6. Mai 2025 | Bundesamt für Cybersicherheit BACS

Halbjahresbericht 2024/II (Juli – Dezember)

Cybersicherheit

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

Management Summary

Das Bundesamt für Cybersicherheit (BACS) beschreibt in seinem Halbjahresbericht die relevanten Vorfälle und Entwicklungen im Kontext der Cyberbedrohungen gegen die Schweiz und international. Im zweiten Halbjahr 2024 erhielt das BACS 28'165 Meldungen zu Cybervorfällen. Dies sind etwas weniger als im Verlaufe des ersten Halbjahres 2024. Über das gesamte Jahr 2024 stieg die Anzahl jedoch um 13'574 auf total 62'954 Meldungen. Die Schwankungen beruhen hauptsächlich auf der grossen Wellenbewegung des Phänomens Fake-Anrufe im Namen von Behörden. Das Verhältnis von 90 % der eingegangenen Meldungen durch Privatpersonen und von 10 % durch Unternehmen bleibt konstant. Die Kategorien Betrug, «Phishing» und «Spam» verbleiben die meistgemeldeten Phänomene.

Betrugsversuche treffen die Bevölkerung am häufigsten

Mit 18’270 Meldungen ist Betrug konstant das am häufigsten gemeldete Phänomen und macht zwei Drittel aller Meldungen im zweiten Halbjahr 2024 aus. Die Meldespitzen des Phänomens aufgrund von Fake-Anrufen im Namen von Behörden blieben im zweiten Halbjahr jedoch aus. Dieses Phänomen wurde im ersten Halbjahresbericht 2024 detailliert behandelt.[1] Eine Verdreifachung der eingegangenen Meldungen beobachtete das BACS in der aktuellen Berichtsperiode hingegen bei betrügerischen Gewinnspielen. Diese Abofallen bewegen sich in rechtlichen Grauzonen, welche die Betrüger mangels wirkungsvoller Gegenmassnahmen vermehrt bewusst ausnutzen. Unternehmensseitig zeigte sich ein starker Anstieg von Meldungen zu CEO-Betrug, wobei sich speziell im Umfeld von Gemeinden und Kirchen viele Betroffene befanden.

Überlastungen führen zu Störungen und fehlerhafte Updates zu Ausfällen

Am 19. Juli 2024 kam es zum disruptivsten IT-Ausfall der Geschichte. Nicht ein Cyberangriff, sondern ein fehlerhaftes Softwareupdate des Cybersicherheitsanbieters CrowdStrike machte über 8,5 Millionen Windows-Systeme **–** vorwiegend von Grossunternehmen **–** unbrauchbar. Neben Auswirkungen bei Organisationen wie Spitälern und Industriebetrieben wurde speziell die Luftfahrt in der Schweiz wie auch weltweit über mehrere Stunden stark eingeschränkt.
Überlastungsangriffe auf die Websites von Kantonen und Gemeinden, aber auch auf Webdienste für Finanzdienstleistungen, schränkten deren Verfügbarkeit für eine gewisse Zeit ein. Sogenannte «Distributed Denial of Service[2]» Angriffe (DDoS) werden durch verteilte Angriffsinfrastruktur – meist in Form eines Botnetzes wie «Gorilla» – ermöglicht.[3]

Schadsoftware wird kreativ verteilt – Ransomware gefährdet Unternehmen

Akteure und Angriffsmethoden im Umfeld von Erpressungen mit Ransomware passen sich laufend den aktuellen Gegebenheiten an und bleiben die relevanteste Bedrohung für Unternehmen. Beispielsweise fluten Cyberkriminelle im Umfeld der Gruppierung «Black Basta»

---

1 Siehe auch Halbjahresbericht 2024/1; Kap. 5.

2 Angriff auf die Verfügbarkeit (DDoS) (ncsc.admin.ch)

3 Siehe technische Analyse zum Botnetz «Gorilla» (ncsc.admin.ch)

E-Mail-Konten mit Spam-Nachrichten, um anschliessend über digitale Kommunikationsplattformen Hilfestellungen anzubieten, in deren Verlauf die Opfer kompromittiert werden.
Die Namen von bekannten Schweizer Unternehmen wie Krankenversicherer und Inkassounternehmen wurden missbraucht, um in deren Namen Schadsoftware an Empfänger bösartiger E-Mails zu verteilen. Auf gefälschten oder kompromittierten Webseiten werden Besucher durch gefälschte «CAPTCHAs» verleitet, bösartige Skripte manuell auszuführen und ihr Gerät dadurch zu infizieren. Über QR-Codes, die auf Briefsendungen aufgedruckt waren, versuchten Cyberkriminelle, die Empfänger dazu zu bewegen, eine infizierte «Alertswiss»-Applikation auf ihren Android-Mobiltelefonen zu installieren.

Phisher suchen neue Aufhänger und Kanäle

Zugangsdaten oder Finanzinformationen durch Phishing abzugreifen, bleibt die am zweithäufigsten gemeldete Kategorie beim BACS. Neben den bekannten Phishing-E-Mails versuchen Cyberkriminelle, ihre vorgetäuschten Abfragen vermehrt auf anderen Kanälen zu streuen. So melden sich angebliche Bankangestellte per Telefon oder es werden mobile Nachrichten über den SMS-Nachfolger «Rich Communication Services» (RCS)[4] versendet. Kleinanzeigenportale bieten Betrügern einen günstigen Vorwand zur Kontaktaufnahme. Ausserdem werden auch QR-Codes auf Parkuhren überklebt, um Zahlungen von Automobilisten umzuleiten.
Des Weiteren haben die Bevölkerung sowie Organisationen in der Schweiz in der zweiten Jahreshälfte 497'096 Hinweise zu verdächtigen Webseiten über die Meldeplattform «antiphishing.ch» abgesetzt[5]. Das BACS konnte daraus 9'355 eindeutige Phishing-Webseiten identifizieren und geeignete Gegenmassnahmen einleiten.

Übrige Phänomene

Die Zeitspanne, die Organisationen bleibt, um Schwachstellen vor einer Ausnützung durch Angreifer zu beheben, wird immer kürzer. Solche ausgenützten Schwachstellen führen immer wieder zu Datenabflüssen, wobei sie aber auch von staatlichen Akteuren zur Spionage und in seltenen Fällen gar zur Sabotage gegen industrielle Kontrollsysteme eingesetzt werden. Diese globalen Tendenzen müssen zum Schutz vor Cyberbedrohungen in der Schweiz adäquat adressiert werden.

---

4 Rich Communication Services (wikipedia.org)

5 Siehe auch Anti-Phishing Bericht 2024 (ncsc.admin.ch)

Inhalt

Editorial

Im Jahr 2024 erhielt das BACS insgesamt 62'954 Meldungen, was einer Zunahme von über 13'500 Meldungen im Vergleich zum Vorjahr entspricht. Auch wenn nicht jede eingegangene Meldung einem erfolgreichen Cyberangriff entspricht, zeigt die Zahl dennoch eindrücklich, wie stark die Bedrohungslage in der digitalen Welt zugenommen hat. Aber nicht nur Cyberangriffe gefährden unsere IT-Infrastruktur. Auch missglückte Manipulationen an der eigenen IT-Infrastruktur oder das Einspielen fehlerhafter Updates können zu massiven Problemen, teilweise mit weltweiten Auswirkungen, führen. Ein Beispiel für die weitreichenden Auswirkungen eines solchen Fehlers wurde am 19. Juli 2024 eindrücklich vor Augen geführt, als ein fehlerhaftes Sicherheitsupdate des Falcon-Schutzmoduls der Firma CrowdStrike zu weltweiten Computerausfällen führte. Schätzungen zufolge waren an diesem Tag international rund 8,5 Millionen Systeme nicht mehr verfügbar. Der entstandene Schaden wird auf mehrere Milliarden US-Dollar geschätzt.

Diese Ereignisse machen einmal mehr deutlich, was unter Expertinnen und Experten schon lange bekannt ist: Technische Massnahmen allein reichen nicht aus. Sie sind zwar unverzichtbar, aber die Effekte wirken sich in der realen Welt aus und müssen entsprechend auch mit organisatorischen Massnahmen begleitet werden. Die Kombination von technischen und organisatorischen Massnahmen erlaubt es uns erst, die Resilienz unserer Systeme maximal zu erhöhen und im Ernstfall schnell reagieren zu können.
Ein effektives Patch-Management ist von zentraler Bedeutung in der IT-Sicherheit. Es gewährleistet nicht nur den sicheren Betrieb von Applikationen, sondern auch deren Stabilität. Ein nach Kritikalität und Exponiertheit von Systemen gestaffeltes Patch-Management ist auf jeden Fall prüfenswert. Die Kunst liegt darin, eine Balance zwischen notwendigen Tests sowie dem zeitnahen Einspielen von Updates zu finden.
Ebenso wichtig ist das regelmässige Training der IT-Mitarbeitenden bezüglich Reaktion auf IT-Ausfälle. Regelmässige Übungen helfen, im Ernstfall schnell und effektiv handeln zu können. Denn bei einem Vorfall zählt jede Sekunde.

Der vorliegende Halbjahresbericht gibt einen umfassenden Einblick in die Herausforderungen der Schweiz im Bereich der Cybersicherheit des zweiten Halbjahres 2024. Neben den bereits erwähnten Vorfällen werden auch Themen wie DDoS-Angriffe, Cyberspionage oder der Umgang mit Schwachstellen behandelt.
Beim Lesen des vorliegenden Halbjahresberichtes wünsche ich Ihnen zahlreiche wertvolle Erkenntnisse und Ansätze, wie Sie die Sicherheit Ihrer IT-Infrastruktur weiter verbessern und die Resilienz Ihrer IT-Infrastruktur gegen Angriffe und Ausfälle weiter steigern können.

Florian Schütz, Direktor Bundesamt für Cybersicherheit

1 Cyberbedrohungen in der Schweiz – ein Überblick

Kenntnisse der Bedrohungen im Cyberraum spielen eine zentrale Rolle in der Sicherung von Kommunikations- und Informationstechnologie in der Schweiz und international. Die meisten dieser Bedrohungen stehen im Zusammenhang mit Akteuren mit unterschiedlichen Motiven und Fähigkeiten. Der Vorfall des fehlerhaften Softwareupdates des Cybersicherheitsunternehmens CrowdStrike im Juli 2024 verdeutlichte aber beeindruckend, dass auch solche Prozesse im Fokus für ein einwandfreies Funktionieren von kritischen Infrastrukturen stehen müssen. Trotzdem sind die klassischen Bedrohungsphänomene in der Beurteilung der Cybersicherheitslage noch immer relevant, da diese durch Bedrohungsakteure kontinuierlich in ihrer Methodik und Taktik optimiert werden. Aktuelle Entwicklungen hierfür sind beispielsweise bei Betrugsfällen der gezielte Einbezug lokaler Charakteristiken wie z. B. der schweizerdeutschen Sprache, das vermehrte Ausnützen von rechtlichen Grauzonen (vgl. Kap. 5.4) sowie öffentlich publizierter Informationen zur Geschäftshierarchie. Dies macht den Cyberraum zu einem dynamischen Umfeld sowohl für Angreifer als auch für Verteidiger. Die Experimentierfreudigen unter den Cyberakteuren setzen so Trends und schaffen Nachahmer, wenn sich eine Herangehensweise als zielführend bewährt.

Mit insgesamt 28'165 Meldungen ist der Meldeeingang des zweiten Halbjahres 2024 im Vergleich zum ersten Halbjahr (34’789) geringfügig zurückgegangen (vgl. Abb. 1). Ungeachtet dessen ist eine generelle, jährliche Zunahme von 13'574 Meldungen auf ein Total von 62'954[6] Meldungen im Jahr 2024 festzuhalten. Die Zunahme beruht vor allem auf dem Phänomen Fake-Anrufe im Namen von Behörden[7] (vgl. Abb. 2). Während im Vorjahr noch 7'193 Meldungen zu solchen Anrufen erfolgten, waren es im Jahr 2024 21’903 Meldungen. Im Gegensatz dazu gingen Drohungen per E-Mail[8] deutlich zurück, bei denen die Kriminellen die Opfer ähnlich wie bei den Anrufen bezichtigen, eine Straftat begangen zu haben. Das BACS erhielt im Jahr 2023 noch 10'120 Meldungen zu diesem Phänomen, im Jahr 2024 waren es hingegen nur noch 3’825. Dies illustriert den sich seit rund vier Jahren abzeichnenden Trend, dass Betrüger das Telefon wieder vermehrt als Kanal nutzen. Beim Telefon ist der individuelle Aufwand für die Betrüger zwar höher, jedoch können sie so besser auf Opfer eingehen und bei aufkommenden Zweifeln sofort entgegenwirken.
Eine signifikante Zunahme der Meldungen beobachtete das BACS bei betrügerischen Gewinnspielen[9] (3'509 Meldungen), wobei sich die Zahl des Jahres 2024 zum Vorjahr verdreifachte. Besonders in der zweiten Berichtsperiode stiegen die Meldungen von 744 im Jahr 2023 auf 2'398 im Jahr 2024. In vielen Fällen werden die Namen bekannter Lebensmittel- und Einzelhandelsunternehmen, Elektrohändler oder Transportunternehmen in der Schweiz missbraucht.

