation in Schweizerdeutsch

Vereinzelt tauchen auch Phishing-E-Mails in Schweizerdeutsch auf. Bereits im letzten Halbjahr hat das NCSC darüber berichtet.[22] Auch hinter diesen E-Mails dürfte KI stecken. Dieses Vorgehen erstaunt allerdings. In der Geschäftswelt ist Hochdeutsch die Regel. Eine angeblich offizielle E-Mail von einer Bank in Dialekt würde das Opfer wohl eher stutzig machen, als dass es das Opfer überzeugen würde, auf den betreffenden Link zu klicken. Es dürfte sich deshalb um Versuchsballone der Angreifer gehandelt haben. Es gibt jedoch einen anderen Bereich, in dem Dialekt in der Kommunikation üblich ist. So hat das NCSC im letzten Halbjahr gerade im Bereich des Kleinanzeigenbetrugs einige Fälle beobachtet, in denen die Kommunikation im Dialekt geführt wurde. Dies schafft beim Opfer Vertrauen, da Verkäufer bzw. Käufer aus der gleichen (Sprach-)Region zu kommen scheinen. Es ist davon auszugehen, dass in diesen Fällen auch KI eingesetzt wird.

2.2.2.4 Investitionsbetrug mit Prominenten

Bei Online-Anlagebetrug werden häufig Bilder von Prominenten verwendet, um den dubiosen Angeboten einen seriösen Anstrich zu geben. Dabei werden nicht nur öffentlich verfügbare Bilder oder Videos verwendet. Es werden unter anderem auch Deep-Fake-Videos generiert. Ein Beispiel war das Deep-Fake-Video von Elon Musk anlässlich des Starts der Starship-Rakete. Die Betrüger haben den Start der Starship-Rakete von Elon Musks Unternehmen SpaceX als Anlass genommen, um für einen «Give Away»-Betrug Werbung zu machen. Auf einer Webseite verspricht Elon Musk per Video, die in Kryptowährungen an ihn überwiesenen Beträge zu verdoppeln und zurückzusenden.[23]

Schlussfolgerungen / Empfehlungen:

Mithilfe von KI-Anwendungen können Cyberakteure Inhalte für glaubhaft aussehende E-Mails und Kurznachrichten erstellen, die sprachlich und in der Darstellung einem legitimen Schreiben täuschend ähnlich sind und kaum mehr vom Werk eines sprachlich versierten Menschen unterschieden werden können. Dies erschwert es den Empfängern solcher Inhalte, diese als Betrugsversuch zu erkennen.

Weiter ermöglicht der Einsatz von KI das Erstellen von täuschend echt aussehenden Fotos und Videos sowie von echt klingenden Stimmen (sogenannten «deep fakes»). Diese können für Social Engineering-Angriffe verwendet werden. Stimmimitationen können die Zielperson überzeugen, dass sie mit einer bekannten Person spricht, die Geld oder andere Hilfe benötigt.

---

22 Woche 14: Phishing in Schweizerdeutsch und eine Rechnung der Schweizerischen Rettungsfahrtwacht (ncsc.admin.ch)

23 Woche 17: Werbung mit Deepfake-Video für einen «Give Away»-Betrug (ncsc.admin.ch)

Betrüger denken sich immer neue Szenarien aus, um die Opfer zu bewegen, unbedacht zu reagieren. Mit Hilfe von KI-generierten Inhalten und Social Engineering soll erreicht werden, dass die Opfer von der Täterschaft gesteuerte Handlungen ausführen, ohne Verdacht zu schöpfen. Lassen Sie sich deshalb nicht täuschen, sondern denken Sie in Ruhe nach und fragen Sie im Zweifelsfall andere Personen oder das BACS, wie diese einen Sachverhalt beurteilen.

2.3 Meldungen zu Phishing

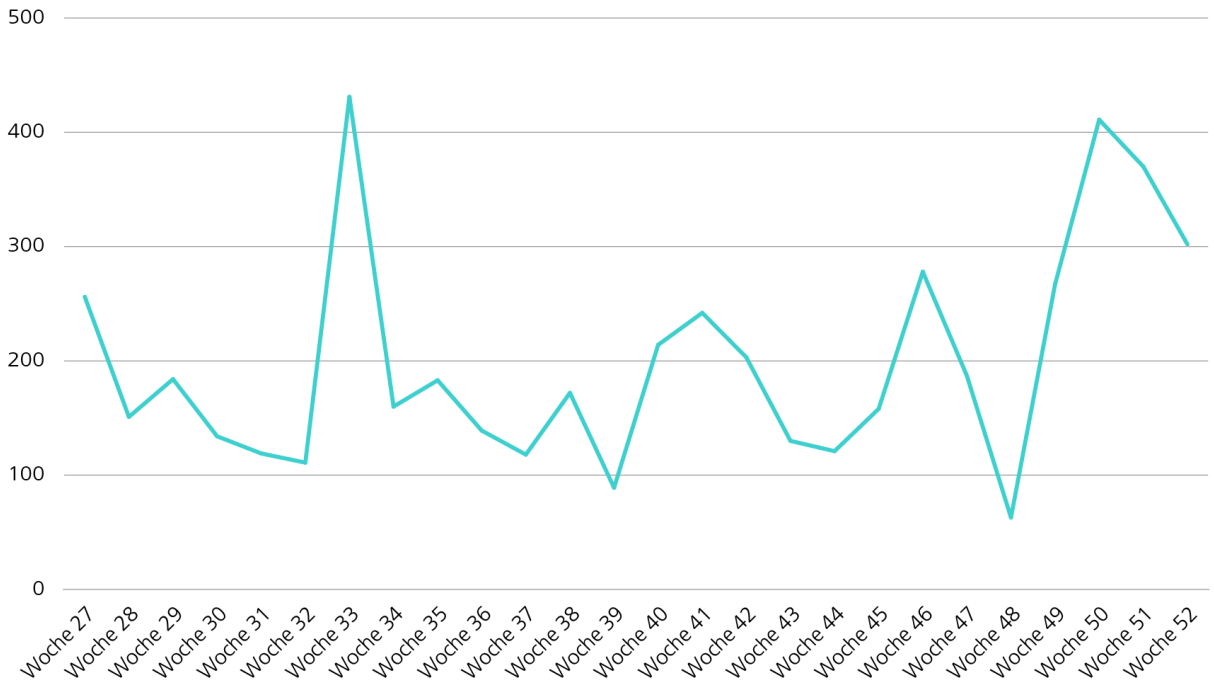

Abb. 3: Anzahl durch das NCSC überprüfte und bestätigte Phishing-URLs pro Woche im zweiten Halbjahr 2023.

2.3.1 Chain-Phishing, Paketpost-Phishing und doppelt bezahlte Rechnungen

Phishing ist nach Betrug weiterhin das am zweitmeisten über das Meldeformular gemeldete Phänomen. Im Vergleich zur Vorjahresperiode gab es beim Meldeeingang zu diesem Phänomen mehr als eine Verdopplung. Im zweiten Halbjahr 2023 stieg der Meldeeingang von 2'179 auf 5'536 Meldungen. Im gesamten Jahr erreichten das NCSC auf diesem Weg 9'415 Meldungen zu Phishing. Das NCSC (jetzt BACS) nimmt auch über die Plattform antiphishing.ch Meldungen zu Phishing entgegen, die dann teilautomatisiert verarbeitet werden.[24]

Beim allergrössten Teil der Phishing-Angriffe handelt es sich um breit gestreute Massenware. Diese sind fehlerbehaftet und werden ohne grossen Aufwand versendet. Ein typisches Zeichen ist beispielsweise immer noch eine unpersönliche Anrede wie «Lieber Kunde» oder gar eine Anrede mit der «E-Mail-Adresse».

[24] Siehe dazu auch den Anti-Phishing Bericht 2023 (ncsc.admin.ch).

Bei den am häufigsten gemeldeten Phishing-Versuchen handelt es sich um dieselben wie im vergangenen Jahr. Immer noch werden gefälschte Paketbenachrichtigungen[25] zu Tausenden versendet. Auch angebliche Rückerstattungs-E-Mails im Namen von Telekommunikationsanbietern, der SBB oder auch der Steuerverwaltung gehören zum Standardrepertoire der Phisher.[26] Die Angreifer nutzen hier vor allem die hohe Wahrscheinlichkeit aus, dass jemand tatsächlich ein Paket erwartet oder eine Rechnung bei einem Provider usw. bezahlt hat. Dies verleiht der E-Mail eine höhere Plausibilität.

Auf der anderen Seite beobachtet das BACS eine Zunahme der Phishing-Angriffe, welche auf Unternehmen zielen. Vor allem steigt der Druck auf Zugangsdaten zu Firmen-E-Mails und hier insbesondere zu Office365-Konten weiter an. Zunehmend sind Phishing-Versuche nach dem Schneeballprinzip zu beobachten. Dabei wird ein Firmen-E-Mail-Konto gehackt und anschliessend im Namen des Opfers eine Phishing-E-Mail an alle Kontakte gesendet, die die Angreifer im gehackten Konto finden. Gerade bei den Mitarbeitenden mit Kundenkontakt können so mehrere tausend Kontakte zusammenkommen. Da in diesen Fällen der Absender dem Empfänger bekannt ist, ist die Wahrscheinlichkeit grösser, dass dieser den Sachverhalt glaubt und auf den Phishing-Versuch hereinfällt. Wird dieser getäuscht, fängt das Spiel von vorne an und es werden wiederum seine Kontakte angeschrieben. Diese Vorgehensweise wird auch «Chain-Phishing» genannt.

2.3.2 Die Renaissance von Voice-Phishing

Voice-Phishing macht nach wie vor nur einen kleinen Teil der Phishing-Meldungen aus. Da die Anrufe aber sehr gezielt sind und der Anrufer auch auf das Opfer eingeht, dürften die Erfolgschancen hier um ein Vielfaches grösser sein. Dies ist sicherlich auch der Grund, wieso die Phisher diesen grösseren Aufwand auf sich nehmen.