---

6 Das BACS weist in seinen Statistiken alle eingegangenen Meldungen aus. Darunter sind auch allgemeine Fragen, Informationen und nicht kategorisierbare Meldungen. Im Jahr 2024 waren dies 1’622 Meldungen, die nicht einem bestimmten Phänomen oder Vorfall zugeordnet werden konnten.

7 Um auf das Phänomen Fake-Anrufe im Namen von Fake-Behörden tiefer einzugehen, hat das BACS einen Bericht verfasst, der gleichzeitig mit dem Halbjahresbericht 2024/1 veröffentlicht wurde. Der Bericht beleuchtet unter anderem die Entwicklungen im Zusammenhang mit diesem Phänomen, verschiedene Vorgehensweisen und dafür eingesetzte Technologien sowie die nationale und internationale Rechtslage.

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

9 Betrügerische Gewinnspiele (ncsc.admin.ch)

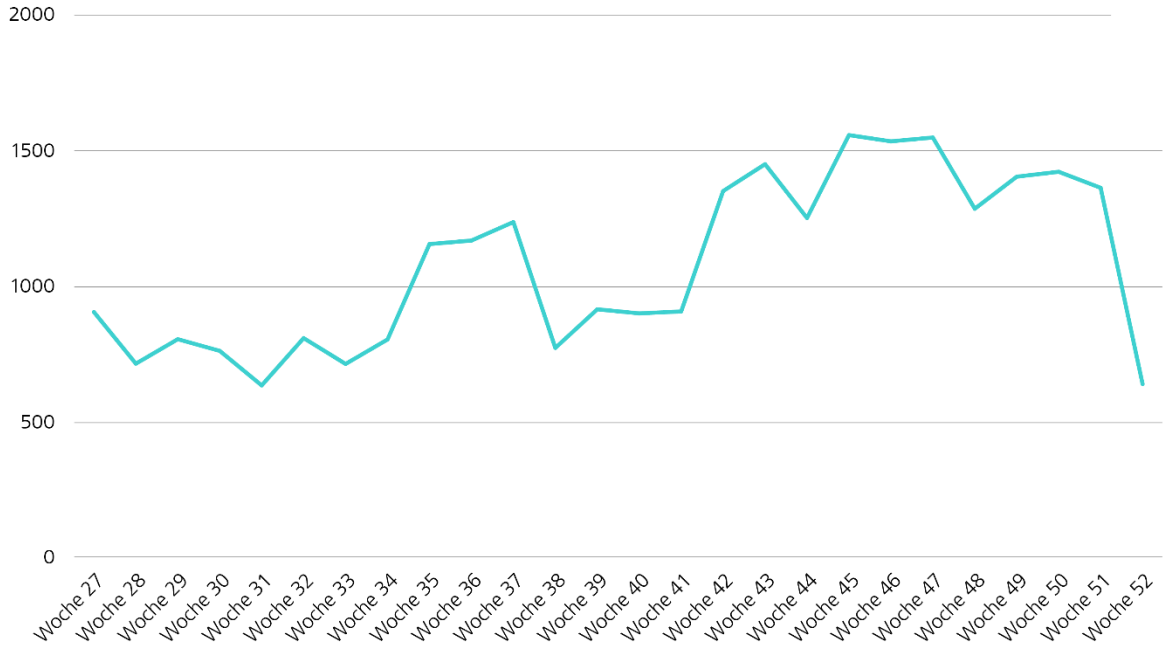


Abb. 1: Anzahl Meldungen pro Woche an das BACS im zweiten Halbjahr 2024, vgl. Aktuelle Zahlen (ncsc.admin.ch)

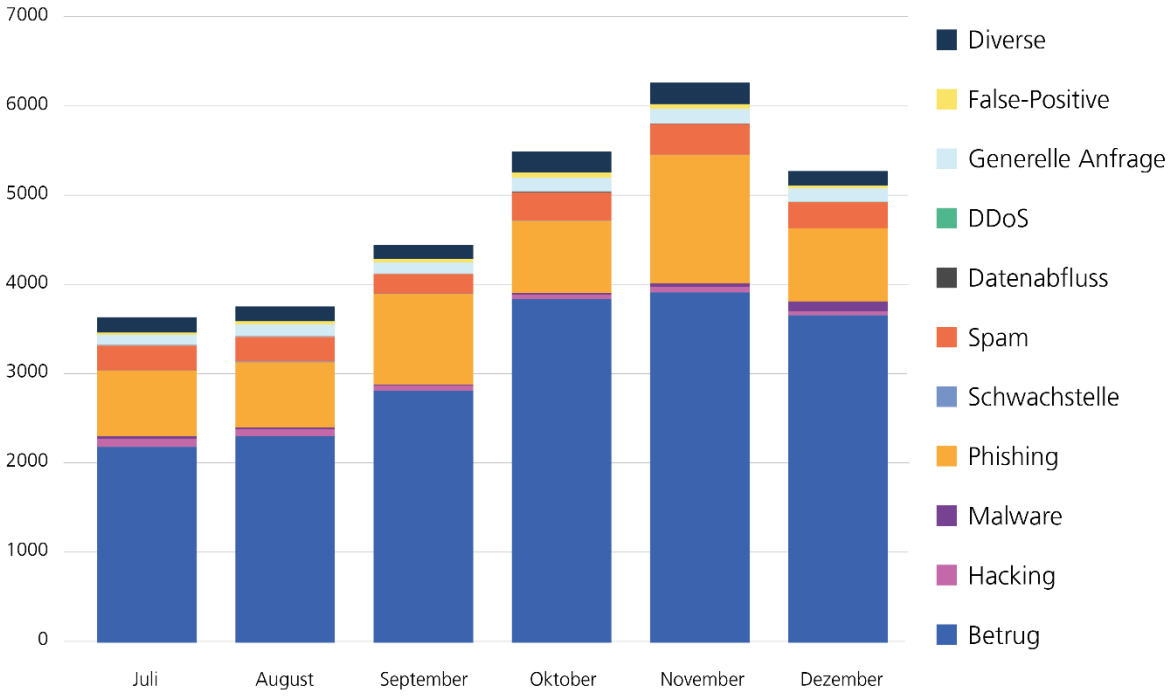


Abb. 2: Meldungen an das BACS im zweiten Halbjahr 2024 nach Kategorien, vgl. Aktuelle Zahlen (ncsc.admin.ch)

Das Verhältnis der Meldungen aus der Bevölkerung (90 %) zu denjenigen von Unternehmen, Vereinen und Behörden (10 %) bleibt weiterhin stabil. Bei den von Unternehmen am häufigsten gemeldeten Betrugsdelikten ist beim Phänomen «CEO-Betrug»[10] ein deutlicher Anstieg mit 487 auf 719 Meldungen zu verzeichnen. Im Jahr 2024 waren Gemeinden und Kirchen von diesem Phänomen übermässig betroffen (vgl. Kap. 5.3). Bei «Ransomware» stoppte der leicht rückläufige Trend. Während im ersten Halbjahr noch 20 Vorfälle weniger gemeldet worden sind, ist die Zahl der eingegangenen Meldungen im zweiten Halbjahr mit 48 verglichen mit der Vorjahresperiode um drei Vorfälle leicht gestiegen. Im ganzen Jahr erreichten das BACS 92 Meldungen zu Ransomware. Generell lässt aber die Anzahl der gemeldeten Fälle keine Aussage über das Schadensausmass zu. Ransomware-Gruppierungen konzentrieren sich zunehmend auf lukrative Ziele, womit der erwartete Schaden pro Vorfall in Zukunft steigen dürfte. Zudem gehen mit Ransomware-Angriffen mittlerweile fast immer Datenabflüsse einher. Dies steigert nicht nur den Schaden für die betroffenen Unternehmen, sondern erhöht auch das Risiko von Folgeauswirkungen für Dritte, deren Informationen sich in den abgeflossenen Datensätzen wiederfinden.

Die Statistik verdeutlicht, dass die Cybersicherheit und der Schutz der Schweiz vor Cyberrisiken eine immerwährende Herausforderung für Wirtschaft, Staat und Gesellschaft darstellt. Entsprechend präsentiert der Halbjahresbericht die Kernphänomene, welche die Bedrohungslandschaft im Cyberraum für die Schweiz und international charakterisieren. Diese beinhaltet «Phishing»[11], «Schadsoftware»[12], Schwachstellen[13], Betrugsfälle und «Social-Engineering»[14], Angriffe auf die Verfügbarkeit von Websites und anderen Internetdiensten (DDoS)[15] und Störungen der Infrastruktur, Datenabflüsse sowie Cyberspionage und -sabotage. Mithilfe der Themenkapitel können sich Leserinnen und Leser einen Überblick über deren aktuelle Ausprägungen, interessante Vorfälle und Entwicklungen verschaffen. Im Sinne der Eigenverantwortung für eine sicherere, digitale Schweiz leitet der Bericht Empfehlungen für die Öffentlichkeit ab, wie diesen Herausforderungen begegnet werden kann.

2 Phishing

Gleich nach Betrug sind Phishing-Versuche die am zweithäufigsten gemeldeten Cybervorfälle ans BACS. Diese ermöglichen es Bedrohungsakteuren, unbemerkt Zugangsdaten, Finanzinformationen und andere vertrauliche Daten von Nutzerinnen und Nutzern zu sammeln. Typisch dabei ist, dass das Austricksen der Nutzerinnen und Nutzer (Social-Engineering) eine wichtige Rolle spielt und dabei keine Schadsoftware zur Anwendung kommt.[16] Während Phishing für einen grossen Empfängerkreis via E-Mail noch immer zur gängigsten Methode gehört, nutzen

[10] CEO-Betrug (ncsc.admin.ch)
[11] Phishing, Vishing, Smishing (ncsc.admin.ch)
[12] Schadsoftware (ncsc.admin.ch)
[13] Schwachstelle (ncsc.admin.ch)
[14] Social Engineering (ncsc.admin.ch)
[15] DDoS-Angriff - Was nun? (ncsc.admin.ch)
[16] International wird das Phänomen Phishing nicht einheitlich verwendet, weshalb in anderen Definitionen auch häufig die Verteilung von Schadsoftware inkludiert wird (vgl. Phishing (attack.mitre.org)). Das BACS exkludiert diese Dimension aber explizit in der angewendeten Definition.

andere Ansätze die Stimme (Voice-Phishing oder Vishing) oder SMS (Smishing), um an sensitive Informationen zu gelangen.

Im Jahr 2024 erhielt das BACS über das Meldeformular 12'038 Meldungen zu Phishing-Versuchen, was einer Zunahme von 2’623 Meldungen im Vergleich zum Vorjahr entspricht. Trotzdem scheint sich aber der Meldeeingang seit dem zweiten Halbjahr auf hohem Niveau mit 5'395 Meldungen zu stabilisieren. Anders zeigt sich die Phishing-Statistik aus der Perspektive der durch das BACS überprüften und bestätigten Phishing-URLs[17]. Hier lässt sich ein steter Zuwachs sowohl jährlich[18] als auch halbjährlich beobachten. So wurden im zweiten Halbjahr 2023 noch 5’242 einzigartige Phishing-URLs rapportiert. Diese Zahl verdoppelte sich im gleichen Zeitraum im Jahr 2024 bereits auf 9’355. Eine detaillierte wöchentliche Entwicklung ist in Abbildung 3 dargestellt. Um die Phishing-Seiten so vertrauenswürdig wie möglich zu gestalten, locken Kriminelle die Opfer immer wieder unerlaubt im Namen bekannter Marken und Unternehmen auf ihre Phishing-Seiten. Am häufigsten wurden in dieser Berichtsperiode der Finanzsektor (23 %), Postdienste (22 %), der öffentliche Verkehr (22 %), der IT- (11 %) und der Telekommunikationssektor (8 %) für Phishing missbraucht. Dieses Verhältnis blieb von Monat zu Monat relativ konstant (vgl. Abb. 4).

Neben den klassischen Phishing-Versuchen gegen Finanzdienstleister thematisieren Phishing-Versuche nach wie vor gefälschte Paketbenachrichtigungen sowie Rückerstattungs-E-Mails im Namen von Lieferanten, der SBB respektive von SwissPass sowie verschiedener Steuerverwaltungen. In dieser Berichtsperiode berücksichtigten Phisher vermehrt lokale Besonderheiten der Schweiz, indem sie beispielsweise im Namen der AHV-Ausgleichskasse Phishings verschickten.[19] Auch Phishing-Versuche gegen Microsoft-365-Konten werden weiterhin beobachtet. Die aktuell verbreitete Vorgehensweise beinhaltet hierbei eine schneeballartige Verteilung von Phishing-E-Mails, das sogenannte «Chain Phishing», bei dem nach der Kompromittierung des E-Mail-Postfachs sofort Phishing-Nachrichten an alle Kontakte im gesamten Adressbuch versendet werden.

Neben E-Mails werden Phishing-Nachrichten aber immer öfter auch über Textnachrichten verschickt. Hier hat das BACS im zweiten Halbjahr 2024 auch die Nutzung des RCS-Systems, respektive iMessage durch die Betrüger beobachtet. Hintergrund dürfte sein, dass die Mobilfunkbetreiber Swisscom, Salt und Sunrise seit 2022 einen SMS-Filter im Einsatz haben und dementsprechend auch betrügerische SMS effizienter stoppen können. Mit der Verwendung von RCS und iMessage können die Betrüger diese Filter umgehen und gelangen so weiterhin an potenzielle Opfer. Wie oftmals im Cybersicherheitsbereich zeigt sich auch hier das Hin und Her zwischen Betrügern und Sicherheitsdienstleistern.

Während der Versand von Phishing-E-Mails und -SMS ein Massengeschäft ist und nur ein geringer Anteil dieser Angriffe mit Erfolg verbunden ist, gab es im Jahr 2024 auch immer wieder Versuche, spezifische Gruppen gezielter anzugehen. Dazu zählen beispielsweise Telefonanrufe von angeblichen Bankmitarbeitern einer Betrugsabteilung, Phishing-Versuche gegen

---

17 Das BACS erhält Meldungen zu Phishing nicht nur in Form von Vorfallsmeldungen, sondern auch über die Plattform antiphishing.ch, welche zusätzliche Quellen miteinspeist. Aufgrund dessen können die hier genannten Zahlen von der Zahl der Direktmeldungen für Phishing abweichen.

18 Eine detaillierte Jahresanalyse zu Phishing in der Schweiz ist im Anti-Phishing Bericht 2024 abgebildet.

19 Vorsicht: Phishing-E-Mails im Namen der AHV (ncsc.admin.ch)

Verkäufer bei Kleinanzeigenplattformen oder das Überkleben von QR-Codes auf Parkuhren. Diese drei Vorgehensweisen werden in den folgenden Unterkapiteln näher erläutert.

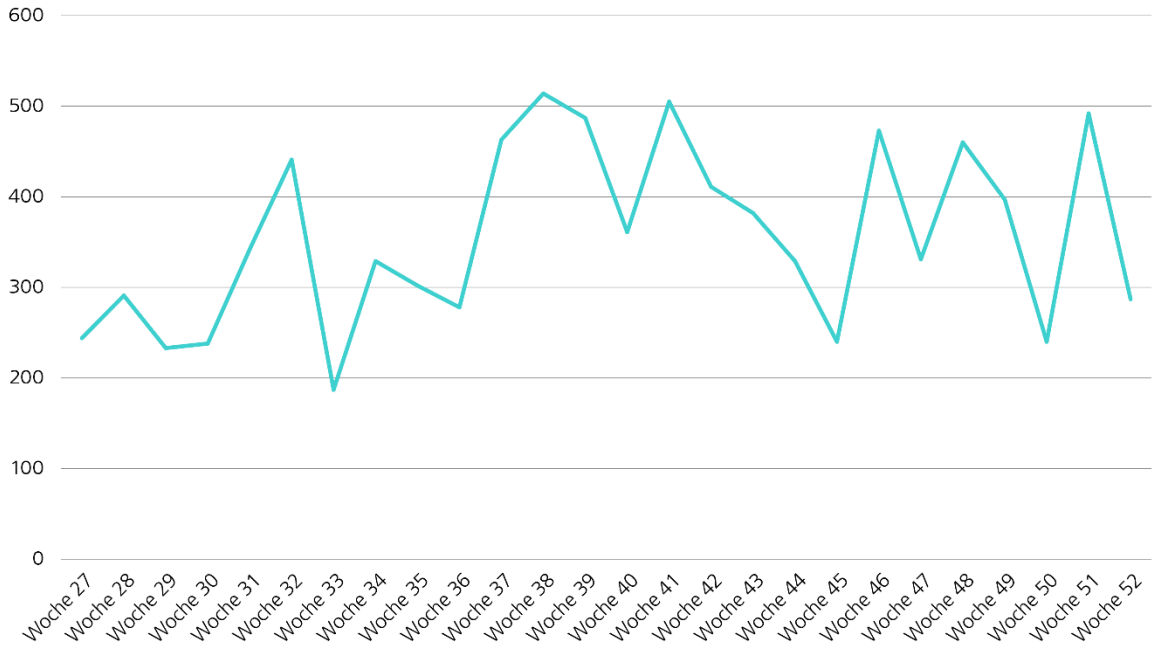


Abb. 3: Anzahl der durch das BACS überprüften und bestätigten Phishing-URLs pro Woche im zweiten Halbjahr 2024

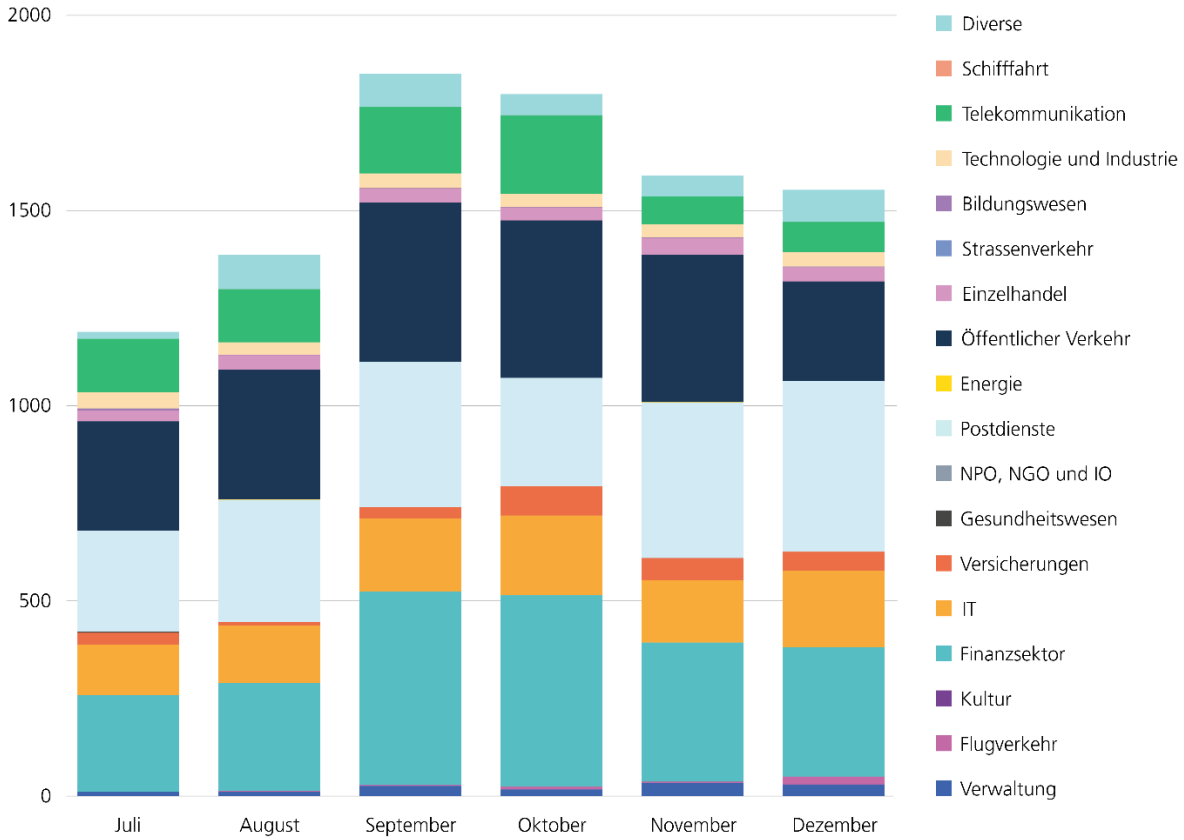


Abb. 4: Anzahl der durch das BACS überprüften und bestätigten Phishing-URLs im zweiten Halbjahr 2024 nach Sektoren von missbrauchten Marken

Empfehlungen

Melden Sie dem BACS verdächtige Phishing-Versuche via reports@antiphishing.ch oder direkt über die Antiphishing-Website (antiphishing.ch). Falls Sie gerne eine Rückmeldung erhalten möchten, können Sie den Phishing-Vorfall auch via Meldeformular oder incidents@ncsc.ch an unsere Spezialistinnen und Spezialisten melden. Mit Ihrer Hilfe kann das BACS gezielt warnen und Massnahmen einleiten, damit die betrügerischen Webseiten vom Internet genommen werden.

2.1 Anrufe von angeblichen Bankmitarbeitenden

Einmal mehr fokussierten mehrere Phishing-Kampagnen in der Berichtsperiode auf Kunden verschiedener Schweizer Banken. Dabei handelte es sich sowohl um Regionalbanken als auch um Grossbanken. Bemerkenswert an diesen Kampagnen war die Kombination verschiedener Methoden, um bei den Opfern glaubwürdig zu wirken. Nebst technischen Mitteln setzten die Kriminellen auf Social-Engineering, indem sie sich z. B. als Angestellte von Banken, Zahlungsportalen wie PayPal oder Polizeikräfte der jeweiligen Betrugsabteilungen ausgaben.

Anrufe von angeblichen Bankmitarbeitenden sind nichts Neues. Bereits in den 2010er-Jahren hat die Melde- und Analysestelle Informationssicherung (MELANI) vor solchen Phishing-Angriffen gewarnt. Die Anrufer gaben damals vor, ein Update beim E-Banking durchführen zu müssen, das anschliessend getestet werden soll. Dabei sollte das Opfer überzeugt werden, eine Fernzugriffs-Software zu installieren, um ein angebliches E-Banking-Update durchzuführen. Mit einer Testzahlung sollte danach die Funktionalität des Systems überprüft werden. Später stellten die Opfer dann fest, dass mehrere tausend Franken auf das Konto eines Komplizen des Betrügers abgebucht worden waren.[20] Aber auch in der jüngeren Vergangenheit hat das BACS wiederholt solche Anrufe registriert. Die grundlegende Vorgehensweise blieb zwar identisch, aber den Vorwand passten die Betrüger in der Zwischenzeit an. Bei den aktuellen Vorfällen geben sich die Betrüger beispielsweise als «Herr Fischer» aus, der bei der Sicherheitsabteilung der Bank arbeitet. Die Anrufer behaupten, eine betrügerische Zahlung stoppen zu wollen. Die angezeigte Telefonnummer entspricht dabei der offiziellen Nummer der Bank, welche die Betrüger angeblich vertreten. Die Nummer wird jedoch von den Betrügern gefälscht, auch bekannt als «Spoofing»[21]. Während in einigen Fällen noch behauptet wird, dass eine Abbuchung für einen Flachbildschirm in einem Elektronikmarkt vorliege, geht es in den jüngeren Fällen meist um eine angebliche, betrügerische Abbuchung von CHF 800. Die Betrüger empfehlen den Opfern, sofort die Betrugsabteilung der Kantonspolizei anzurufen und liefern die dazugehörige Nummer gleich mit. Um die betrügerische Zahlung zu stoppen, soll das Opfer ebenfalls eine Fernzugriffs-Software auf dem Computer installieren und den Zugriff sowohl auf den Computer als auch auf das Bankkonto freigeben. Anstatt die Zahlung dann zu stoppen, werden auch hier betrügerische Zahlungen ausgelöst.

In anderen Varianten erhielt das Opfer nebst dem Anruf vorgängig eine SMS mit einem vierstelligen Code, welcher der angeblichen Betrugsabteilung zur Verifikation genannt werden soll.

---

20 Social Engineering: Neue Angriffsmethode richtet sich gegen Firmen (ncsc.admin.ch)

21 Spoofing (ncsc.admin.ch)

Auch hierbei rief danach ein angeblicher Bankmitarbeiter das Opfer an, um bei vermeintlichen Problemen mit dem E-Banking-Portal zu unterstützen. Insbesondere das akzentfreie Schweizerdeutsch gewisser Betrüger erhöhte nebst den technischen Massnahmen wie z. B. dem Einbezug von Spoofing das Vertrauen. In der Folge gaben Opfer in der Annahme, mit einem Bankmitarbeiter zu telefonieren, auch Sicherheits-Token wie ihren Zweitfaktor heraus. Mit diesem Element erhielten die Betrüger Zugang zum E-Banking der Opfer.

Die Täter greifen zu solchen Methoden, um in Echtzeit an die erforderlichen Zugangsdaten zu gelangen, bevor sie ungültig werden. Verwendet eine Applikation eine Multi-Faktor-Authentifizierung (MFA) ist dies notwendig, weil die Täter sich nur genau zu dem Zeitpunkt einloggen können, wenn das Opfer die eigenen Daten preisgibt. Ein späteres Verwenden der abgegriffenen Daten ist nicht möglich. Dadurch unterscheiden sich solche Vishing-Angriffe von klassischen Phishing-Angriffen, wie beispielsweise das SwissPass-Phishing oder zum Teil auch das Kreditkarten-Phishing, bei denen die Daten auch zu einem späteren Zeitpunkt verwendet werden können. In diesen Fällen reicht eine statische Phishing-Seite.

Empfehlungen

Aktivieren Sie wo immer möglich die Multi-Faktor-Authentifizierung (MFA) als zusätzliche Sicherheit Ihrer Konten. Obwohl MFA das Risiko für eine Kompromittierung enorm reduziert, kann MFA durch Social-Engineering[22]-Techniken ausgehebelt werden. Seien Sie deshalb wachsam vor gefälschten Anfragen – insbesondere via E-Mail und SMS, wenn Sie Zugriffe bestätigen oder Ihren Sicherheits-Token an jemand anderes weiterleiten sollen. Keine Schweizer Bank wird sich per Telefon zur Verifikation ihrer Kunden einen solchen Sicherheits-Token diktieren lassen. Bedenken Sie auch, dass E-Mail-Absender und Telefonnummern leicht gefälscht werden können.