Gegen Ende des Jahres 2023 häuften sich die Meldungen über Anrufe von angeblichen Bankmitarbeitenden. Die Anrufer gaben dabei vor, eine betrügerische Zahlung stoppen zu wollen. Die angezeigte Telefonnummer entsprach in einigen Fällen sogar der offiziellen Nummer der Bank. Diese wird von den Betrügern «gespoofed», d. h. gefälscht, um glaubwürdig zu erscheinen. In vielen Fällen wurde dann z. B. behauptet, dass eine Abbuchung für einen Flachbildschirm in einem Elektronikmarkt vorliege. Es wurde empfohlen, sofort die Betrugsabteilung der Kantonspolizei anzurufen. Die entsprechende Telefonnummer der Polizei, die angerufen werden soll, wurde ebenfalls gleich mitgeliefert. Diese gehört natürlich auch den Phishern.

Was auf den ersten Blick plausibel erscheint, ist jedoch gar nicht möglich. Die Bank sieht zwar in ihrem System die abgebuchten Beträge, weiss aber nicht, welche Produkte oder Dienstleistungen der Kunde gekauft hat. Insofern kann eine Bank grundsätzlich gar nicht wissen, was von einem Kunden gekauft worden ist.

In der Regel geben sich die Anrufer als Mitarbeitende grosser Banken aus. Die Wahrscheinlichkeit, dass der Angerufene tatsächlich ein Konto bei der Bank hat, für die sich der Betrüger ausgibt, ist bei grossen Banken höher. Doch auch für den Fall, dass die Bank beim Anruf nicht

---

25 Paket Abofalle (ncsc.admin.ch); Woche 23: Wie aus einem Phishing-Versuch eine Abofalle wird (ncsc.admin.ch); siehe auch den Anti-Phishing Bericht 2023 (ncsc.admin.ch)

26 Woche 46: Phishing mit angeblicher Steuerrückerstattung und KryptoWallet-Phishing (ncsc.admin.ch); Woche 41: Office 365- und SBB-Phishing in verschiedenen Varianten (ncsc.admin.ch)

korrekt erraten werden kann, haben die Täter ein Rezept gefunden. Sie versuchen im Telefongespräch die richtige Bank des Opfers herauszufinden, nur um kurze Zeit später erneut anzurufen, diesmal jedoch unter dem Namen der «richtigen» Bank.

Wie Meldungen an das BACS zeigen, verwenden die Angreifer auch öffentlich verfügbare Informationen. So wurde das Opfer in einem Fall von einem angeblichen Bankmitarbeitenden angerufen und gefragt, ob es tatsächlich in den letzten Tagen eine grössere Summe überwiesen habe. Erstaunlicherweise war der angebliche Empfänger dem Opfer aus einer früheren Tätigkeit bekannt. Eine Internet-Recherche durch das BACS ergab, dass sowohl Name als auch Telefonnummern des Opfers wie auch des angeblichen Empfängers auf einer früheren gemeinsamen öffentlichen Präsentation ersichtlich waren. Dies zeigt, dass die Angreifer systematisch das Internet nach solchen Informationen durchkämmen, die sie dann für gezielte Social-Engineering-Angriffe nutzen können. Bislang war diese Vorgehensweise vor allem in Zusammenhang mit CEO-Betrug beobachtet worden und scheint sich nun auch auf das Phänomen Voice-Phishing zu erweitern.

2.4 Meldungen zu Schadsoftware und Hacking

2.4.1 Ransomware

Nicht bei allen Phänomenen wurde eine Zunahme beobachtet. Gerade in der Kategorie Ransomware sind die Zahlen, verglichen mit dem Jahr 2022, deutlich zurückgegangen. Mit rund 109 Meldungen gingen fast 40 Meldungen weniger ein als im Vorjahr. Der Rückgang betrifft allerdings vor allem Privatpersonen und nicht Unternehmen. So gingen 2023 lediglich 11 Meldungen ein, die Privatpersonen betrafen. Im letzten Jahr waren dies noch 56. Die bei Privatpersonen besonders im Fokus stehenden heimischen NAS-Systeme (Netzwerkspeicher) werden nur noch vereinzelt angegriffen. Zum einen, weil in diesem Jahr eine gravierende Schwachstelle ausgeblieben ist, zum anderen dürften die Angriffe auch zu wenig lukrativ gewesen sein.

Betrachtet man die Zahl der Meldungen zu Ransomware bei Unternehmen, so ist der Abwärtstrend deutlich moderater und die Zahl der Meldungen stabilisiert sich praktisch auf dem Niveau des Vorjahres – 98 anstelle von 103 Meldungen. Festzuhalten ist, dass die Angriffe mittlerweile fast immer mit einem Datenabfluss einhergehen, was das Schadensausmass zusätzlich erhöht (vgl. Kap. 3.3 zu Ransomware).

Besonders aktiv war weiterhin die Ransomware «LockBit». Weitere gemeldete Ransomware-Familien sind «Play», «MedusaLocker», «BlackCat/ALPHV», «Phobos», «BlackByte», «BlackBasta», «Babuk», «ECh0raix» und «Akira».

Empfehlungen:

Auf der Website des BACS finden Sie eine Auflistung von präventiven Massnahmen zum Schutz vor Ransomware sowie Handlungsanweisungen für den Ereignisfall.

2.4.2 Meldungen zu Hacking

Auch bei Hacking wurde im Jahr 2023 eine Zunahme festgestellt. Verglichen mit dem zweiten Halbjahr 2022 stiegen die Meldungen in der Berichtsperiode von 276 auf 351 Meldungen an.

Gerade Social-Media-Konten stehen hier unter Druck. Insgesamt 186 Meldungen (+78) erreichten das NCSC in dieser Kategorie. Dabei konzentrieren sich die Angreifer zunehmend auf Geschäftskonten, bei denen eine Kreditkarte hinterlegt ist. Über ein solches Konto können die Angreifer dann auf Kosten des Opfers Werbung – z. B. für dubiose Angebote – schalten. Neben dem Schaden, der durch den Verlust des Social-Media-Accounts entsteht, kann sich der finanzielle Schaden auf mehrere tausend Franken belaufen.

2.4.3 Hotels im Visier

In der zweiten Jahreshälfte 2023 standen insbesondere Hotels, deren Kunden und in diesem Zusammenhang vor allem die Plattform booking.com, im Fokus. Bereits Anfang des Jahres 2023 hat das NCSC vor Vorfällen gewarnt, bei denen sich ein falscher Rezeptionist bei einem Hotelgast meldete, um an Kreditkartendaten zu gelangen.[27] Die Angreifer kannten dabei sämtliche Buchungsdetails und nutzten diese Informationen, um das Gegenüber zu überzeugen, dass es sich wirklich um eine Anfrage des Hotels handelt. Der Verdacht lag damals nahe, dass sich die Angreifer Zugriff auf das «booking.com»-Konto des Hotels verschaffen konnten.

Im zweiten Halbjahr gab es dann weitere Hinweise, wie die Angreifer vorgehen, um an die Zugangsdaten von Portalen wie booking.com zu gelangen. Dabei werden verschiedene Social-Engineering-Methoden eingesetzt, um das Hotelpersonal dazu zu bringen, auf einen Link zu klicken und Malware zu installieren.

In einer Variante wird behauptet, dass ein Gast derzeit mit pornografischen Bildern erpresst werde, die angeblich in dem Hotelzimmer aufgenommen worden seien. Der Gast gibt dem Hotel zwei Tage Zeit, um den Sachverhalt zu klären und den Täter zu benennen, weil sich andernfalls das Hotel zum Mittäter mache. Als Beweis sei die gesamte Dokumentation des Falles archiviert worden. Die entsprechende Datei könne unter dem angegebenen Link heruntergeladen werden. Durch Anklicken des Links wird eine Schadsoftware heruntergeladen, die alle eingegebenen Zugangsdaten aufzeichnet und an die Angreifer übermittelt. Damit können die Täter auf aktuelle Buchungen des Hotels über Online-Plattformen wie booking.com zugreifen.[28]

Neben E-Mails mit Schadsoftware im Anhang sind auch reine Phishing E-Mails im Umlauf, die sich direkt an das Hotelpersonal richten. Auch hier wird versucht, den entsprechenden Mitarbeitenden zu verleiten, die Zugangsdaten zu booking.com preiszugeben.

Empfehlungen:

Gerade Hotels müssen viele Dokumente öffnen, die von Gästen übermittelt werden. Ausführbare Dateien dürfen aber unter keinen Umständen geöffnet werden. Überlegen Sie sich eine Strategie, bei der die Computer für die Gästekommunikation vom restlichen Netz abgetrennt sind (Netzwerksegmentierung). Halten Sie die Systeme immer auf dem neuesten Stand.

---

27 Woche 4: Schadsoftware in Hotels - Buchungsdaten werden für Betrug gegen Hotelgäste verwendet (ncsc.admin.ch)

28 Woche 47: Hotels im Visier von Cyberkriminellen (ncsc.admin.ch)

3 Lage

3.1 Initialer Zugang mit Schadsoftware (Trojaner)

Trojaner gehören in die Kategorie Schadsoftware, die Zugang zum System eines Opfers durch das Einfügen einer Hintertür ermöglichen. Sie werden häufig installiert, nachdem die Benutzer getäuscht worden sind, beispielsweise indem der Schadcode in ein anderes Programm integriert oder auf andere Weise versteckt worden ist. Diese Art von Schadsoftware wird regelmässig über E-Mails verteilt, entweder als Anhang oder über einen Link. Der Kontext der E-Mail wird ebenfalls genutzt, um den Benutzer zur unbewussten Ausführung des Schadcodes zu verleiten. Um die Legitimität der bösartigen E-Mail zu erhöhen, verwenden einige Angreifer frühere E-Mail-Korrespondenz, die sie auf betrügerische Weise erlangt haben. Diese Vorgehensweise wurde insbesondere bei den «Qakbot»-Betreibern beobachtet, einer Schadsoftware, deren Erstinfektion regelmässig zu Ransomware-Infektionen führte. Aktivitäten mit «Qakbot» gingen jedoch in der zweiten Jahreshälfte 2023 drastisch zurück, nachdem eine multinationale Operation gegen die mit «Qakbot» infizierten Systeme und die von den Betreibern der Schadsoftware genutzte Infrastruktur durchgeführt worden war.[29] Trotz der Stilllegung konnten die dahinterstehenden kriminellen Akteure ihre Aktivitäten in angepasster Form weiterführen. So wurden nach der Auflösung von «Qakbot» zunehmend Kampagnen zur Verbreitung der Schadsoftware «PikaBot» und «DarkGate» beobachtet, die mehrere Ähnlichkeiten mit den «Qakbot»-Aktivitäten aufweisen, wie z. B. die Verwendung früherer E-Mail-Korrespondenz oder die Nutzung bestimmter gleicher Infrastrukturen.[30] Es kamen jedoch auch neue Verbreitungswege hinzu, wie z. B. die Verwendung von Instant-Messaging-Software für den beruflichen Gebrauch (u. a. «Microsoft Teams» oder «Skype») oder die Verwendung von betrügerischer Suchmaschinenwerbung (Malvertising).[31]

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 die 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.

Schliessen Sie keine unbekannten, respektive gefundenen USB-Geräte am Computer an.

---

29 Qakbot Malware Disrupted in International Cyber Takedown (justice.gov)

30 Woche 42: Dynamit-Phishing – Nach Emotet und Qakbot folgt nun DarkGate (ncsc.admin.ch);
Are DarkGate and PikaBot the New QakBot? (cofense.com)

31 PikaBot distributed via malicious search ads (malwarebytes.com);
Microsoft Teams used to deliver DarkGate Loader malware (malwarebytes.com)

3.2 Schwachstellen: Ivanti CVE-2023-35078 und CVE-2023-35081

Ivanti ist ein Anbieter von Unified Endpoint Management-, Zero-Trust-Sicherheits- und Service Management-Lösungen und bietet Unternehmen somit eine zentrale Steuerung, um ihre Geräte zu schützen sowie zu warten. Rund um den Globus vertrauen insgesamt mehr als 40'000 Unternehmen auf die Produkte dieses Herstellers.

Im Ivanti Endpoint Manager Mobile (EPMM) – früher bekannt als MobileIron Core - wurde im Sommer 2023 eine Schwachstelle entdeckt. Der Hersteller informierte seine Kunden am 24. Juli 2023 und stellte einen Patch zur Installation zur Verfügung.[32] Die Sicherheitslücke ist bekannt unter der Nummer CVE-2023-35078 und betrifft mit 11.10, 11.9 und 11.8 alle zum damaligen Zeitpunkt unterstützen Produktversionen. Zudem sind auch ältere, schon länger nicht mehr unterstützte Versionen betroffen.

Die kritische Sicherheitslücke mit einer maximalen CVSS[33]-Bewertung von 10.0 ermöglicht einem nicht-authentifizierten Angreifer aus dem Internet den Zugriff auf bestimmte API[34]-Pfade. Dadurch können unter Umständen persönlich identifizierbare Informationen (PII) wie Namen, Telefonnummern und andere Details zu mobilen Geräten eingesehen werden. Ausserdem kann ein Angreifer auch Konfigurationsänderungen ausführen sowie ein EPMM-Administratorkonto anlegen. Dies wiederum eröffnet einem Eindringling weitere, tiefgreifendere Möglichkeiten für manipulative Handlungen auf dem verwundbaren System.

Zum Zeitpunkt der Veröffentlichung der Details zur Schwachstelle wurde diese – wie bei zahlreichen Schwachstellen üblich – bereits ausgenutzt. So informierte beispielsweise die nationale Sicherheitsbehörde Norwegens die Öffentlichkeit am 24. Juli 2023[35], dass die Schwachstelle nachweislich für einen Angriff auf norwegische Ministerien ausgenutzt worden war. Auch der Hersteller Ivanti erwähnt in seinem Advisory, dass ihm eine begrenzte Anzahl von Kunden bekannt ist, die bereits Opfer eines entsprechenden Angriffs geworden sind.

Während zahlreiche betroffene Unternehmen noch mit der Behebung von CVE-2023-35078 beschäftigt waren, wurde nur wenige Tage später, am 28. Juli 2023, mit der Kennung CVE-2023-35081[36], bereits die nächste Sicherheitslücke im Ivanti Endpoint Manager Mobile (EPMM) bekannt. Diese konnte im Rahmen der Untersuchungen zu CVE-2023-35078 identifiziert werden. Der Hersteller stellte auch in diesem Fall Informationen und Patches zur Verfügung, um die Sicherheitslücke zu schliessen.

Die zweite Schwachstelle wurde mit einer CVSS-Bewertung von 7.2 etwas weniger kritisch eingestuft als Erstere. Dennoch macht es die Sicherheitslücke einem authentifizierten Administrator möglich, schadhafte Dateien auf EPMM-Server zu installieren (Arbitrary File Write).

---

32 CVE-2023-35078 - New Ivanti EPMM Vulnerability (ivanti.com)

33 Das Common Vulnerability Scoring System (CVSS, deutsch: «Allgemeines Bewertungssystem für Schwachstellen») ist ein Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in Computer-Systemen. Siehe CVSS (wikipedia.org).

34 Ein API (application programming interface, wörtlich ‚Anwendungs-programmier-schnittstelle'), ist ein Programmteil, der von einem Softwaresystem anderen Programmen zur Anbindung an das System zur Verfügung gestellt wird. Siehe Programmierschnittstelle (wikipedia.org).

35 Nulldagssårbarhet i Ivanti Endpoint Manager (MobileIron Core) - Nasjonal sikkerhetsmyndighet (nsm.no)

36 CVE-2023-35081 - Remote Arbitrary File Write (ivanti.com)

Wird diese Schwachstelle in Verbindung mit CVE-2023-35078 ausgenutzt, so können Administrator-Authentifizierung und ACL[37]-Beschränkungen gänzlich umgangen werden.

Betroffen von der Schwachstelle sind – identisch wie bei der zuerst entdeckten Schwachstelle – alle zum Zeitpunkt der Veröffentlichung unterstützen Produktversionen sowie auch ältere, schon länger nicht mehr unterstützte Versionen.

Der Hersteller Ivanti bestätigte auf seiner Webseite zudem, dass sich die Angriffskomplexität für CVE-2023-35081 für einen Eindringling erwiesenermassen reduziert, sofern ein Systembetreiber die zuerst veröffentlichte Schwachstelle CVE-2023-35078 auf einem betroffenen System noch nicht behoben hat.

Das NCSC hat die Betreiber kritischer Infrastrukturen sowie auch zahlreiche weitere Schweizer Unternehmen aktiv vor beiden Schwachstellen gewarnt. Basierend auf technischen Analysen des NCSC wurden potenziell betroffene Firmen zusätzlich persönlich informiert und es wurden konkrete Handlungsempfehlungen abgegeben. Trotz der hohen Kritikalität beider Schwachstellen sind verhältnismässig nur wenig bestätigte Schweizer Opfer bekannt.

Schlussfolgerung / Empfehlungen:

Es ist durchaus realistisch, dass für dasselbe Produkt innerhalb von nur wenigen Tagen mehrere gravierende Schwachstellen öffentlich bekannt werden. Dies belegt der vorliegende Fall bei Ivanti eindrücklich. Der Faktor Zeit ist im Management von Schwachstellen ein äusserst wichtiges Kriterium. Publizierte Patches sollten in jedem Fall möglichst ohne Zeitverlust auf den betroffenen Systemen installiert werden. Empfehlungen des Herstellers sind dringend zu befolgen. Dazu ist es aber unerlässlich, dass jede Organisation und Unternehmung ihre Infrastruktur kennt und ein aktuelles Inventar der eingesetzten Produkte führt.

Rasches Handeln beim Schliessen von Sicherheitslücken gewährleistet einerseits den sicheren Betriebszustand der IT-Systeme und reduziert gleichzeitig auch die Angriffsfläche (Attack Surface) eines Unternehmens. Andererseits kann damit in bestimmen Fällen auch erfolgreich verhindert werden, dass ein Angreifer von einem sogenannten «Vulnerability Chaining» profitiert. Bei der Verkettung von mehreren Schwachstellen kombiniert ein Eindringling mehrere vorhandene Sicherheitslücken, um ein System zu kompromittieren. Schliesst ein Systembetreiber Schwachstellen mit Hilfe eines etablierten Vulnerability- und Patch-Management-Prozesses kontinuierlich, so erschwert dies die Arbeit des Angreifers und reduziert damit auch die Chance auf einen erfolgreichen Angriff.

3.3 Ransomware

3.3.1 Ransomware-Vorfälle

Im Berichtshalbjahr waren unter anderem Unternehmen, die Informatiklösungen für öffentliche Verwaltungen und KMU anbieten, von Ransomware-Angriffen betroffen. Diese immer häufiger

[37] Eine Access Control List (Zugriffssteuerungsliste) ist eine Software-Technik, mit der Zugriffe auf Daten und Funktionen eingegrenzt werden können. Siehe Access Control List (wikipedia.org).

auftretenden Angriffe auf die Lieferkette verdeutlichen, wie wichtig es ist, einfache, aber wirksame Präventionsmassnahmen zum Schutz vor Cyberangriffen einzuführen, den Erfahrungsaustausch (auf nationaler und internationaler Ebene) zu pflegen sowie während und nach einem Vorfall kompetent zu kommunizieren.[38]

3.3.1.1 Eine Schwachstelle in der Lieferkette (Supply-Chain)

Im November 2023 wurde der, unter anderem für öffentliche Verwaltungen tätige, Informatikdienstleister Concevis AG Opfer eines Ransomware-Angriffs.[39] Als Reaktion auf den Cyberangriff haben zahlreiche Kunden die Nutzung der von der Concevis AG angebotenen Dienstleistungen vorübergehend eingestellt, um ihre Systeme vor einer allfälligen Ausbreitung des Vorfalles über die Schnittstellen zum Dienstleister zu schützen.