2.2 Phishing nach Kleinanzeigen

Kleinanzeigen bieten Betrügern eine Vielzahl von Angriffsmöglichkeiten. Zu den klassischen Varianten gehört der Verkauf inexistenter Waren oder das Nichtbezahlen von gekaufter und bereits versandter Ware. Daneben haben sich Phishing-Varianten, die sich gegen Verkäufer richten, mittlerweile etabliert. Die Betrüger täuschen Interesse an einem Produkt vor und drängen das Opfer, die Lieferung und den Geldtransfer über einen vom angeblichen Käufer definierten Paketlieferdienst zu tätigen. Ist das Opfer damit einverstanden, werden vom angeblichen Paketlieferdienst fiktive Gebühren verlangt, die das Opfer dann mit der Kreditkarte bezahlen soll. Die Angreifer haben es in diesen Fällen vor allem auf Kreditkartendaten abgesehen. In einigen anderen dem BACS gemeldeten Fällen wurde versucht, ein Twint-Konto mit der Telefonnummer des Opfers zu erstellen. Dabei wurden die Opfer zuerst nach der Telefonnummer und der Kontonummer gefragt. Mit diesen Angaben registrierten die Betrüger ein Twint-Konto. Anschliessend sollte das Opfer über eine Webseite den Sicherheitscode von Twint an diese übermitteln. Denn dieser Code bestätigt, dass die Telefonnummer tatsächlich der Person gehört, die das Konto eröffnen will.

22 Social Engineering (ncsc.admin.ch)

Im Gegensatz zu den unspezifischen und in grosser Zahl versendeten Phishing-E-Mails, bei denen der generische Text einzelne Opfer täuschen soll, betreiben die Phisher in den aktuellen Fällen einen grossen Aufwand. Sie kommunizieren direkt und individuell auf das Opfer abgestimmt, womit sie das Szenario der jeweiligen Gegebenheit anpassen können. So werden im Zusammenhang mit diesen Phishing-Versuchen auch immer wieder Versuche in Schweizerdeutsch festgestellt.

Empfehlungen

Seien Sie vorsichtig bei Forderungen von Käufern. Beharren Sie darauf, dass Versand- und Transaktionsgebühren durch den Käufer bezahlt werden. Schreiben Sie dies auch explizit in die Anzeige.

2.3 Parkgebühren-Phishing mit gefälschtem QR-Code

Online-Bezahlmöglichkeiten beim Parken erfreuen sich steigender Beliebtheit in der Bevölkerung. Moderne Bezahllösungen ermöglichen es Autofahrern, Parkgebühren schnell und effizient über verschiedene Plattformen wie Applikationen auf Mobilgeräten, Webseiten oder speziellen Parkautomaten zu bezahlen. Dabei nutzen diese meist QR-Codes für einen nutzerfreundlichen Bezahlvorgang.

Abb. 5: Überklebter QR-Code auf einem Parkautomaten

Diese Vereinfachung birgt aber auch Gefahren. In verschiedenen Schweizer Städten haben Betrüger in der Berichtsperiode mehrfach die echten QR-Codes auf Parkplätzen mit manipulierten Codes überklebt, welche die Opfer dann auf eine falsche, aber täuschend echt aussehende Bezahl-Webseite leiteten. Dabei konnte zwischen einer Zahlung mit Twint oder einer Kreditkartenzahlung gewählt werden.

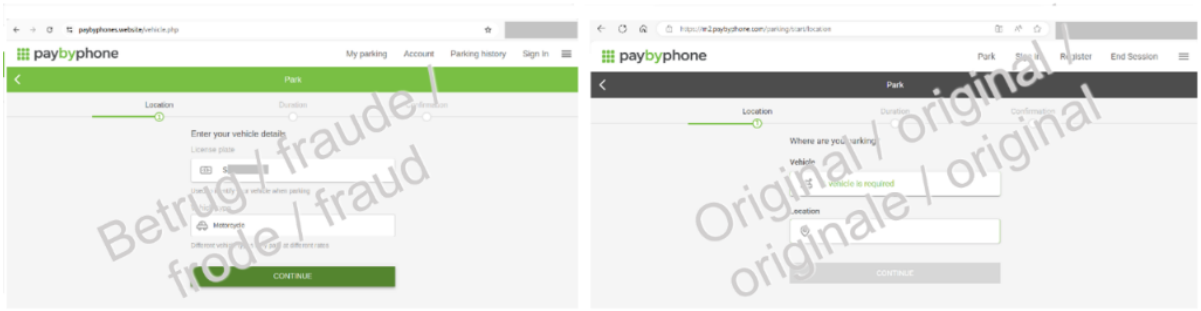


Abb. 6: Täuschend echte Betrugs-Webseite (links). Nur die Internetadresse verrät, dass es eine Fälschung ist.

Da die Opfer in der Regel bei der Suche nach einem Parkplatz unter zeitlichem Druck stehen, werden die Zahlungsdetails, wie der abgebuchte Betrag oder der Empfänger, kaum kontrolliert. Das Opfer autorisiert die Zahlung, wodurch mehrere hundert Franken auf ein betrügerisches Konto transferiert werden.

Im Gegensatz zu den klassischen Phishing-Methoden müssen die Betrüger bei dieser Variante mindestens einmalig vor Ort sein, um die Aufkleber anzubringen. Dabei riskieren sie, während ihrer Straftat entdeckt zu werden. Diese Versuche wurden aber nicht nur einmal, sondern immer wieder von Neuem durchgeführt. Nachdem die Betrugsversuche bemerkt und die Aufkleber entfernt worden waren, dauerte es in einigen Fällen nur kurze Zeit, bis neue Aufkleber von den Betrügern angebracht worden waren.

Empfehlungen

Betrachten oder berühren Sie einen physischen, öffentlichen QR-Code, bevor Sie ihn scannen, um zu prüfen, ob es sich um einen Aufkleber handelt. Achten Sie darauf, ob die aufgerufene Internetadresse (URL) der erwarteten Adresse entspricht. Schauen Sie genau hin, denn die Abweichungen können sehr gering ausfallen. Brechen Sie unbedingt den Zahlungsvorgang ab, wenn Sie Ungereimtheiten feststellen.

3 Schadsoftware

Um sich auf einem Gerät oder in einem Netzwerk festzusetzen, ist Schadsoftware (sogenannte «Malware») weiterhin ein Hauptwerkzeug von Cyberkriminellen. Das nachfolgende Unterkapitel behandelt den Einsatz von Schadsoftware, um Systeme initial zu infizieren. Auffällig waren hierbei Versuche, Schadsoftware im Namen von Schweizer Krankenversicherern und Inkassounternehmen zu verteilen. Auch beobachtete das BACS neue Methoden, welche potenzielle Opfer mittels gefälschter «CAPTCHAs»[23] verleiten wollen, ihre Systeme durch Ausführen von bösartigem Programmcode gleich selbst zu infizieren. Für einen Grossteil der Unternehmen stellt Ransomware weiter die grösste Bedrohung dar. Das zweite Unterkapitel beleuchtet Vorfälle in der Schweiz und relevante Entwicklungen zu diesem Phänomen im internationalen Kontext. Abschliessend beschreibt das dritte Unterkapitel eine Kampagne, die über QR-Codes auf klassisch versendeter Briefpost versucht, die Empfänger zur Installation einer mit Schadsoftware infizierten Android-App zu bewegen.

3.1 Initialer Zugang mit Schadsoftware

Zur Kompromittierung von Computersystemen nutzen Cyberkriminelle häufig Schadsoftware als Einfallstor. In vielen Fällen werden diese Angriffe durch sogenannte Social-Engineering Methoden begleitet. Diese Vorgehensweise soll Benutzerinnen und Benutzer dazu verleiten, bestimmten Handlungen, wie beispielsweise dem Ausführen der erwähnten Schadsoftware,

[23] CAPTCHAs sind Aufforderung bei Internetformularen, bei welchen Nutzerinnen und Nutzer bestätigen müssen, dass sie ein Mensch und keine Maschine sind. Dies beinhaltet beispielsweise Rechenaufgaben oder das Auswählen aller Bilder, bei denen Tiere, Autos, Brücken oder ähnliches abgebildet sind.

nachzukommen. Im Folgenden werden die wichtigsten Trends im Bereich des initialen Zugangs mit Schadsoftware und die begleitenden Social-Engineering-Methoden für die zweite Hälfte des Jahres 2024 beleuchtet. Der Fokus liegt dabei auf den Entwicklungen in der Schweiz.

Im Berichtszeitraum wurden in der Schweiz zahlreiche Versuche beobachtet, Systeme mit Schadsoftware wie «Agent Tesla», «SnakeKeyLogger», «Formbook», «Lumma Stealer», «Vidar Stealer», «Strela Stealer» oder der mobilen Schadsoftware «Coper/Octo2» zu infizieren. Die meisten dieser Verteilkampagnen wiesen keine spezifischen Merkmale für die Schweiz auf. Das Vorgehen unterschied sich nicht vom internationalen Muster. Dies lässt auf ein opportunistisches Vorgehen der Kriminellen schliessen, die Systeme infizieren wollen, ohne diese davor gezielt auszuwählen. Zwei Kampagnen, die im November 2024 stattfanden, stachen jedoch als spezifisch für die Schweiz heraus: Die eine verteilte die mobile Schadsoftware Coper/Octo2 per physischer Briefsendung mit einem Link, der zur Schadsoftware führte, wobei die Firmenidentität von MeteoSchweiz missbraucht wurde (vgl. Kap. 3.3). Die andere missbrauchte in einer E-Mail-Kampagne die Firmenidentität von verschiedenen Schweizer Unternehmen, um Lumma Stealer zu verbreiten.

Das BACS erhielt zahlreiche Meldungen zu verdächtigen E-Mails, die angeblich von einem Schweizer Inkassounternehmen oder einer Schweizer Krankenkasse versendet worden waren. In diesen Nachrichten wird auf eine fiktive Gutschrift oder Zahlungserinnerung hingewiesen. Der Empfänger wird aufgefordert, auf einen Link zu klicken, um die Rechnung einzusehen. Durch das Anklicken wird eine bösartige Datei heruntergeladen, die bei Ausführung auf einem Windows-System ein Skript auslöst. Dieses Skript startet einen ersten Loader, der von verschiedenen IT-Sicherheitsfirmen als «Emmenhtal»[24] oder «PEAKLIGHT»[25] bezeichnet wird. In der Folge wird ein Informationsdiebstahl-Trojaner («Infostealer») des Typs Lumma Stealer installiert. Das Programm sammelt und versendet sensitive Informationen wie Login-Daten, Browser-Cookies oder Informationen von Wallets für Kryptowährungen.[26]

Darüber hinaus wurden in der Schweiz weitere Verteilkampagnen von Lumma Stealer beobachtet, die jedoch mit den international üblichen Methoden durchgeführt worden waren. Eine dieser Vorgehensweisen, die als «ClickFix» bezeichnet wird, ist in letzter Zeit vermehrt beobachtet worden. Dabei werden Benutzer durch einen gefälschten CAPTCHA getäuscht, welcher eigentlich zur Unterscheidung zwischen realen und automatisierten Nutzern dient. Durch das Anklicken des «Ich bin kein Roboter»-Buttons wird der bösartige Code in die Zwischenablage kopiert und die Webseite fordert die Opfer auf, die Tastenkombinationen «Windows + R», «Strg + V» und «Eingabe» zu drücken, um die Überprüfung abzuschliessen.[27] Tatsächlich führt diese Aktion jedoch zum Ausführen eines bösartigen Skriptes und zur Installation der Schadsoftware. Diese Methode, bei der Nutzerinnen und Nutzer unbewusst bösartigen Code ausführen, scheint sehr effektiv zu sein, da viele Variationen beobachtet worden sind, die verschiedene Arten von Schadsoftware verteilen. So wurden beispielsweise YouTube-Kanäle entweder kompromittiert oder extra dafür geschaffen, um betrügerische Anleitungen zu veröffentlichen, die Nutzer dazu bringen sollen, Schadcode auszuführen. Die Behauptung, dass

[24] Emmenhtal: A little-known loader distributing commodity infostealers worldwide (orangecyberdefense.com)
[25] PEAKLIGHT: Decoding the Stealthy Memory-Only Malware (google.com)
[26] Vorsicht: E-Mails mit Schadsoftware im Namen von Inkassounternehmen und Krankenkassen (ncsc.admin.ch)
[27] Wie Angreifer versuchen, mit betrügerischen CAPTCHAs Schadsoftware zu verteilen (ncsc.admin.ch)

dieser Code die Lösung für ein bestimmtes Anliegen sei, wie etwa Kryptowährungen, Software-Lizenzierung oder Computerprobleme, dient dabei als Vorwand.[28]