Das Interesse der Cyberkriminellen an den Lieferketten wächst. So hat beispielsweise die Ransomware-Gruppe Everest ihre Aktivitäten neu auf die Tätigkeit als Erstzugangsmakler (Initial-Access-Broker) ausgerichtet. Das heisst, die Gruppe hat sich auf das Auffinden von Hintertüren in den Systemen von Organisationen und auf den Verkauf dieser Zugänge an andere Cyberkriminelle spezialisiert, statt wie bisher selber Angriffe durchzuführen. Gemäss FBI[40] basiert diese Aktivität auf der Erlangung eines initialen Zugangs zu den IT-Umgebungen der Opfer über Dritte. Dabei werden Schwachstellen der vom Anbieter oder von Drittdiensten kontrollierten Fernzugriffe ausgenutzt und legale Systemverwaltungs-Tools zur Rechteausweitung innerhalb der betroffenen Organisationen verwendet.

Schlussfolgerung / Empfehlungen:

Auch Angriffe und Vorfälle in den Lieferketten können den eigenen Betrieb beeinträchtigen und grosse (Folge-) Schäden verursachen. Es ist deshalb unerlässlich, Cybersicherheit und Datenschutz mit Partnern zu thematisieren, vertraglich zu regeln und auch zu überprüfen.[41]

3.3.1.2 Offline-Backups und regelmässige Software-Updates

Im August 2023 war das Netz der sri-lankischen Regierung, das Lanka Government Network (LGN), von einem Ransomware-Angriff betroffen, der eine Verschlüsselung von Systemen und Daten des LGN umfasste. Die Systeme konnten zwar innerhalb von zwölf Stunden wiederhergestellt werden, bei einigen Daten gelang die Wiederherstellung jedoch nicht. Mangels Offline-Backups musste auf die Online-Backups zurückgegriffen werden, die durch den Angriff jedoch ebenfalls korrumpiert waren. Deshalb konnten u. a. E-Mails, die zwischen dem 17. Mai und 26. August 2023 gesendet und empfangen wurden, nicht mehr wiederhergestellt werden. Der

---

38 Siehe auch die Empfehlungen des BACS: Cyberangriff – wie kommunizieren? (ncsc.admin.ch)

39 Concevis AG Opfer eines Ransomware-Angriffs (ncsc.admin.ch)

40 FBI Private Industry Notification 231108.pdf (ic3.gov)

41 Supply chain security guidance (ncsc.gov.uk); ICT Supply Chain Resource Library (cisa.gov); Empfehlungen für die Zusammenarbeit mit IT-Providern (ncsc.admin.ch)

Ransomware-Angriff war unter anderem erfolgreich, weil im LGN noch veralteten Versionen von «Microsoft Exchange» (2013) genutzt wurden.[42]

Schlussfolgerung / Empfehlungen:

Erstellen Sie regelmässig Sicherungskopien (Backups) Ihrer Daten (auch) auf einem externen Medium.[43]

Aktualisieren Sie Ihre Software, wenn Sicherheitsupdates verfügbar sind. Antizipieren Sie das Ende des Lebenszyklus einer Software und ersetzen Sie sie rechtzeitig.

3.3.1.3 Eine überlegte Kommunikation während der Bewältigung des Vorfalls ist gefragt

Im Mai 2023 wurde die Unico Data AG, ein Schweizer Anbieter von Informatiklösungen für KMU, Opfer eines Ransomware-Angriffs der Gruppe Play. In der Folge waren die meisten Dienstleistungen des Anbieters offline. Das Unternehmen reagierte schnell auf den Angriff und bildete einen Krisenstab, der mit der Behebung der durch den Angriff entstandenen Probleme, der Meldung des Vorfalls an die zuständigen Behörden und der Information der betroffenen Kunden betraut wurde. Da die Unico Data AG kein Lösegeld bezahlte, veröffentlichte die Ransomware-Gruppe die entwendeten Daten im Darkweb. Einige Zeit später kommentierte der Geschäftsführer von Unico Data AG den Vorfall öffentlich und thematisierte dabei die finanziellen Auswirkungen des Angriffs sowie die personellen und zeitlichen Ressourcen, die für die Lösung des Problems erforderlich waren.[44] Der Geschäftsführer sprach auch über die Lehren, die das Unternehmen aus dem Vorfall gezogen hatte. Er rief andere Unternehmen dazu auf, sich auf Cyberangriffe vorzubereiten und sich dabei auf Pläne für die Notfallwiederherstellung (Disaster-Recovery), aber auch auf die – interne und externe – Kommunikation zu konzentrieren. Er betonte, wie wichtig es sei, festzulegen, welche Informationen von welchen Personen über welche Kanäle kommuniziert werden.

Schlussfolgerung / Empfehlungen:

Durch überlegte, proaktive Kommunikation können Opfer von Cyberangriffen die Vorfälle einordnen und ihre Mitarbeitenden, ihre Kundschaft, ihre Partner, die Medien und die Bevölkerung sachlich informieren und Spekulationen vorbeugen.

Empfehlungen des BACS zu Cyberangriff – wie kommunizieren? (ncsc.admin.ch).

3.3.2 Nachverfolgung von Ransomware-Varianten und Akteuren

Ransomware-Gruppen passen sich rasch an sich ändernde Umstände an, seien dies neue Schwachstellen, technische oder personelle Entwicklungen in der Szene, Massnahmen von Behörden oder neue rechtliche Vorgaben. Ein Beispiel für Ersteres ist die Ausnutzung einer

---

42 Sri Lankan government loses months of data following ransomware attack (therecord.media); Crisis & Consequences: An Emerging Cyber Quandary for Sri Lanka (capsindia.org)

43 S-U-P-E-R.ch – Dies gilt es bei der Datensicherung zu beachten (ncsc.admin.ch)

44 "Der Cyberangriff hat uns insgesamt weit über 1 Million Franken gekostet" (inside-it.ch)

neuen Schwachstelle in der Atlassian-Software «Confluence», welche für die Verbreitung der Ransomware «C3RB3R» genutzt wurde.[45]

3.3.2.1 Entwicklung der Akteure und ihrer Dienstleistungen

Im Berichtshalbjahr gab es erneut Veränderungen bei den Ransomware-Gruppen und ihren Aktivitäten. Die Gruppen ändern häufig ihre Zusammensetzung, ihren Namen und die Art ihrer Aktivitäten, sie fusionieren manchmal mit anderen Gruppen oder bieten ihnen ihre Dienstleistungen an, z. B. in Form von Ransomware als Dienstleistung (Ransomware-as-a-Service, RaaS). Der Ransomware-Markt blüht wie nie zuvor, was auch weniger erfahrenen Akteuren einfache Möglichkeiten eröffnet, Schadsoftware selbst herzustellen und anzupassen. Das war etwa beim Ransomware-Baukasten «Lockbit 3.0» der Fall, dessen Code im September 2022 durchsickerte. Die Forschenden von Kaspersky fanden 396 verschiedene Samples, die diesen Code enthielten.[46] Das Vorhandensein zahlreicher Varianten von «Lockbit» erschwert es den Cybersicherheitsforschenden, Angriffe bestimmten Gruppen oder Einzelpersonen zuzuordnen und ihre Aktivitäten nachzuverfolgen. Eine weitere Schwierigkeit ist der grosse Zuwachs an neuen Akteuren und Varianten in der Ransomware-Landschaft.[47]

Die Gruppe Royal beispielsweise scheint von der Gruppe BlackSuit abgelöst worden zu sein. Es könnte sich dabei um eine Namens- oder Markenänderung und/oder um eine abgeleitete Variante handeln, da die Schadsoftware «BlackSuit» gewisse Code-Merkmale aufweist, die denjenigen von Royal ähnlich sind.[48]

2023 wurden nicht nur bestehende Varianten umgestaltet, es wurden auch neue, sich als innovativ und einzigartig präsentierende Ransomware-Familien entwickelt, so etwa die RaaS «Rhysida». Diese verfügt über einen Selbstzerstörungsmechanismus und ist kompatibel mit Microsoft-Betriebssystemen, die älter als Windows 10 sind. Sie wurde mit der Programmiersprache C++ geschrieben und mit dem Entwicklungswerkzeug «MinGW» und gemeinsam genutzten Bibliotheken (Shared Libraries) kompiliert. «Rhysida» ist seit Mai 2023 aktiv.[49]

3.3.2.2 Reaktion auf eine Polizeiaktion

Ende 2023 leitete das FBI eine internationale Aktion gegen die Gruppe BlackCat/ALPHV.[50] Während mehrerer Tage war die Data-Leak-Site (DLS) der Gruppe als beschlagnahmt gekennzeichnet. Die Strafverfolgungsbehörden konnten 946 Schlüsselpaare sicherstellen, mit denen sie Zugang zur verschlüsselten Kommunikationen der Täter mit den Opfern, den Sites mit den entwendeten Daten und zum Partner-Panel der Gruppe erhielten. Die Cyberkriminellen haben jedoch kurz darauf die Aufschaltung einer neuen DLS bekannt gegeben, auf der umgehend sechs mutmassliche Opfer aufgeführt wurden. Die Ransomware-Gruppe Lockbit

---

45 C3RB3R Ransomware | Ongoing Exploitation of CVE-2023-22518 Targets Unpatched Confluence Servers (sentinelone.com)

46 Leaked Lockbit ransomware builder analysis (securelist.com)

47 Orange Cyber Defense publiziert regelmässig eine Aufstellung zu den verschiedenen Ransomwarevarianten und -akteuren: Map tracking ransomware, by OCD World Watch team (github.com)

48 Investigating BlackSuit Ransomware's Similarities to Royal (trendmicro.com); BlackSuit ransomware - what you need to know (tripwire.com)

49 Kaspersky crimeware report: GoPIX, Lumar, and Rhysida. (securelist.com)

50 Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant (doj.gov)

versuchen seither, Partner sowie Entwicklerinnen und Entwickler von BlackCat/ALPHV zu rekrutieren.