Ein weiterer erwähnenswerter Fall in der Schweiz betraf einen Entwickler, der via LinkedIn kontaktiert worden war. Er wurde unter dem Vorwand eines Jobangebots zum Download einer Schadsoftware und deren Ausführung verleitet. Diese zielte darauf ab, insbesondere Daten im Zusammenhang mit Kryptowährungen zu stehlen. International berichteten mehrere Sicherheitsdienstleister über ähnliche Kampagnen. Der vorliegende Fall ist möglicherweise Teil einer internationalen Kampagne namens «Contagious Interview», die sich spezifisch an IT-Entwickler richtete und deren Ziel darin bestand, diese via LinkedIn zu täuschen, um Schadsoftware während des Bewerbungsprozesses auszuführen.[29] Dies geschah beispielsweise durch das Verstecken des bösartigen Codes in einem Programm, das der Bewerber einer Fehlersuche unterziehen solle, oder in einem Installer für Videokonferenz-Software, die für das Vorstellungsgespräch benötigt wurde. Darüber hinaus gelang es Angreifern in einer verwandten Kampagne, auf der NPM-Plattform (Node Package Manager) infizierte Kopien rechtmässiger Software-Pakete zu verbreiten. NPM ist eine Plattform, die es Programmierern ermöglicht, sogenannte «Bibliotheken» oder «Pakete» zu teilen, die dann für die Entwicklung von Programmen verwendet werden. Die Angreifer nutzen das Vertrauen in solche Plattformen aus, indem sie täuschend echte Kopien mit ähnlich klingenden Namen veröffentlichen.[30] In einem besonders ausgeklügelten Fall Ende des Jahres gelang es den Angreifern sogar, bösartigen Code in Updates von zwei originalen Paketen einzuschleusen. Dadurch wurden Systeme, welche die kompromittierte Version dieser Pakete installiert hatten, mit der Krypto-Mining-Software «XMRig» infiziert.[31]

Diese Fälle demonstrieren lediglich eine kleine Auswahl der vielfältigen Schadprogramme und Angriffsmethoden, die von Cyberkriminellen eingesetzt werden. Um profitabel zu sein, müssen diese Kriminellen einen Ertrag erzielen, der abstrahiert aus zwei Variablen besteht: dem erforderlichen Investitionsaufwand und dem zu erwartenden Gewinn. Bis anhin hatten Fortschritte im Feld der Künstlichen Intelligenz (KI) noch keinen disruptiven Einfluss auf die Entwicklung dieser Bedrohungen. Allerdings ist eine zunehmende Integration von KI-Mitteln durch Kriminelle festzustellen.[32] Sie optimieren spezifische Aufgaben und gleichen bestehende Defizite aus, wodurch der erforderliche Aufwand gesenkt werden kann. Die zunehmende Verbreitung von Kryptowährungen und deren Speicherung auf privaten Geräten fördert die Rentabilität solcher Angriffe zusätzlich. Es ist daher davon auszugehen, dass solche Bedrohungen auch in Zukunft ein probates Mittel bleiben.

---

28 Your Data Is Under New Lummanagement: The Rise of LummaStealer (cybereason.com)

29 Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers (paloaltonetworks.com)

30 Tenacious Pungsan: A DPRK threat actor linked to Contagious Interview (datadoghq.com)

31 Supply Chain Attack on Rspack npm Packages Injects Cryptojacking Malware (socket.dev)

32 Siehe auch Halbjahresbericht 2024/1; Kap. 5.1.

Empfehlungen

Klicken Sie in verdächtigen Nachrichten nicht auf Links, öffnen Sie keine angehängten Dateien und scannen Sie keine QR-Codes. Fragen Sie im Zweifelsfall über andere Kanäle beim vermeintlichen Absender nach, ob die Nachricht tatsächlich von ihm stammt.

Verifizieren Sie bei der Suche nach Software im Internet vor dem Download, dass Sie sich auf den Websites der Hersteller oder einer anderen vertrauenswürdigen Website – z. B. einer bekannten Computerzeitschrift – befinden. Beachten Sie besonders beim Nutzen von Suchmaschinen, ob die angezeigte Website als bezahlte Werbung deklariert ist oder nicht. Handelt es sich um bezahlte Werbung, ist Vorsicht geboten, da Angreifer oft auf diese Methode setzen, um bei Suchergebnissen ganz oben platziert zu sein.

Seien Sie immer vorsichtig, wenn sich ein Download-Fenster öffnet.

Lassen Sie Programme, wenn immer möglich, automatisch aktualisieren. Ansonsten verwenden Sie die integrierte Update-Funktion oder laden Sie die neueste Version direkt beim Hersteller herunter.

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

3.2 Ransomware

Dieses Unterkapitel stellt die aktuelle Lage bezüglich Ransomware dar. Bei dieser Art des Angriffs verschlüsseln Cyberkriminelle mithilfe einer Schadsoftware Daten auf den IT-Systemen des Opfers, was die Daten für das Opfer unbrauchbar macht.[33] In der Regel exfiltrieren die Kriminellen zugleich die Daten und fordern im Anschluss vom Opfer ein Lösegeld. Wenn das Opfer zahlt, stellen die Kriminellen ein Entschlüsselungstool (Dekryptor) und die Nichtweiterverbreitung der gestohlenen Daten in Aussicht. Zuerst beleuchtet der Bericht die Lage in der Schweiz, danach die Vorfälle und Trends auf internationaler Ebene.

3.2.1 Ransomware-Aktivitäten in der Schweiz

Nach der Zerschlagung grosser Ransomware-Gruppen wie «LockBit» und «ALPHV» im ersten Halbjahr vom Jahr 2024 mussten sich einige der Entwickler und Komplizen von Ransomware-Gruppen nach neuen Allianzen umsehen. Dies führte zu einem verstärkten Wettbewerb, da andere Ransomware-Gruppen – wie z. B. «RansomHub»[34], «Akira», «BlackCat» und «Play»[35] – versuchten, diese erfahrenen Operatoren zu einer Zusammenarbeit durch attraktivere Arbeitsbedingungen zu bewegen. Wie der folgende Abschnitt zu Vorfällen in der Schweiz zeigt, dominieren auch einige der bekannteren Ransomware-Namen wie Akira, LockBit und «INC Ransom» die Schweizer Ransomware-Statistiken.

Beim Phänomen Ransomware stoppte statistisch der leicht rückläufige Trend der letzten Jahre. Während im ersten Halbjahr noch 20 Vorfälle weniger gemeldet worden sind, ist die Zahl der eingegangenen Meldungen im zweiten Halbjahr verglichen mit der Vorjahresperiode

33 Ransomware (ncsc.admin.ch)

34 RansomHub Overtakes LockBit as Most Prolific Ransomware Group (infosecurity-magazine.com)

35 Play & LockBit Ransomware Join Hands to Launch Cyber Attacks (gbhackers.com)

mit 48 Fällen um drei Vorfälle leicht gestiegen. Dementsprechend sind die Meldungen im Jahr 2024 verglichen zum Vorjahr um 17 Meldungen von 109 auf 92 Vorfälle zurückgegangen. Im Gegensatz dazu ist der Trend stabil, dass sich Ransomware grösstenteils gegen Unternehmen richtet.[36] Ransomware-Vorfälle gegen Privatpersonen – insbesondere gegen deren NAS-Geräte – sind im zweiten Halbjahr deutlich gesunken. Nur gerade acht Vorfälle betrafen Privatpersonen.

Werden die am häufigsten gemeldeten Ransomware-Gruppen betrachtet (vgl. Abb. 7), so fällt vor allem Akira mit 15 Vorfällen auf, da diese doppelt so viele Vorfälle wie die zweithäufigste Ransomware-Variante LockBit verantwortete. Akira charakterisiert sich durch ein opportunistisches Angriffsverhalten, was bereits im ersten Halbjahr 2024 beobachtbar war. Dies resultiert in einer verhältnismässig hohen Anzahl Opfer, die verschiedene Sektoren und Grössen von Unternehmen miteinbeziehen. Anders wurde LockBit zwar durch die Polizeiaktion «Cronos» Mitte Februar 2024 ausgebremst, gehört aber immer noch zu den am häufigsten gemeldeten Ransomware-Varianten in der Schweiz. Bei der Polizeioperation übernahmen und zerstörten Strafverfolgungsbehörden Infrastruktur von LockBit, zersplitterten das Netzwerk der Beteiligten und stellten Entschlüsselungstools gratis für Opfer zur Verfügung. Dennoch verbleibt die Ransomware-Aktivität auf einem stabilen Niveau, was die LockBit-Gruppe auch mit einer Ankündigung für eine neue Version – «LockBit 4.0» – per Februar 2025 im Dezember 2024 unterstreicht.[37]

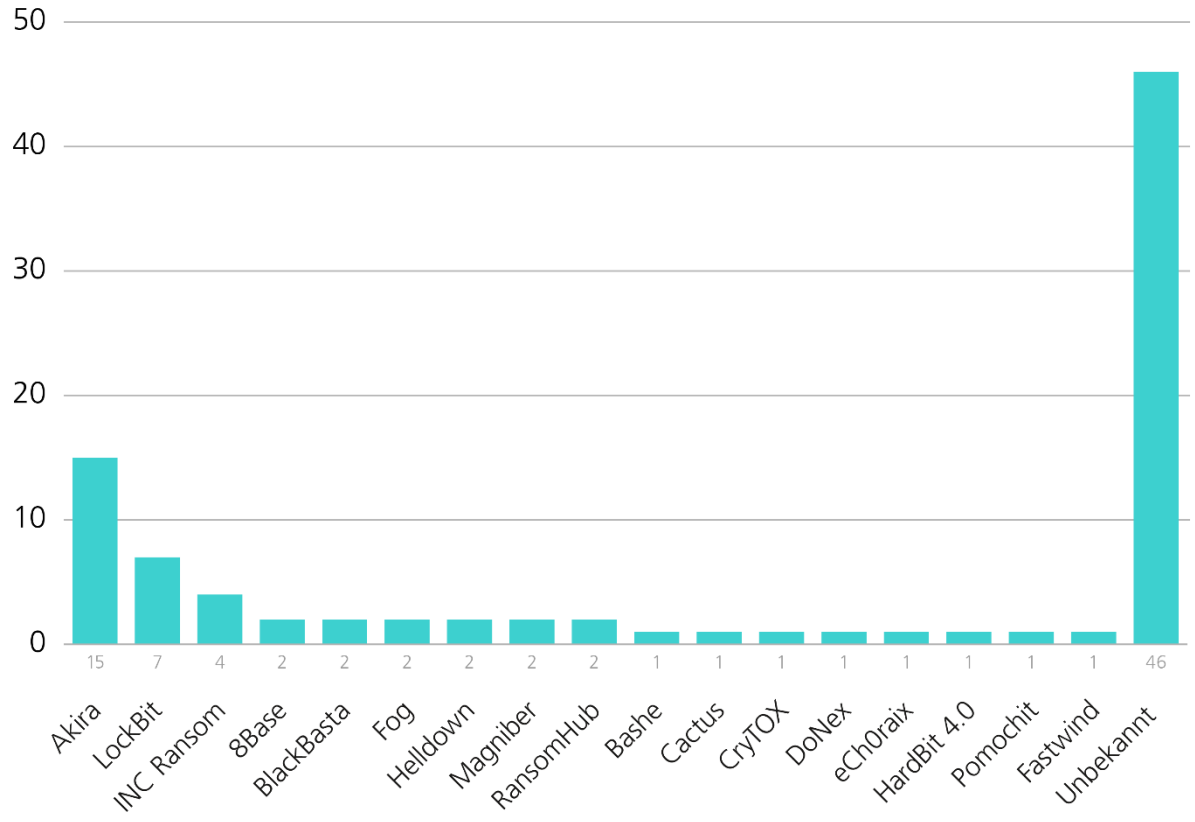


Abb. 7: Anzahl der gemeldeten Ransomware-Vorfälle an das BACS im zweiten Halbjahr 2024

[36] Siehe Halbjahresbericht 2024/1; Schlussfolgerung im Kap. 3.2.1.

[37] LockBit Admins Tease a New Ransomware Version (infosecurity-magazine.com)

An dritter Stelle folgt mit vier gemeldeten Fällen die Ransomware INC Ransom. Der Rest des Feldes besteht aus 14 weiteren Ransomware-Familien. Neben einigen bekannteren Akteuren verteilt sich die Bedrohungsaktivität auf viele – darunter auch kleinere Gruppen, was auf eine Entwicklung zu einem modulareren und dezentralisierten Ansatz hindeutet. Grosse Ransomware-Gruppen sind somit vielen kleinen Gruppen gewichen, in denen Ransomware-Angreifer abwechselnd oder gleichzeitig für mehrere verschiedene Operationen tätig sind.[38]

Neue Ransomware-Varianten

Zu den vom BACS in der Schweiz beobachteten neuen Ransomware-Familien zählen[39]: «RansomHub», «INC Ransom», «Fog», «Helldown», «Pomochit» und «Cicada». Obwohl diese Ransomware-Varianten als neu gelten, weisen diese häufig Ähnlichkeiten zu schon bestehender Schadsoftware auf, wie dies beispielsweise mit Cicada der Fall ist.[40] Im Fall der Ende Sommer aufgekommenen Variante Helldown griff die gleichnamige Gruppe einen Schweizer IT-Dienstleister an und stahl Daten im Umfang von 67 GB.[41] Über Helldown ist noch immer wenig bekannt. Meist nutzten sie Schwachstellen aus, um die Netzwerke der Opfer zu infiltrieren und die Ransomware zu installieren. Deren Ransomware-Code ist zumindest teilweise von «LockBit 3.0» abgeleitet worden. Erstmals bekannt wurde die Gruppe nach der breiten Ausnutzung einer Schwachstelle in den Zyxel-Produkten.[42]
RansomHub ist ein im Februar 2024 erschienener Anbieter für «Ransomware-as-a-Service» (RaaS), wobei frühere Anwender von ALPHV und LockBit rekrutiert wurden. Seit Februar 2024 zählt RansomHub bereits über 210 Opfer, darunter auch mindestens drei Opfer aus der Schweiz: ein Innenarchitekturunternehmen aus der Romandie, ein Industrieunternehmen aus dem Kanton Zürich und ein Software-Unternehmen aus dem Kanton Bern[43]. Die Ransomware zielt auf schlecht konfigurierte Cloud-Speicherorte und Backups ab. Gemäss einer Analyse der US-amerikanischen Behörde «Cybersecurity and Infrastructure Security Agency» (CISA) gehören kritische Infrastrukturen ebenfalls zur Zielgruppe von RansomHub.[44]
Von der seit Juli 2023 aktiven Schadsoftware INC Ransom[45] waren schon das Gesundheitswesen, die Finanzbranche sowie mindestens ein Verein und mehrere KMUs in der Schweiz betroffen. Der initiale Zugang kann bei dieser Software variieren, wobei die beobachteten Methoden Spear-Phishing per E-Mail sowie die Ausnutzung von Schwachstellen umfassen.

Aktivitäten bereits bekannter Ransomware-Varianten

Im Berichtshalbjahr gab es auch Angriffe mit bereits bekannteren Ransomware-Varianten wie «Akira» oder «Play», welche die Bereiche Industrie, Immobilien, Bildungswesen, Dienstleistung und Handel, Finanzwesen sowie KMU in der Schweiz angriffen. In einem Fall von «Play» war das Opfer ein Schweizer Vermögensverwalter. Bei einem Viertel der in den abgeflossenen

---

38 Siehe Halbjahresberichts 2024/1; Schlussfolgerung im Kap. 3.2.
39 Neue Ransomware-Banden zielen auch auf Schweizer Firmen (inside-it.ch)
40 Cicada 3301 - Ransomware-as-a-Service - Technical Analysis (truesec.com)
41 Ransomware-Angriff auf Schweizer IT-Dienstleister (inside-it.ch)
42 Helldown Ransomware: an overview of this emerging threat (sekoia.io)
43 Aufstrebende Ransomware-Bande attackiert Schweizer Software-Firma (inside-it.ch)
44 #StopRansomware: RansomHub Ransomware (cisa.gov)
45 Ransomware Spotlight: INC (trendmicro.com)

Daten erwähnten Kundinnen und Kunden handelte es sich um Hochrisiko- oder politisch exponierte Personen verschiedener Länder.[46] Dieser Fall zeigt exemplarisch, dass die Veröffentlichung sensitiver Personendaten nicht nur Risiken für das Unternehmen selbst darstellt, sondern auch für in Daten erwähnte Privatpersonen eine Gefährdung sein kann.

Empfehlungen

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

3.2.2 Ransomware als globale Herausforderung

Vielfältige Techniken finden Einzug bei Angriffsversuchen

Die veränderte Dynamik im Ökosystem rund um Ransomware zwang gewisse Ransomware-Gruppen dazu, flexibler zu werden und sich im Hinblick auf Technik und Taktik weiterzuentwickeln. Die bereits im ersten Halbjahr 2024 beobachtete Ransomware-Gruppe «Black Basta» ist ein Beispiel hierfür.[47] Die Gruppe, die bekannt für ihre hochkarätige Zielauswahl ist, setzte für die Verteilkampagnen ihrer Ransomware neue und/oder vielseitigere Methoden zur Infektion ein.[48] Dies umschloss unter anderem:

- E-Mail-Bombing: Die Angreiferinnen und Angreifer fluten das E-Mail-Konto der Opfer mit Tausenden von Spam-Nachrichten, um die E-Mail-Konten der Empfänger zu überlasten oder andere verbotene Aktivitäten zu verbergen.
- Falscher Support: Mithilfe von kompromittierten Microsoft-365-Konten senden die Kriminellen Nachrichten oder rufen über die Kollaborationsplattform MS Teams an und geben sich als technischen Support der Organisation aus. Sie bringen die Opfer dazu, Überwachungs- und Fernwartungssoftware (RMM: Remote Monitoring and Management) herunterzuladen oder senden ihnen schädliche QR-Codes, um Zugang zur gewünschten IT-Umgebung zu erhalten.
  Eine Variante des falschen Supports besteht darin, den Fernzugriff auf das Gerät des Opfers anzufordern. Damit muss das Opfer nicht überzeugt werden, selbst schädlichen Inhalt herunterzuladen. Durch die vorhandenen Funktionalitäten von Microsoft Quick Assist oder der Steuerungsfreigabe in MS Teams übernehmen die Angreiferinnen und Angreifer die Kontrolle über das Gerät des Opfers und installieren schliesslich Ransomware, sofern sie Administratorenrechte erlangen können.

Die neuste Verteiltechnik von Black Basta mithilfe des QR-Codes über MS Teams wurde auch gegen Schweizer Unternehmen eingesetzt.[49] Eine Einflussgrösse zum Wechsel auf diese neue Angriffsmethode könnte die Zerschlagung des Botnets «Qakbot» im Jahr 2023 gewesen

---

46 Boreal Capital: Hacker erbeuten Daten von Vermögensverwalter (tagesanzeiger.ch)

47 Siehe Halbjahresbericht 2024/1; Kap. 3.2.1.

48 Sophos tracks two ransomware campaigns using “email bombing,” Microsoft Teams “vishing” (sophos.com), ReliaQuest Uncovers New Black Basta Social Engineering Technique (reliaquest.com)

49 Woche 44: «Black Basta» - Mittels Spam zur Verschlüsselung: Ausgeklügelte Angriffsvariante auf Unternehmen (ncsc.admin.ch)

sein, welche neue Partnerschaften mit Händlern für den initialen Zugang und neue personalisierte Tools nötig gemacht haben.[50]
Diese Anpassungsfähigkeit sowie der Wille zur Diversifizierung und Optimierung der eigenen Operationen zeigte sich auch bei anderen Gruppen wie Akira.[51] Der Fokus der Gruppe liegt nun vorwiegend auf der Entwendung von Daten. Im Vorfeld dieses Vorgangs führen die Angreifer eine Vorauswahl und eine Sortierung der gesammelten Daten durch.[52] Sie recherchieren gezielt, um wertvolle sensitive Informationen zu extrahieren, darunter beispielsweise Finanzdaten, Personal- und Patientenakten, klassifizierte Dokumente, Daten zu eingesetzten Informationstechnologien und Netzwerken sowie weitere besonders schützenswerte Daten.

Tendenzen bei Opfern und Bedrohungsakteuren

Gemäss einer Studie von Semperis im Jahr 2024 zahlten mehr Opfer als erwartet das Lösegeld nach einer Ransomware-Infektion.[53] Als Hauptgründe wurden die Notwendigkeit der möglichst raschen Wiederaufnahme der Geschäftstätigkeiten, das Schützen der Patienten-, Kunden- oder Unternehmensdaten oder die Gefahr eines Reputationsschadens genannt. Ein weiteres Argument war die Cyberversicherung, welche die Kosten deckte.

Empfehlungen

Generell raten das BACS und seine internationalen Partner[54] den Opfern von Ransomware ab, Lösegeld zu zahlen. Es besteht keine Garantie, dass Cyberkriminelle ihr Wort halten. Mit einer Lösegeldzahlung werden die Cyberkriminellen finanziell unterstützt, um ihre Strukturen weiter auszubauen und weitere Angriffe auszuführen

Eine weitere im Berichtshalbjahr beobachtete internationale Tendenz ist die Verwendung von Ransomware durch Bedrohungsakteure, deren Motive nicht ausschliesslich finanzieller Natur sind. Gemäss Microsoft setzen eng mit einem Staat verbundene Cyberspionage-Akteure Ransomware als letzten Schritt ihrer Operationen ein, um einen finanziellen Nutzen, Störungen, eine Ablenkung, falsche Attribution oder die Löschung von Beweisen zu erreichen.[55] Dies ist mutmasslich bei der chinesischen Gruppe «ChamelGang»[56] und bei nordkoreanischen, iranischen oder russischen[57] Gruppierungen der Fall. Im Zusammenhang mit Nordkorea zeigt ein Forschungsbericht auf, wie der Staat mit Mitgliedern der Gruppe Play zusammengearbeitet hat.[58]

Hacktivistengruppen, wie beispielsweise «CyberVolk» mit angeblichem Bezug zu Indien, setzen Ransomware nun auch gegen staatliche und öffentliche Institutionen in Ländern ein, die

50 UNC4393 Goes Gently into the SILENTNIGHT (cloud.google.com)
51 Akira ransomware continues to evolve (talosintelligence.com)
52 Ransomware-driven data exfiltration: techniques and implications (sekoia.io)
53 Ransomware-Risikobericht (semperis.com)
54 Guidance for organisations considering payment in ransomware incidents (ncsc.gov.uk)
55 Microsoft Digital Defense Report 2024 (microsoft.com)
56 ChamelGang | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware (sentinalone.com)
57 Escalating Cyber Threats Demand Stronger Global Defense and Cooperation (microsoft.com)
58 Jumpy Pisces Engages in Play Ransomware (unit42.paloaltonetworks.com)

gegensätzliche Interessen verfolgen.[59] Im Gegensatz dazu betreiben gewisse hauptsächlich finanziell motivierte Gruppen wie «FunkSec»[60] nebenbei noch Hacktivismus.

Ausnutzung von Schwachstellen bei Ransomware-Angriffen

Die Ausnutzung von Schwachstellen in den Authentifizierungs- und Fernzugangssystemen ist als initialer Zugriff bei Ransomware-Angriffen beliebt (vgl. auch Kap. 4).[61] Bei den ausgenutzten Schwachstellen handelt es sich zudem oft um noch unbekannte Zero-Day-Schwachstellen. In diesem Fall werden die Opfer selten gezielt durch die Cyberkriminellen ausgesucht. Letztere durchsuchen das Internet vielmehr auf verwundbare virtuelle private Netzwerke (VPN) und Firewalls, deren Verwaltungsschnittstellen im öffentlichen Internet zugänglich sind. Da solche Lösungen als Zugangspunkt zu internen Netzwerken dienen, werden sie oft zum Einfallstor von Ransomware-Angriffen. Die Täterschaft handelt demzufolge opportunistisch, ohne auf einen spezifischen Sektor abzuzielen. Sobald sie jedoch ein mögliches Opfer identifiziert haben, fokussieren sie ihre Anstrengungen darauf. Im Berichtshalbjahr zeigte sich, dass Ransomware-Akteure die Ausnutzung verschiedener Schwachstellen für ihre Aktivität instrumentalisierten. Dies beinhaltete etablierte sowie neuere Ransomware-Varianten wie Akira, Black Basta, Fog, Helldown aber auch LockBit.[62]

Neben der Ausnutzung von Schwachstellen sind Unternehmen insbesondere im Umfeld ihrer Lieferkette gefährdet. Das Risiko entsteht oft aufgrund von Auswirkungen, denen sich das Unternehmen nach einem Vorfall bei einem externen Partner oder einem Subunternehmen ausgesetzt sieht. Die Lieferkette ist häufig komplex und macht die durchgängige Umsetzung der Cybersicherheitsmassnahmen schwieriger. Beispielsweise gilt die produzierende Industrie[63] aufgrund der Komplexität der Systeme und Installationen, die mit dem Internet verbunden sind, als besonders exponiert.

Per Ende des zweiten Halbjahres 2024 ist festzuhalten, dass es immer mehr Gruppen, aber weniger Ransomware-Familien gibt und die Zahl der Angriffe global zunimmt.[64] Dies zeigt sich auch in der steigenden Anzahl von Datenabflüssen und Websites, die solche Daten anbieten. Hinzu kommt die Tatsache, dass der verstärkte Einsatz von KI neuen Bedrohungsakteuren wie FunkSec einen noch leichteren Zugang zu mehr potenziellen Zielen ermöglicht.

In Europa und in der Schweiz werden die Anstrengungen in der Rechtsetzung intensiviert, um die Vorbereitung auf, die Erkennung von und die Reaktion auf Cybersicherheitsvorfälle zu ver-

---

59 'CyberVolk' hacktivists use ransomware in support of Russian interests (therecord.media)

60 FunkSec – Alleged Top Ransomware Group Powered by AI (checkpoint.com)

61 Dragos Industrial Ransomware Analysis: Q3 2024 (dragos.com)

62 VMware ESXi (CVE-2024-37085) zur Installation beispielsweise der Ransomware Akira, Black Basta und LockBit
Veeam Backup & Replication (CVE-2024-40711) sowie SonicWall SonicOS (CVE-2024-40766) zur Installation von Akira und Fog
Zywall Zyxel (CVE-2024-11667) zur Installation von Helldown, siehe auch Kap. 3.2.1.
Windows Error Reporting Service (CVE-2024-26169) zur Installation von Black Basta

63 Manufacturing Cyber Risk Report 2024 (blackkite.com)

64 2024-rapid7-ransomware-radar-report (rapid7.com)

bessern. Dies beispielsweise im Rahmen des «Cyber Solidarity Act» für das Gesundheitswesen in der Europäischen Union[65], die «Cyber Security and Resilience Bill» im Vereinigten Königreich[66] und die Cybersicherheitsverordnung (CSV) in der Schweiz[67].

Empfehlungen

Jeder Fernzugriff muss ausreichend gesichert sein. Dies beinhaltet eine Zwei-Faktor-Authentifizierung für jeden aus dem Internet erreichbaren Dienst. Wenn dies nicht möglich ist, sollte der Zugang auf bestimmte IP-Adressen und Ports beschränkt und eine passende Überwachung eingerichtet werden.