Für die Ransomware «BlackCat/ALPHV» gibt es derzeit kein universelles Entschlüsselungs-Tool. Einige Opfer können jedoch mittels der Schlüssel, die dank der Polizeiaktion verfügbar sind, ihre Daten wiederherstellen.

3.3.2.3 Anpassung der Erpressungen an die regulatorische Entwicklung

Die Cyberkriminellen passen sich auch an neu eingeführte Vorschriften und Regulierungen an, wie etwa die Einführung von Meldepflichten.

Die neue Gruppe RansomedVC wendet eine entsprechende Erpressungstaktik an, indem sie die Opfer vor der Busse warnt, die es nach Datenschutzgesetzgebung (DSGVO oder andere Gesetzestexte) erwartet, wenn es die geforderte Lösegeldsumme nicht bezahlt und der Fall deshalb publik gemacht werde. Die Gruppe nennt ihre Lösegeldforderung «Steuer für digitalen Frieden» (engl. «Digital Peace Tax»), ähnlich wie die Ransomware-Gruppe LockBit ihre Operationen als «Penetrationstest-Service mit nachträglicher Zahlung» bezeichnet.

3.3.2.4 Attraktive Branchen für Cyberkriminelle: Energie und Gesundheit

Der Energie- und der Gesundheitssektor sind beliebte Ziele für Ransomware-Akteure. In diesen beiden Branchen können aufgrund der erbrachten Dienstleistungen nur kurze Ausfallzeiten toleriert werden. Bei den Gesundheitsorganisationen kommt hinzu, dass sie den Patientinnen und Patienten unerlässliche, oft sogar lebenswichtige Dienstleistungen anbieten und sich zunehmend auf vernetzte Systeme, elektronische Patientendossiers und Telemedizin stützen. Dies kann dazu führen, dass Betreiber kritischer Infrastrukturen den Lösegeldforderungen rasch nachkommen, um wieder Zugang auf ihre Systeme zu erhalten.

Bei den Vorfällen, die sich im zweiten Halbjahr 2023 im Gesundheitssektor zugetragen haben, konnte die Behandlung der Patientinnen und Patienten zumeist ohne grössere Einschränkungen weitergeführt werden, und die Aktivitäten der Kliniken blieben verfügbar. Betroffene Spitäler melden sich jedoch, allenfalls vorsichtshalber, vom System der Notfallversorgung ab, was zu Umverteilungen von Patientinnen und Patienten auf umliegende Krankenhäuser führen kann.

Bei den Vorfällen im Energiesektor (einschliesslich Kernanlagen und Forschungseinrichtungen) ist seit 2022 ein Wiederanstieg der Ransomware-Angriffe zu beobachten. In vielen Fällen hat ein solcher Vorfall zwar Auswirkungen auf die IT-Systeme und es kommt zur Verschlüsselung von Dateien, das Ereignis hat aber keine Störungen bei der Erzeugung oder Verteilung zur Folge und die Energieversorgung kann ohne Unterbruch fortgeführt werden.

Empfehlungen:

Auf der Website des BACS finden Sie eine Auflistung von präventiven Massnahmen zum Schutz vor Ransomware wie auch Handlungsanweisungen für den Ereignisfall.

3.4 Datenabflüsse / Datenmanagement

Daten sind das Gold des Informationszeitalters. Datenabflüsse haben nicht nur für die direktbetroffenen Organisationen weitreichende Konsequenzen: Die gestohlenen Daten können für weitere Angriffe verwendet werden, wodurch auch Privatpersonen in das Visier von Bedrohungsakteuren geraten. Cyberkriminelle sind sich dieser Entwicklung bewusst, weshalb sich Schadsoftware für Datenbeschaffung (sog. Infostealer) und illegale Plattformen zum Datenverkauf steigender Beliebtheit erfreuen.[51] Im Dezember 2023 verursachten u. a. zwei grosse Leaks Schlagzeilen: Zum einen boten über Weihnachten verschiedene Hacker auf dem Darkweb kostenfrei Millionen von heiklen Personendaten von Datenabflüssen aus aller Welt an.[52] Zum anderen informierte die Firma 23andme, die Gentests zur Herkunftsforschung anbietet, dass vom Datenabfluss im Oktober 2023 persönliche und genetische Daten von fast 7 Millionen Kunden betroffen sind.[53] Für den Angriff wurden schwache und wiederverwendete Passwörter von Benutzern verwendet, die aus älteren Datenabflüssen stammen. Dies erhöht das Risiko für Betroffene insbesondere für weitere Angriffe, wie Kontoübernahmen, Phishing-Angriffe, Identitätsdiebstahl oder Finanzbetrug. Diese Vorfälle werfen nicht nur erneut die Frage nach der Verantwortung von Organisationen auf, heikle Personendaten von Kunden angemessen zu schützen. Auch Individuen stehen in der Verantwortung, die eigenen Konten mit starken Sicherheitsmassnahmen zu schützen. Zudem ist ein erhöhtes Bewusstsein dafür erforderlich, welche Daten mit welchen Organisationen geteilt werden.

Empfehlungen:

Speichern Sie nur Daten, die Sie wirklich brauchen (Datensparsamkeit) und löschen Sie nicht mehr benötigte Daten beziehungsweise archivieren Sie aufbewahrungswürdige aber nicht mehr aktiv gebrauchte Daten offline. Schützen Sie Zugänge zu Konten und Daten mit starken Passwörtern und wo möglich mit einer Mehrfaktor-Authentifizierung (MFA).[54]

Hinweis:

Am 1. September 2023 ist das totalrevidierte Bundesgesetz über den Datenschutz (DSG) in Kraft getreten. Dieses erfordert u. a. eine Meldung an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), wenn die Datensicherheit verletzt worden ist.[55]

3.4.1 Datenabflüsse im Gesundheitssektor (international)

Im zweiten Halbjahr 2023 hat sich der Trend von grossen Datenabflüssen im Gesundheitssektor fortgesetzt. Global gesehen befindet sich der Gesundheitssektor an dritter Stelle betreffend der Häufigkeit von Datenabflüssen, insbesondere in englischsprachigen Ländern. Auch in Europa sind Gesundheitsorganisationen im Visier von Cyberakteuren.

---

51 Vgl. Studie von Trend Micro zu Daten und Marktplätzen: Your Stolen Data for Sale (trendmicro.com)

52 Cybercriminals launched “Leaksmas” event in the Dark Web exposing massive volumes of leaked PII and compromised data (resecurity.com)

53 23andMe confirms hackers stole ancestry data on 6.9 million users (techcrunch.com)

54 Vgl. Schützen Sie Ihre Konten / Passwörter (ncsc.admin.ch)

55 DataBreach (edoeb.admin.ch)

Da viele Bedrohungsakteure finanziell motiviert sind, ist die konkrete Zielauswahl mehrheitlich opportunistisch bedingt. Dabei ist der Gesundheitssektor speziell attraktiv für die Hacker: Sie vertrauen darauf, dass Spitäler, Krankenversicherungen und Anbieter von Dienstleistungen in diesem Bereich eher Lösegeld bezahlen, um die Veröffentlichung dieser besonders schützenswerten Daten – und die Folgeschäden wie Vertrauensverlust oder rechtliche Folgen aufgrund Privatsphäre- und Datenschutzverletzungen – zu verhindern. Die Folgen für die Kunden und Patienten können ebenfalls verheerend sein. Zum einen ist für viele das Wissen, dass ihre Gesundheitsdaten von Unberechtigten eingesehen werden können, eine psychische Belastung. Die gestohlenen Daten können nicht zuletzt deshalb für die Erpressung der Patienten selber verwendet werden (sog. «data extortion»). Sie erlauben aber zum andern auch Identitätsdiebstahl, Versicherungsbetrug und weitere Delikte oder können schlicht an Dritte weiterverkauft werden.

Die Angriffe unterscheiden sich in der Komplexität und Form. Sie nutzen dabei verschiedene Angriffsvektoren wie zum Beispiel Phishing (vgl. Kap. 2.3) und andere Social-Engineering-Techniken[56] oder Schwachstellen in Software und Cloud-Lösungen sowie Angriffe auf Drittanbieter von Dienstleistungen. Insbesondere Angriffe auf die Lieferkette (vgl. Kapitel 4.5.2 im Halbjahresbericht 2023/1) haben massgeblich zu den erhöhten Zahlen von Meldungen beigetragen. Gewisse Trends, die bereits im ersten Halbjahr 2023 beschrieben wurden, u. a. Datenleaks durch die Gruppe Cl0p oder Angriffe auf Software-Dienstleister, haben sich im zweiten Halbjahr fortgesetzt.[57] Während gewisse Akteure manchmal den Datendiebstahl mit Verschlüsselungssoftware kombinieren (beispielsweise die Gruppen Hunters International[58] und BlackCat/ALPHV), fokussieren sich andere auf den reinen Datendiebstahl, etwa die Gruppe Karakurt. In der Vergangenheit behaupteten einige Bedrohungsakteure, explizit darauf zu verzichten, Organisationen im Gesundheitsbereich aufgrund derer Kritikalität anzugreifen. Gerade aber Gruppierungen, die ihre Kompetenzen als Dienstleistung verkaufen (Ransomware-as-a-Service) und aktuell zu den aktivsten Akteuren zählen – wie die Gruppe LockBit oder BlackCat/ALPHV – sind von dieser Haltung abgerückt.[59]

Während sich Schweizer Gesundheitsinstitutionen aktuell nicht gezielt im Fokus von Bedrohungsakteuren befinden, können opportunistische Angriffe auch den Schweizer Gesundheitssektor treffen. Ein Cyberangriff auf den Anbieter von digitalen Gesundheitslösungen Medgate im August und ein Folgeangriff im September 2023 konnten zwar erfolgreich abgewehrt

---

56 Social Engineering – der Mensch als Schwachstelle (bsi.bund.de)

57 Die Massenausnützung einer Schwachstelle in der Dokumententransfersoftware «MOVEit», die im Mai 2023 begann, betrifft unterdessen Daten von rund 90 Millionen Personen weltweit (Stand: Dezember 2023), siehe Unpacking the MOVEit Breach: Statistics and Analysis (emsisoft.com).