Die Protokolle des Fernzugriffs müssen auf atypische Zugriffsmuster überwacht werden, insbesondere auf Zugriffe aus Regionen, in denen z. B. Unternehmen keine Mitarbeitenden haben. Auch IP-Bereiche, die grossen Hosting-Anbietern zugewiesen sind, von bekannten VPN-Endpunkten verbinden oder aus dem TOR-Netzwerk stammen, sind wenn möglich im Zugriff einzuschränken.

Ausserdem ist es wichtig, ein regelmässiges Patch-Management einzurichten, um Schwachstellen zeitgerecht zu beheben und mit Schwachstellen-Scans zu verifizieren. Updates, welche kritische Sicherheitslücken in über das Internet erreichbare Systemen beheben, sollten innerhalb von 24 Stunden eingespielt werden können. Software oder Systeme, welche vom Hersteller nicht mehr unterstützt werden («End of Life», EOL) sollten abgeschaltet oder – wenn möglich – in eine separate, abgeschottete Netzwerkzone verlegt werden.

3.3 Schadsoftware bei Mobilgeräten

Im November 2024 erhielten das BACS, das Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz) und das Bundesamt für Bevölkerungsschutz (BABS) Meldungen zu verdächtigen physischen Briefen, die angeblich vom Bundesamt für Meteorologie und Klimatologie stammten. Diese Briefe waren gefälscht und stammten von Betrügern, die versuchten, Schadsoftware auf Mobiltelefone zu laden.
Im Brief wurden die Empfängerinnen und Empfänger aufgefordert, eine neue «Unwetter-Warn-App» zu installieren. Eine solche Applikation des Bundes mit dem erwähnten Namen existiert aber nicht. Vielmehr führt der im Brief abgebildete QR-Code zum Download einer Schadsoftware namens «Coper» (auch bekannt als «Octo2»). Bei Installation der vermeintlichen Unwetter-Warn-App versucht die Schadsoftware, sensitive Daten wie beispielsweise Zugangsdaten von 383 Smartphone-Apps (z. B. E-Banking-Apps) zu stehlen.
Die Malware infiziert nur Smartphones, welche über das Android-Betriebssystem verfügen. Sobald die Malware heruntergeladen worden ist, wird sie bei betroffenen Telefonen als «AlertSwiss»-App mit einem abgewandelten Logo dargestellt, bei dem die Schreibweise («AlertSwiss» statt «Alertswiss») und das Logo von der echten App abweichen. Anstatt eines

---

65 The EU Cyber Solidarity Act (ec.europa.eu)
66 Cyber Security and Resilience Bill (gov.uk)
67 Bundesrat eröffnet Vernehmlassung zur Cybersicherheitsverordnung (news.admin.ch)[68] Vorsicht: Gefälschte Briefe im Namen von MeteoSchweiz – Statt «Unwetter-Warn-App» lädt es eine Schadsoftware (ncsc.admin.ch)

runden Logos, wie bei der originalen Applikation, hat die falsche ein rechteckiges Logo in einem weissen Kreis. Die echte Alertswiss-App des BABS ist eine App zur Information, Warnung und Alarmierung der Bevölkerung, die von verschiedenen Stellen des Bundes und der Kantone genutzt wird.[68]

Empfehlung

Auf der Website des BACS finden Sie eine Auflistung von neun praktischen Tipps, die die Nutzung des Mobiltelefons sicherer machen (ncsc.admin.ch).

4 Schwachstellen

Die «Time-To-Exploit» (TTE) ist eine kritische Kennzahl im Bereich des Schwachstellenmanagements. Sie misst die Zeitspanne, die zwischen der Veröffentlichung oder Entdeckung einer Schwachstelle und ihrer aktiven Ausnutzung (Exploit) durch Angreifer liegt. Die Metrik gibt Aufschluss darüber, wie rasch Organisationen auf Schwachstellen reagieren müssen, um potenzielle Angriffe zu verhindern.
Verschiedene Faktoren beeinflussen die TTE. Auf technischer Ebene sind Aspekte wie die Verfügbarkeit von Exploit-Details und Exploit-Kits entscheidend. Mit der Veröffentlichung von Details zu einer Schwachstelle, wie ein Proof of Concept oder Exploit-Code, reduziert sich die TTE. Aber auch die Komplexität einer Schwachstelle ist relevant. Da Schwachstellen, die leicht verständlich und ausnutzbar sind, die TTE zum Teil drastisch reduzieren, dauert es bei komplexen Sicherheitslücken länger, bis eine Ausnutzung erfolgt. Letztere erfordern vom Angreifer mehr Kompetenzen und Vorbereitung.
Während früher zudem weniger systematisch nach Sicherheitslücken gesucht worden ist, nutzen Angreifer heute KI und maschinelles Lernen (ML), um verwundbare Systeme zu identifizieren und in der Folge Exploits rasch zu entwickeln. Ausserdem tragen auch die Aktivitäten der potenziellen Angreifer im Darkweb dazu bei, dass Schwachstellen nun rascher ausgenutzt werden. Exploits werden schneller in Foren und auf digitalen Marktplätzen gehandelt.

Empirisch betrachtet, hat sich die TTE über die Jahre nachweislich und kontinuierlich verkürzt. Mandiant, ein US-amerikanisches IT-Sicherheitsunternehmen, begann 2018 mit der Analyse von Schwachstellen in Bezug auf diese Kennzahl. Die Ergebnisse der Untersuchungen sind alarmierend. Während 2018/2019 im Schnitt noch eine TTE von 63 Tagen beobachtet worden war, verkürzte sich die Zeitspanne für die Jahre 2020/2021 bereits auf 44 Tage. In den beiden darauffolgenden Jahren 2021/2022 lag die durchschnittliche TTE erneut 12 Tage tiefer bei 32 Tagen. Im Jahr 2023 musste nach durchschnittlich nur fünf Tagen mit einer potenziellen Ausnutzung einer entdeckten oder veröffentlichten Schwachstelle gerechnet werden.[69]
Diese Veränderung ist das Ergebnis technologischer, organisatorischer und krimineller Entwicklungen, die es Angreifern schliesslich ermöglichte, Schwachstellen schneller zu identifizieren und auszunutzen. Die kürzere TTE hat zur Folge, dass Unternehmen immer weniger

[68] Vorsicht: Gefälschte Briefe im Namen von MeteoSchweiz – Statt «Unwetter-Warn-App» lädt es eine Schadsoftware (ncsc.admin.ch)
[69] How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends (cloud.google.com)

Zeit zur Verfügung steht, um Schwachstellen zu patchen oder andere notwendige Sicherheitsmassnahmen zu ergreifen. Der Druck auf die Betreiberinnen und Betreiber von IT-Infrastrukturen, rasch zu handeln, steigt mit sinkender TTE signifikant. Insbesondere bei kritischen Schwachstellen vergeht oft nur wenig Zeit, bis erste Angriffe beobachtet werden.

Im Kontext dieser Herausforderung hat das BACS Betreiberinnen kritischer Infrastrukturen in der zweiten Jahreshälfte 2024 wiederum vor verschiedenen Schwachstellen gewarnt. Die Warnungen betrafen sogenannte Zero-Day-, wie auch N-Day-Schwachstellen. Eine Zero-Day Schwachstelle ist der breiten Öffentlichkeit wie auch dem Hersteller noch weitestgehend unbekannt. Ein Patch zur Installation steht deshalb noch nicht zur Verfügung, während die Sicherheitslücke aber bereits aktiv ausgenutzt wird. Diese Konstellation stellt für Organisationen eine hohe Gefahr dar. Das BACS hat unter anderem für CVE-2024-47575 (in FortiManager) sowie CVE-2024-0012 (in Palo Alto Networks PAN-OS) entsprechende Warnungen publiziert. Beides betraf Zero-Day-Schwachstellen in Produkten, die in der Schweiz eine breite Nutzerbasis aufweisen. In beiden Fällen blieb den Unternehmen faktisch keine Zeit für die Behebung der Schwachstellen.

Im Gegensatz dazu steht die N-Day-Schwachstelle. Hier steht den Nutzern zum Zeitpunkt der Veröffentlichung der Schwachstelle bereits eine Software-Korrektur (Patch/Fix) zur Verfügung, da der Hersteller zu einem früheren Zeitpunkt bereits involviert worden war und dementsprechend eine gewisse Vorbereitungszeit für Gegenmassnahmen hatte. In dieser Schwachstellen-Kategorie hat das BACS beispielsweise aktiv auf CVE-2024-40766 (in SonicWall SonicOS) hingewiesen. Die Sicherheitslücke betrifft breit genutzte Dienstleistungen eines Anbieters im Bereich der Netzwerksicherheit. Zwischen Publikation der Sicherheitslücke durch den Hersteller (21. August 2024) und der erstmaligen Beobachtung einer potenziellen Ausnutzung (6. September 2024) vergingen im konkreten Fall lediglich 16 Tage.

Empfehlungen

Die erheblich verkürzte Time-To-Exploit (TTE) stellt Organisationen und Unternehmen vor neue Herausforderungen. Angreifer werden stets effizienter darin, Schwachstellen rasch zu identifizieren und auszunutzen. Daher ist eine Kombination aus zügigem Ausrollen von Updates, proaktiver Sicherheitsarbeit und Automatisierung entscheidend, um sich wirkungsvoll dagegen zu schützen. Zahlreiche Organisationen bekunden Mühe damit, die Geschwindigkeit der Patch-Verteilung an die stetig kürzer werdende TTE-Zeitspanne anzupassen.

Tragen Sie der jüngsten Entwicklung der TTE unbedingt Rechnung und adaptieren Sie die Patch-Management-Prozesse in Ihrem Unternehmen an die stetig kürzeren Exploit-Zeitspannen. Optimieren und beschleunigen Sie Ihre Patch-Zyklen, insbesondere für kritische Schwachstellen. Priorisieren Sie die Behebung von Schwachstellen in exponierten Teilen Ihrer Infrastruktur. Führen Sie regelmässig Penetrationstests und Schwachstellen-Scans durch, um allfällige Sicherheitslücken proaktiv zu identifizieren. Nutzen sie ein Monitoring und verfügbare Bedrohungsinformationen (Threat Intelligence). Die Echtzeitüberwachung Ihrer Infrastruktur gepaart mit den Möglichkeiten der Automatisierung hilft Ihnen bei der zeitnahen Erkennung von Sicherheitslücken. Stellen Sie sicher, dass Ihr Unternehmen über ein aktuelles Inventar der Infrastruktur und der eingesetzten Produkte verfügt.

Auch flankierende Massnahmen wie der Einsatz von Red-Teaming, regelmässige Sicherheitsprüfungen oder der Betrieb eines Bug-Bounty-Programms in Ihrem Unternehmen können helfen, die Effektivität der Reaktionszeiten in Bezug auf die Bewältigung von Schwachstellen zu bewerten.

5 Betrug und Social Engineering

Auch im zweiten Halbjahr 2024 machte das Phänomen «Betrug» den grössten Teil der Meldungen an das BACS aus. Fast zwei Drittel aller eingegangenen Meldungen (18'270) betrafen diese Kategorie. Während die Zahl der Betrugsversuche über das ganze Jahr von 30'496 auf 41'374 stark angestiegen ist, liegt der Meldeeingang allerdings im zweiten Halbjahr um 1'052 unter demjenigen der Vorjahresperiode. Die Schwankungen in dieser Kategorie sind fast ausschliesslich auf das Phänomen der «Drohanrufe von Fake-Behörden» zurückzuführen.[70] Im Frühjahr 2024 verzeichnete das BACS zeitweise Rekordmeldeeingänge. So gingen in den Wochen 12 und 14 zeitweise mehr als 1'600 Meldungen pro Woche allein zu diesem Phänomen beim BACS ein. Diese Meldespitzen blieben in der zweiten Jahreshälfte aus. Nachdem in den Sommermonaten ein Rückgang mit Meldeeingängen im nur noch zweistelligen Bereich beobachtet wurde, stiegen die Zahlen im Herbst erneut an und pendelten sich zwischen 500 und 700 Meldungen pro Woche ein.
Eine Zunahme beobachtete das BACS in der Berichtsperiode bei «betrügerischen Gewinnspielen». Verglichen mit dem zweiten Halbjahr 2023 stiegen die Meldungen von 744 auf 2'398. Auch auf das ganze Jahr betrachtet, hat sich der Meldeeingang von 1'025 auf über 3'509 mehr als verdreifacht. In vielen Fällen werden bei diesem Phänomen die Namen bekannter Lebensmittel- oder Einzelhandelsunternehmen, Elektronikhändler oder Transportunternehmen missbraucht. Um den vermeintlichen Gewinn zu erhalten, wird das Opfer auf eine Webseite weitergeleitet, auf der persönliche Daten wie Kreditkartendaten, Namen, E-Mail-Adresse oder Mobiltelefon-Nummer angegeben werden müssen. Versteckt in den AGBs – ganz klein auf der Webseite dargestellt oder gar ausserhalb des sichtbaren Webseitenbereichs – wird darauf hingewiesen, dass das Opfer nun ein mehrjähriges Abonnement abschliesst. Die Gebühr wird dann unverzüglich der Kreditkarte belastet. Die Vorgehensweise zeichnet sich dadurch aus, dass hier rechtliche Grauzonen ausgenutzt werden (vgl. Kap. 5.4).
Bei den am häufigsten von Unternehmen gemeldeten Betrugsdelikten ist ein starker Anstieg beim Phänomen «CEO-Betrug» zu verzeichnen. Vor allem Organisationen im Umfeld von Gemeinden und Kirchen waren davon betroffen. Die Gründe werden im dritten Unterkapitel beleuchtet (vgl. Kap. 5.3). Bei Meldungen zu «Rechnungsmanipulationsbetrug» ist hingegen eine leichte Abnahme zu verzeichnen. Diese Meldungen sind im gesamten Jahr 2024 um vier auf 114 Meldungen gesunken.