58 Z. B. Angriffe auf das amerikanische Krebszentrum Fred Hutchinson und das Crystal Lake Gesundheitszentrum: Hunters International ransomware gang claims to have hacked the Fred Hutch cancer center (securityaffairs.com); Ransomware gang claims to have stolen Crystal Lake Health Centers data (databreaches.net)

59 ALPHV hat diese Einschränkung in einer Ankündigung im Dezember 2023 – angeblich als Reaktion auf repressive Massnahmen der amerikanischen Strafverfolgung – aufgehoben: ALPHV/BlackCat Claims Healthcare Restrictions Removed for Affiliates (hipaajournal.com). LockBit griff im Dezember 2023 ein Kinderspital in den USA an, entgegen früherer anderslautender Versprechungen: Ransomware-Bande Lockbit wirft Skrupel über Bord (inside-it.ch)

werden, jedoch waren auch hierbei kurzfristige Dienstleistungsunterbrüche die Folge.[60] Im Oktober 2023 führte derweil ein Verschlüsselungsangriff auf die Psychiatrie Baselland zu einem technischen Ausfall der Systeme während zwölf Tagen, wobei der Vorfall ohne schwerwiegende Konsequenzen bewältigt werden konnte.[61] Dem BACS liegen keine Informationen über allfällige Datenabflüsse im Rahmen dieser Vorfälle vor.

3.4.2 Datenabfluss Stadt Baden

Am 4. Dezember 2023 wurde über einen Datenabfluss bei der Stadt Baden im Kanton Aargau berichtet.[62] Rund 3 GB Daten der Stadt wurden zum Herunterladen auf dem Hackerforum BreachForum angeboten. Eine vertiefte Analyse zeigte, dass die Daten Informationen wie Namen, Adressen, Telefonnummern, IBAN und Rechnungen von Einwohnerinnen und Einwohnern, aber auch zu Investitionen der Stadt Baden enthalten.[63]

Die Stadt Baden reagierte zeitnah, indem sie externe Experten für die Aufarbeitung des Vorfalls beauftragte, die Öffentlichkeit durch eine Medienmitteilung informierte[64] und ein Meldeformular[65] für mögliche Betroffene einrichtete. Auch erstattete sie Anzeige bei der Polizei. Gemäss eigener Angaben der Stadt Baden registrierten die Informatikdienste Mitte Oktober 2023 Unbekannte, die sich unbefugten Zugriff zu Servern der Informations- und Kommunikationstechnik (IKT) der beiden Städte Aarau und Baden zu verschaffen versuchten. Die Sicherheitslücke sei aber umgehend geschlossen und weitere Sicherheitsmassnahmen seien eingeleitet worden. Weiter lasse die Art der Daten darauf schliessen, dass sie aus einem verwaltungsinternen System stammen, in dem Rechnungen an und durch die Stadt Baden verwaltet werden.[66] Eine Kompromittierung von weiteren Systemen konnte dabei nicht festgestellt werden.

Der Vorfall zeigt exemplarisch die Entwicklung eines Bedrohungsakteurs, der versucht, sich im kriminellen Umfeld zu etablieren und an Glaubwürdigkeit zu gewinnen. Die Daten wurden zuerst von einer Person, die sich DragonForce nennt, auf einem Hackerforum publiziert. Zu jenem Zeitpunkt war diese Person noch kein etablierter Nutzer der Seite, sondern hatte sich erst Tage zuvor bei der Plattform registriert. Auch dass die Daten unentgeltlich zur Verfügung gestellt wurden, ist aussergewöhnlich. Normalerweise geschieht dies nur in Zusammenhang mit Datenerpressung bei fehlender Kooperation des Opfers (vgl. auch Kap. 3.3) oder bei Hacktivisten im Sinne von «hack and leak»[67]. Die Stadt Baden erhielt aber keine Lösegeldforderung[68] und DragonForce prangerte auch keine Missstände an. Vieles deutet darauf hin, dass sich der Akteur im kriminellen Umfeld einen Namen machen wollte. Dafür spricht auch, dass sich DragonForce Mitte Dezember dann eine eigene Datenleak-Seite im Darkweb erstellte und

60 Medienmitteilung: Cyberangriff auf Teile der IT-Infrastruktur von Medgate.pdf (medgate.ch)
61 Psychiatrie Baselland nimmt Normalbetrieb wieder auf - Psychiatrie Baselland (pbl.ch)
62 Baden ist Opfer eines Hackerangriffs geworden (nzz.ch)
63 Hackerangriff auf Baden: Meldeformular eingerichtet (badenertagblatt.ch)
64 Medienmitteilung: IT-Sicherheit der Stadt Baden (baden.ch)
65 Meldestelle Datenexposition (baden.ch)
66 Stadt Baden: "Nur Rechnungsdaten betroffen" (inside-it.ch)
67 Vgl. Halbjahresbericht 2023/1 (ncsc.admin.ch), Kapitel 2.3
68 Medienmitteilung: IT-Sicherheit der Stadt Baden (baden.ch)

die Stadt Baden erneut als Opfer auflistete. Weitere angebliche Opfer fügte der Akteur ebenfalls hinzu. Die Liste mit weltweiten Opfern verdeutlicht, dass der Akteur opportunistisch handelt und Schweizer Unternehmen oder Organisationen nicht per se im Fokus stehen.

Schlussfolgerung / Empfehlungen:

Grundsätzlich gilt: Daten sind wertvoll. Daher gibt es auch ein kriminelles Interesse, sich diese mit unlauteren Mittel zu beschaffen und zu verkaufen oder die Opfer mit der Drohung einer Veröffentlichung von sensitiven Daten zu erpressen. Aufgrund dessen sollte sich die Diskussion der Datensicherheit von der Frage wegbewegen, *ob* ein Datenabfluss stattfinden kann, und hin zur Frage, *wann* dieser geschieht und wie die Daten selbst im Extremfall eines Abflusses für den Angreifer nutzlos sind. Besonders bei sehr raffinierten Bedrohungsakteuren mit hohen Cyberfähigkeiten kann ein vollständiger Schutz gegen einen Datenabfluss kaum erreicht werden. Schwierig kontrollierbare Faktoren wie beispielsweise Schwachstellen haben dabei einen Einfluss. Daher ist es umso wichtiger, dass zentrale Prinzipien bezüglich Datensicherheit und -management beachtet werden.

Die **5Ws** der Datenhaltung: Festlegen, **wer welche** Daten, in **welcher Form, wo** ablegt und bearbeitet und mit **wem** diese geteilt werden. Dies bedeutet insbesondere, dass es sinnvoller ist, Daten konservativ zu speichern: Je weniger Daten gespeichert werden, desto weniger Daten müssen vor unautorisiertem Zugriff geschützt werden. Auch sollte der Datenbestand in regelmässigen Abständen überprüft und Unnötiges gelöscht werden. Zu prüfen ist ebenfalls, ob eine Archivierung von digitalen Daten offline erfolgen kann.

Technische Aspekte sind in der Umsetzung ebenso wichtig: Nebst den herkömmlichen Massnahmen für eine funktionierende Cyberhygiene[69] sollten Daten – wenn möglich – verschlüsselt gespeichert werden.

Sensibilisierung: Das Bewusstsein für die Problematik sollte bei Mitarbeiterinnen und Mitarbeitern regelmässig geschärft werden. Klare, umsetzbare Prozesse für den Datenumgang und -schutz sollten festgelegt, implementiert und kontrolliert werden. Nicht zuletzt sollte sich jede Person darüber im Klaren sein, dass Informationen – ob freiwillig oder unfreiwillig – im Netz öffentlich verfügbar sind. Akteure mit böswilligen Interessen können diese ausnutzen, und für «Social Engineering» verwenden. Lassen Sie sich im Ereignisfall nicht unter Druck setzen, bewahren Sie Ruhe und ziehen Sie gegebenenfalls Fachspezialisten hinzu.

Überprüfen: Daten aus älteren Datenabflüssen können für weitere Angriffe wiederverwendet werden. Überprüfen Sie periodisch, ob Ihre Zugangsdaten in einem Datenleck aufgetaucht sind, etwa auf der Website Have I Been Pwned: Check if your email has been compromised in a data breach (haveibeenpwned.com) oder dem Identity Leak Checker des Hasso Plattner Instituts (hpi.de). Verwenden Sie möglichst mehrere solche Websites. Denn, wenn Ihre Zugangsdaten auf einer Website nicht als Datenleck verzeichnet sind, bedeutet das nicht automatisch, dass Ihre Zugangsdaten nicht doch Teil eines Datenlecks sind.

[69] Kernthemen für eine gesunde Cyberhygiene sollten unter anderem folgende Themen umfassen: Passwortmanagement (z. B. Hashing und Salting), Prinzip der geringsten Privilegien, Netzwerksegmentierung sowie ein Patch- und Produktzyklusmanagement.

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

Die Vernetzung und Digitalisierung sämtlicher Lebensbereiche schreitet unaufhaltsam voran und macht selbstredend auch vor dem industriellen Umfeld nicht halt. Auf operativer Technologie basierende Prozesssteuerungen, welche in digitale Geschäftsabläufe integriert werden, ermöglichen erhebliche Effizienzsteigerungen und eine flexiblere Umsetzung. Eine solche Verzahnung der physischen und digitalen Welt ermöglicht jedoch auch weitreichendere Angriffe gegen industrielle Systemlandschaften. Staatliche Akteure und vermehrt auch Hacktivisten greifen ungenügend gesicherte industrielle Steuerungen an, um Prozesse zu manipulieren oder Verunsicherung in der betroffenen Bevölkerung zu schüren. Die grösste Bedrohung für den Betrieb industrieller Kontrollsysteme bleiben aber weiterhin Ransomware-Angriffe gegen angrenzende und ungenügend isolierte IT-Systeme, die den Weiterbetrieb des Gesamtverbundes zumindest temporär beeinträchtigen können.

3.5.1 Staatliche Akteure zeigen agilere Fähigkeiten im OT-Bereich

Während Raketenangriffe auf ukrainische Städte und kritische Infrastrukturen die Berichterstattung zu den Kriegshandlungen dominierten, führte der dem russischen militärischen Nachrichtendienst zugeordnete Bedrohungsakteur Sandworm am 10. Oktober 2022 einen Cybersabotageangriff gegen einen Betreiber der ukrainischen Stromversorgung durch. Gemäss dem Bericht[70] des Cybersicherheitsdienstleisters Mandiant vom November 2023 verschafften sich die Angreifer Zugang zur Infrastruktur, auf welcher eine microSCADA-Steuerung zur Kontrolle der Operational Technology (OT)-Umgebungen von Unterwerken des Elektrizitätsunternehmens betrieben wurde. Der erlangte Zugang wurde folglich missbraucht, um Befehle zur Abschaltung der Unterwerke auszuführen. Das Spezielle an dem analysierten Angriff ist die Methodik, auf bestehende Funktionalitäten für den Angriff zurückzugreifen. In der IT wird dieser «Living-of-the-Land (LOTL)» Ansatz bereits seit einiger Zeit beobachtet und hat nun auch Einzug ins OT-Umfeld gehalten. Gegenüber einer selbst entwickelten Malware[71], wie sie bei den Angriffen gegen die Stromversorgung um Kiew im Jahr 2016 eingesetzt wurde, ermöglicht diese Vorgehensweise eine schnellere Abfolge von erlangtem Netzwerkzugriff zur Ausführung des eigentlichen Sabotageangriffs. Da die missbrauchten Komponenten auch in vielen anderen Systemlandschaften eingesetzt werden, lässt sich dieser Modus Operandi auch flexibler auf weitere Ziele anpassen.

Neben der Stromversorgung wurden auch Cybersabotageangriffe gegen Ziele in der ukrainischen Landwirtschaft in zeitlicher Überlappung mit Raketenangriffen beobachtet.[72]

3.5.2 Wasserversorgung von Hacktivisten gestört

Im Umfeld internationaler Konflikte wie dem Krieg in der Ukraine oder der Eskalation im Nahen Osten schrecken Hacktivisten neben Angriffen auf die Verfügbarkeit (DDoS) oder dem Veröffentlichen abgefasster Informationen auch nicht vor sabotierenden Manipulationen auf expo-

---

70 Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology (mandiant.com)

71 CrashOverride Malware (cisa.gov)

72 Russian influence and cyber operations adapt for long haul and exploit war fatigue (blogs.microsoft.com)

nierten OT-Geräten zurück (vgl. Kap. 3.6). So begann die Hacktivisten-Gruppierung «CyberAv3ngers», Geräte des israelischen Herstellers Unitronics[73] anzugreifen. Die Aktivitäten störten Wasser- und Abwasserversorgungssysteme mindestens in den USA[74] und Irland[75]. Der Gruppierung wird eine Nähe zu den iranischen Revolutionsgarden[76] attestiert. Sie nutzt die Aufmerksamkeit, um ihre anti-israelische Propaganda-Botschaft zu verbreiten (vgl. Abb. 4).

Abb. 4: Propagandabotschaft auf kompromittierten Geräten[77]

Im Gegenzug störte die Gruppe «Predatory Sparrow» erneut den Betrieb von Tankstellen[78] im Iran. Auch im Umfeld des Krieges in der Ukraine veröffentlichen Hacktivisten wie das «Team OneFist» oder die «People's Cyber Army of Russia» immer wieder mutmassliche Dokumentationen von Angriffen gegen industrielle Steuerungen auf ihren Social Media Kanälen.

Schlussfolgerung / Empfehlungen:

Sichern Sie Ihre industriellen Systeme, um wie in diesem Kapitel beschriebene Angriffe zu verhindern. Das BACS schlägt hierzu Massnahmen zum Schutz von ICS vor.

Etwas umfassender sind die Branchenstandards, welche das Bundesamt für wirtschaftliche Landesversorgung BWL in Zusammenarbeit mit den jeweiligen Branchenorganisationen erarbeitet hat.

---

73 Exploitation of Unitronics PLCs used in Water and Wastewater Systems (cisa.gov)

74 Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa (waterisac.org)

75 Two-day water outage in remote Irish region caused by pro-Iran hackers (therecord.media)

76 IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (cisa.gov)

77 Iranian Cyber Av3ngers Compromise Unitronics Systems (secureworks.com)

78 Iran petrol stations hit by cyberattack, oil minister says (reuters.com)

Um zu prüfen, ob die eigenen Sicherheitsdispositive aktuellen Bedrohungen im industriellen Umfeld genügen, kann das Emb3d Framework von MITRE beigezogen werden.

3.5.3 IoT-Geräte werden als Angriffsinfrastruktur missbraucht

Noch häufiger als Angriffe gegen die durch OT gesteuerten Prozesse oder die Geräte selbst, ist deren Missbrauch als Angriffsinfrastruktur gegen anderweitige Ziele. Speziell davon betroffen sind schlecht gesicherte oder am Ende ihrer Lebenszeit angelangte (I)IoT[79]-Geräte wie Router, Kameras und dergleichen. Das dänische SektorCERT[80] veröffentlichte im November 2023 eine Analyse zu einer Reihe von im Mai 2023 kompromittierten Zyxel-Routern seiner Mitgliederorganisationen aus der Energieversorgungsbranche. Schwachstellen in diesen Geräten wurden umgehend von mehreren Akteuren ausgenutzt, um sie beispielsweise in Botnetze zu integrieren, welche dann für DDoS-Angriffe gegen weitere im Internet exponierte Ziele wie Websites missbraucht werden können. Auch in der Schweiz wurden mehrere Router dieser Modelle kompromittiert. Das BACS hat die Betreiber dieser Router darüber informiert, damit die Geräte bereinigt werden konnten.

Neben Zyxel wurden anderweitig auch alte Cisco und Netgear Geräte missbraucht, um das KV-Botnet[81] aufzubauen, welches dem Akteur Volt Typhoon zugeschrieben wird. Volt Typhoon wird mit Aufklärungsangriffen gegen kritische Infrastrukturen der USA in Verbindung gebracht.

Um den Missbrauch solcher Geräte künftig zu erschweren, hat die EU das Cyberresilienzgesetz[82] verabschiedet. Mit diesem neuen Rechtsakt werden EU-weite Cybersicherheitsanforderungen für Konzeption, Entwicklung, Herstellung und Inverkehrbringen von Hardware- und Softwareprodukten eingeführt. Die Verordnung gilt für alle Produkte, die direkt oder indirekt mit einem anderen Gerät oder einem Netz verbunden sind.

Schlussfolgerung / Empfehlungen:

Nicht nur eigentliche Netzwerkgeräte wie Router, sondern viele andere elektronische Geräte im Haushalt sind heutzutage vernetzt und konstant online. Auch diese Geräte müssen adäquat abgesichert und bei Bekanntwerden von Schwachstellen aktualisiert werden.[83]

3.6 Cyber in Konflikten

Im letzten Halbjahresbericht wurde neben einem Überblick über die wichtigsten Ereignisse im Cyberraum im Zusammenhang mit dem Krieg in der Ukraine auch darauf hingewiesen, dass es keine Anzeichen für einen Rückgang bösartiger Aktivitäten gab und dass ein erhöhtes Ri-

79 Internet der Dinge (wikipedia.org); Industrial internet of things (wikipedia.org)
80 The-attack-against-Danish-critical-infrastructure.pdf (sektorcert.dk)
81 Routers Roasting on an Open Firewall: the KV-botnet Investigation (blog.lumen.com)
82 Cyberresilienzgesetz: Rat und Parlament erzielen Einigung über Sicherheitsanforderungen für digitale Produkte (consilium.europa.eu)
83 Cybertipp: Was beim Internet der Dinge zu beachten ist (ncsc.admin.ch); Massnahmen zum Schutz von IOT Geräten (ncsc.admin.ch)

siko von Kollateralschäden im Zusammenhang mit Hacktivistengruppen bestand, die zerstörerische Angriffe durchführen wollten.[84] Beide Prognosen haben sich bewahrheitet, wie die Hauptentwicklungen in den Konflikten in der zweiten Hälfte des Jahres 2023 zeigen.

3.6.1 Krieg in der Ukraine

In Zusammenhang mit dem Krieg in der Ukraine setzten sich bösartige Aktivitäten im Cyberraum auch in der zweiten Hälfte des Jahres 2023 mit steigender Kadenz fort. So berichtete das ukrainische CERT, dass es im Jahr 2023 mit insgesamt 2'543 Vorfällen 15% mehr Vorfälle als im Jahr 2022 bearbeitet hat, darunter die Verbreitung von Malware, Phishing oder auch die Kompromittierung von Konten und Systemen.[85] Die öffentliche Verwaltung, die Verteidigung, die Energieversorgung und die Telekommunikation sollen zu den am meisten anvisierten Sektoren gehören. Die Ukraine berichtete auch über die zunehmende Tendenz Russlands, ukrainische Behörden, die mögliche russische Kriegsverbrechen untersuchen, mit Spionagekampagnen ins Visier zu nehmen. Ausserdem verzeichnete die Ukraine wiederholte Angriffsversuche auf Ziele, die bereits in der Vergangenheit angegriffen worden waren.[86] Eine neue Vorgehensweise ukrainischer Behörden ist die offizielle Bekanntgabe der Ergebnisse von Cyberkampagnen. So berichtete der ukrainische Militärnachrichtendienst im November 2023, dass er durch eine komplexe Cyberoperation in den Besitz zahlreicher vertraulicher Dokumente der russischen Föderalen Agentur für Lufttransport gelangt sei.[87] Der bemerkenswerteste Vorfall in diesem Zeitraum betraf jedoch die Ukraine: Am 12. Dezember 2023 war Kyivstar von einem Cybervorfall betroffen. Kyivstar ist der grösste Telekommunikationsanbieter der Ukraine, der mehr als die Hälfte der ukrainischen Bevölkerung mit Mobiltelefonie und Internetzugang versorgt. Der Angriff führte zu Unterbrechungen der Dienste für Kyivstar-Nutzer und der bei Kyivstar gehosteten Dienste. Dadurch war zum Beispiel für einen Teil der Bevölkerung der Zugang zu Finanzdienstleistungen eingeschränkt, und der Empfang von Warnungen vor Luftangriffen war nicht mehr gewährleistet. Eine teilweise Wiederherstellung der Dienste wurde am Abend des 13. Dezember 2023 erreicht, aber es dauerte mehr als eine Woche, bis alle Dienste wieder verfügbar waren.[88] Die Hacktivistengruppen KillNet und Solnetspek bekannten sich zu dem Angriff. KillNet legte keine Beweise vor und hatte sich in der Vergangenheit bereits mit Vorfällen gebrüstet, die nicht von ihnen ausgingen. Solnetspek hingegen veröffentlichte Screenshots, die den privilegierten Zugang zu den Systemen von Kyivstar belegen. Laut der Ukraine und verschiedenen westlichen IT-Sicherheitsfirmen soll die Gruppe Sandworm, die dem russischen Militärnachrichtendienst zugeschrieben wird und in der Vergangenheit bereits Telekommunikationsunternehmen ins Visier genommen hat, der Urheber des Angriffs sein und Solnetspek als Fassade nutzen.[89] Der Vorfall soll eine Kombination aus DDoS-Angriffen und dem Einsatz von Datenlösch-Schadsoftware (sogenannten Wiper) gewesen sein. Solnetspek

---

84 Siehe Halbjahresbericht 2023/1 (ncsc.admin.ch), Kap. 4.7

85 The CERT-UA Team has processed 2,543 cyber incidents over 2023 (cip.gov.ua)

86 How russian government-controlled hacking groups shift their tactics, objectives and capacities (cip.gov.ua)

87 Defence Intelligence of Ukraine conducted a cyber operation against Rosaviatsia (gur.gov.ua)

88 NetBlocks on X: Metrics show that connectivity on Ukraine telco Kyivstar is now largely restored (twitter.com); Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

89 Hacker Group Linked to Russian Military Claims Credit for Cyberattack on Kyivstar (wired.com); Russia's Sandworm blamed for Kyivstar telecom cyberattack (theregister.com)

gibt an, mehr als 10'000 Stationen und 4'000 Server von Kyivstar «zerstört» zu haben, darunter auch alle Speicher in der Cloud und Backupsysteme. Es gab bereits im März 2023 erste Versuche, in die Systeme der Organisation einzudringen. Im Mai 2023 gelang es den Angreifern schliesslich, sich durch die Kompromittierung des Kontos eines Kyivstar-Mitarbeiters einen ersten Zugang zu verschaffen und sich in den Systemen auszubreiten.[90] Dieser monatelange unentdeckte Zugang hätte es unter anderem ermöglicht, Kundeninformationen zu erhalten, Mobiltelefone zu orten, SMS abzufangen und unter anderem Internetkonten zu kompromittieren, die durch eine an eine Mobiltelefonnummer gebundene Authentifizierung geschützt sind, wie z. B. Telegram.

Für die Schweiz ist es äusserst unwahrscheinlich, dass sie Ziel ähnlicher Sabotageangriffe von staatlichen Akteuren wird. Wahrscheinlich ist jedoch, dass Hacktivistengruppen, die in einem Konflikt verwickelt sind, die Schweiz ins Visier nehmen. So führte NoName057(16), eine pro-russische Hacktivistengruppe, die schon im Juni 2023 Kampagnen von DDoS-Angriffen auf Schweizer Websites ausgeführt hatte,[91] in der zweiten Hälfte des Jahres 2023 fünfmal DDoS-Angriffe auf Schweizer Websites durch. Diese Angriffe waren hauptsächlich eine Reaktion auf Schweizer Aktivitäten in Zusammenhang mit dem Krieg in der Ukraine. So führte NoName057(16) beispielsweise am 28. November – drei Tage nach dem Besuch des Bundespräsidenten in der Ukraine – Angriffe auf Websites der Bundesverwaltung und von Organisationen durch, die im Finanzsektor und im Tourismus tätig sind. Diese Angriffe hatten zwar nur geringe Auswirkungen – es kam zu keiner nennenswerten Einschränkung der Verfügbarkeit, sie werden aber dennoch von Hacktivistengruppen zu Propagandazwecken genutzt.[92] Im Gegensatz zu früheren Kampagnen greift NoName057(16) nicht mehr kontinuierlich Websites aus demselben Land während einer Woche an, sondern ändert seinen Fokus täglich.

3.6.2 Nahost-Konflikt

Nach dem Angriff der Hamas auf Israel am 7. Oktober 2023, der zu einer erneuten Eskalation der Gewalt in der Region geführt hat, haben zahlreiche hacktivistische Gruppen ihre Beteiligung an dem Konflikt angekündigt. In vielerlei Hinsicht war der Hacktivismus in Zusammenhang mit diesem Konflikt ähnlich wie im Ukraine-Krieg. Bei einem Grossteil der Tätigkeit dieser Hacktivistengruppen geht es um Propaganda und/oder Desinformation. Nur eine kleinere Anzahl von Hacktivisten führte Aktionen im Cyberraum durch, die sich direkt auf Computersysteme auswirkten. Diese Aktionen betrafen hauptsächlich die Verunstaltung von Website und DDoS-Angriffe und wurden auch gegen Ziele ausserhalb der Konfliktzone beobachtet, meist als Reaktion auf Unterstützungserklärungen für einen der Protagonisten.[93] Mehrere Hacktivistengruppen haben jedoch raffiniertere und schädlichere Aktionen durchgeführt. So soll die Gruppe Cyber Toufan mehr als hundert israelische Organisationen kompromittiert haben, wobei sie sensible Daten veröffentlichte, nachdem sie die Infrastruktur der Organisationen durch

---

90 CEO of Ukraine's largest telecom operator describes Russian cyberattack that wiped thousands of computers (therecord.media); Exclusive: Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

91 Siehe Halbjahresbericht 2023/1 (ncsc.admin.ch), Kap. 2.1.
Detaillierter Analysebericht zu den DDoS-Angriffen «NoName057(16)» (ncsc.admin.ch)

92 Ukraine-Krieg: Russische Hackergruppe schürt in der Schweiz Verunsicherung (nzz.ch)

93 Hacktivist Involvement in Israel-Hamas War Reflects Possible Shift in Threat Actor Focus (securityscorecard.com)

den Einsatz von Wipern gestört hatte.[94] Die Karma-Gruppe soll auch mehrere israelische Organisationen infiltriert haben, um dort einen einzigartigen Wiper einzusetzen, der eine Version für Windows-Systeme und eine andere für Linux-Systeme aufweist.[95] Die Gruppe Cyber Av3ngers zielte auf industrielle Kontrollsysteme aus israelischer Produktion ab, indem sie deren Benutzeroberfläche verunstaltete und sie so unbrauchbar machte. Die Systeme wurden unabhängig von ihrer geographischen Lage ins Visier genommen, was zu Vorfällen in mehreren Ländern ausserhalb der Konfliktzone führte.[96] Bei einigen dieser Gruppen wird vermutet, dass sie als Fassade für staatliche Akteure, insbesondere des Irans, dienen oder von einem Staat unterstützt werden.[97] Die Schwierigkeit, solche Verbindungen nachzuweisen, können Staaten nutzen, um ihre Verantwortung zu bestreiten und gleichzeitig die Medienwirksamkeit ihrer Aktionen zu erhöhen.

3.6.3 Zukünftige Entwicklungen

Nichts deutet auf eine rückläufige Entwicklung der Cyberaktivitäten in Zusammenhang mit dem Ukraine-Krieg oder dem Nahost-Konflikt hin. Die Tendenz, dass rein zivilgesellschaftlich organisierte oder als Fassade eines Drittstaates fungierende Hacktivistengruppen im Zusammenhang mit Konflikten in den Cyberraum involviert sind, scheint sich zu konsolidieren und als neuer Standard zu etablieren. Obwohl diese Gruppen nach bisherigen Erkenntnissen für keinen der Protagonisten entscheidend gewesen zu sein scheinen, könnten ihre Aktivitäten auch dazu beitragen, staatliche Kräfte im Cyberbereich zu binden und deren Aufmerksamkeit zu erhalten. Zudem erschweren diese zusätzlichen Grundgeräusche in Kombination mit der konfliktbedingt unvollständigen Sicht die Einschätzung der Lage.

---

94 Cyber Toufan goes Oprah mode, with free Linux system wipes of over 100 organisations (doublepulsar.com)

95 Mission "Data Destruction": A Large-scale Data-Wiping Campaign Targeting Israel (securityjoes.com)

96 Siehe Kap. 3.5.2.

97 Iranian Hacktivist Proxies Escalate Activities Beyond Israel (checkpoint.com);
Iran surges cyber-enabled influence operations in support of Hamas (microsoft.com)