5.1 Online-Anlagebetrug und Rückforderungsbetrug

Auch im Berichtshalbjahr ist «Online-Anlagebetrug» die Betrugskategorie mit dem höchsten gemeldeten finanziellen Schaden. Die Schadenssumme ist pro Fall teilweise sehr hoch und

[70] Siehe auch Bericht:Telefonbetrug im Cyberbereich (ncsc.admin.ch)

kann im sechsstelligen Bereich liegen. Eine Variante ist die Kombination mit einem sogenannten «Romance-Scam». In dieser Variante geben sich die Betrüger zuerst online als liebevollen, potenziellen Partner aus, gewinnen das Vertrauen der Opfer und bauen emotionale Bindungen auf. Der Erstkontakt erfolgt dabei beispielsweise über Partnerbörsen. Sobald das Vertrauen aufgebaut und genügend gefestigt ist, überredet die vermeintliche Freundin respektive der vermeintliche Freund, das Opfer zu angeblich lukrativen Investitionen und behauptet, selbst grosse Gewinne erzielt zu haben. Die Opfer sind auf diese Weise weniger vorsichtig und kritisch gegenüber den vorgeschlagenen Anlageangeboten, da sie von einer als vertrauenswürdig eingeschätzten Person stammen.

Aber selbst nach dem Anlagebetrug und dem finanziellen Gewinn ist das Interesse der Betrüger in vielen Fällen noch nicht erloschen. Denn diese nutzen die Frustration des Opfers, um wiederum zu betrügen. Zu diesem Zweck kontaktieren sie das Opfer nach einer gewissen Zeit erneut, diesmal jedoch nicht als «Investmentunternehmen», sondern als «Finanzmarktaufsichtsbehörde», «Strafverfolgungsbehörde» oder als Opferhilfe, um das verlorene Geld zurückzuholen. In der Verzweiflung klammern sich viele Opfer an diese Hoffnung. Den E-Mails der Betrüger sind in der Regel offiziell aussehende, aber gefälschte Dokumente angefügt, die mit Stempeln, Unterschriften und offiziellen Logos versehen sind. Geht ein Opfer darauf ein, werden Gebühren oder Steuern verlangt, um den Rückerstattungsprozess in Gang zu setzen. Anschliessend werden immer neue Gebühren erfunden, bis das Opfer schliesslich aufgibt und nicht mehr zahlt.[71]

Empfehlungen

Je grösser die versprochene Rendite ist, desto grösser ist in der Regel auch das Risiko. Seien Sie vorsichtig, wenn sich plötzlich angebliche Anwälte, Organisationen, Finanzmarktaufsichtsbehörden oder ähnliche Stellen melden, die versprechen, verlorenes Geld zurückzuholen und dabei wiederum Gebühren im Voraus verlangen. Zahlen Sie nie Gebühren. Wenn Firmen das Geld zurückerhalten hätten, könnten sie die Gebühren direkt vom zurückgeholten Betrag abziehen und Ihnen die Restsumme gebührenfrei überweisen.
Überprüfen Sie bei Anfragen von Finanzdienstleistern, ob diese von der Finanzmarktaufsicht (FINMA) bewilligt sind. Auf der Webseite der FINMA[72] finden Sie Informationen zu bewilligten Finanzdienstleistern in der Schweiz. Ist ein Finanzdienstleister nicht bewilligt, ist besondere Vorsicht geboten. Überprüfen Sie den Finanzdienstleister anhand von Erfahrungsberichten im Internet.

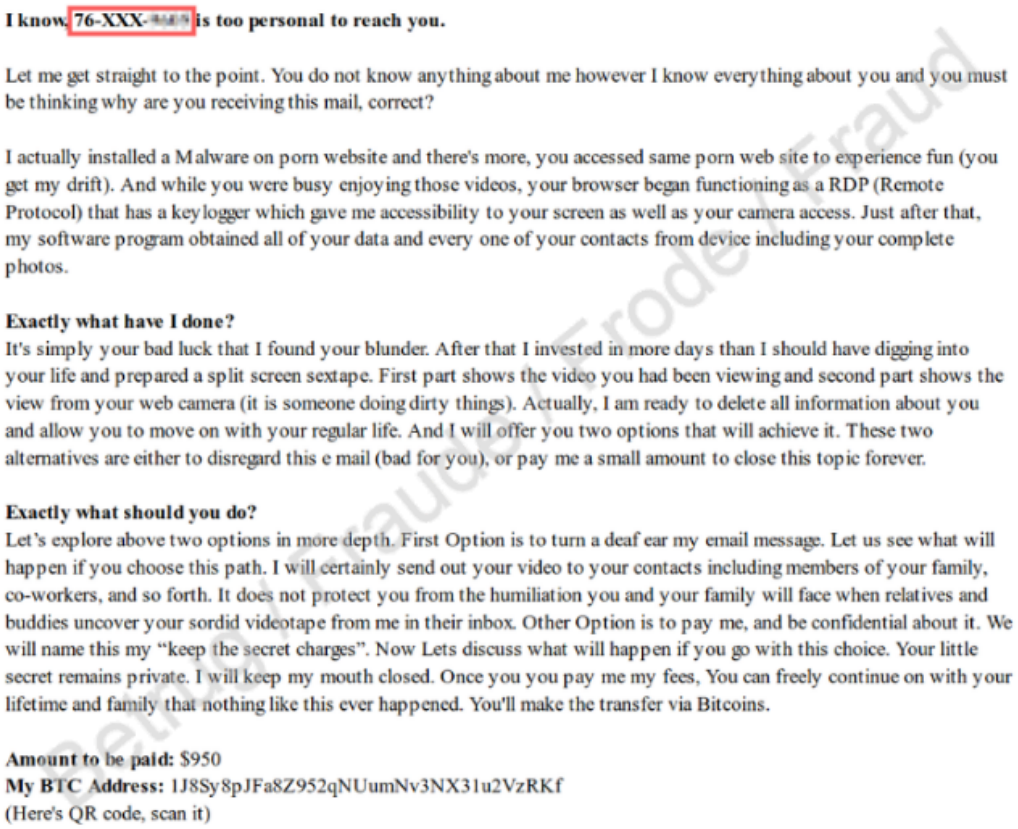
5.2 Variationen von Fake-Sextortion

Bei «Fake-Sextortion» behaupten die Betrüger, dass der Computer oder das E-Mail-Konto des Opfers gehackt worden sei und dass sie Foto- oder Videomaterial gesammelt hätten, welches den E-Mail-Empfänger während eines angeblichen Besuchs auf pornografischen Websites zeigen soll. Die Erpresser versenden solche Schreiben auf gut Glück. Computer und E-Mail-Konten sind in diesen Fällen weder gehackt noch existieren kompromittierende Bilder der

71 Woche 38: Investmentbetrug – Vermeintliche Hilfestellung nach hohem Verlust (ncsc.admin.ch)
72 Bewilligte Unternehmen: FINMA-Bewilligung ist eine Eintrittskarte zum Finanzmarkt (finma.ch)

Empfänger. Um ihre Drohungen glaubwürdig erscheinen zu lassen, verwenden die Angreifer seit Jahren verschiedene Tricks. Sie fälschen die E-Mail-Absenderadressen (Spoofing) so, dass es aussieht, als sei die E-Mail vom eigenen Konto des Opfers versendet worden. In einer weiteren Variante erwähnen die Betrüger in der E-Mail alte Passwörter aus Datenlecks, um ebenfalls vorzugeben, dass das E-Mail-Konto gehackt worden sei. In einigen Fällen nutzen die Täter diese Passwörter, um Konten sozialer Medien zu übernehmen und regelwidrige Inhalte hochzuladen, damit eine Kontosperrung provoziert wird. Das Opfer soll glauben, dass die Täter Zugriff auf kompromittierende Daten haben. Im zweiten Halbjahr gab es in kurzer Abfolge zwei neue Varianten. Dies kann bedeuten, dass die Betrugsmasche nicht mehr allzu lukrativ ist und neue Methoden gefunden werden müssen, um das Geschäftsmodell weiterzuführen.

Bei der ersten Variante wurden Fake-Sextortion-Nachrichten gemeldet, in denen dem Empfänger ein Teil seiner Telefonnummer gezeigt wird (vgl. Abb. 8). Recherchen des BACS zeigten, dass auch diese Daten aus einem Datenleck – in diesen Fällen wahrscheinlich aus dem Datenleck des Kryptowährungs-Dienstleisters «Gemini» – stammen dürften. Alle Empfänger der ans BACS gemeldeten Betrugs-E-Mails waren von diesem Datenleck betroffen.[73]



I know 76-XXX- is too personal to reach you.

Let me get straight to the point. You do not know anything about me however I know everything about you and you must be thinking why are you receiving this mail, correct?

I actually installed a Malware on porn website and there's more, you accessed same porn web site to experience fun (you get my drift). And while you were busy enjoying those videos, your browser began functioning as a RDP (Remote Protocol) that has a keylogger which gave me accessibility to your screen as well as your camera access. Just after that, my software program obtained all of your data and every one of your contacts from device including your complete photos.

Exactly what have I done?
It's simply your bad luck that I found your blunder. After that I invested in more days than I should have digging into your life and prepared a split screen sextape. First part shows the video you had been viewing and second part shows the view from your web camera (it is someone doing dirty things). Actually, I am ready to delete all information about you and allow you to move on with your regular life. And I will offer you two options that will achieve it. These two alternatives are either to disregard this e mail (bad for you), or pay me a small amount to close this topic forever.

Exactly what should you do?
Let's explore above two options in more depth. First Option is to turn a deaf ear my email message. Let us see what will happen if you choose this path. I will certainly send out your video to your contacts including members of your family, co-workers, and so forth. It does not protect you from the humiliation you and your family will face when relatives and buddies uncover your sordid videotape from me in their inbox. Other Option is to pay me, and be confidential about it. We will name this my "keep the secret charges". Now Lets discuss what will happen if you go with this choice. Your little secret remains private. I will keep my mouth closed. Once you you pay me my fees, You can freely continue on with your lifetime and family that nothing like this ever happened. You'll make the transfer via Bitcoins.

Amount to be paid: $950
My BTC Address: 1J8Sy8pJFa8Z952qNUumNv3NX31u2VzRKf
(Here's QR code, scan it)

Abb. 8: Fake-Sextortion-E-Mail mit eingeblendeter Telefonnummer des Empfängers

In der zweiten Variante verwendeten die Betrüger auch Wohnadressen, die sie ebenfalls aus Datenlecks erhalten hatten und so mit der E-Mail-Adresse des Opfers verknüpfen konnten. Nachdem solche Fälle zuerst in den USA beobachtet worden waren, gingen im zweiten Halbjahr 2024 auch beim BACS erste Meldungen aus der Schweiz ein. Im Gegensatz zu den US-

73 Woche 33: Fake-Sextortion und Datenabflüsse (ncsc.admin.ch)

Varianten gingen die Betrüger aber noch einen Schritt weiter und erwähnten in der Erpresser-E-Mail nicht nur die Wohnadresse des Opfers, sondern suchten auf Google Maps nach Bildern der Wohnadresse oder der näheren Umgebung und fügten diese der Erpresser-E-Mail hinzu (vgl. Abb. 9). Damit wollen die Betrüger das Opfer überzeugen, dass sie die volle Kontrolle über den Computer haben und auch das persönliche Umfeld des Opfers kennen. Diese Kombination von digitalen und physischen Informationen verstärkt die Drohkulisse und kann das Opfer dazu verleiten, den Forderungen der Betrüger nachzukommen.[74]

Important: You got one day to sort this out and I will only accept Bitcoin. I have a special pixel in this e mail, and now I've been notified that you have read through this email message. This email and Bitcoin address are custom-made for you, untraceable. If you are unfamiliar with Bitcoin, google it. You can buy it online or through a Bitcoin ATM in your neighborhood. There's no point in replying to this email or negotiating, it's pointless my price is fixed. As soon as you send the complete payment, my system will inform me and I will wipe out all the dirt I got on you. Remember if I notice that you've shared or discussed this mail with someone else, your video will instantly start getting sent to your contacts and I will post a physical tape to all of your neighborhood next week. And don't even think about turning off your phone or resetting it to factory settings. It's pointless. I don't make mistakes.

Looks familiar?

Abb. 9: Fake-Sextortion-E-Mail mit Telefonnummer, Adresse und Bild einer Wohnadresse auf Google Maps

Empfehlungen

Ignorieren Sie Fake-Sextortion-E-Mails und lassen Sie sich nicht einschüchtern. Bisher sind dem BACS keine Fälle bekannt, in denen kompromittierendes Bildmaterial tatsächlich vorhanden gewesen wäre.

5.3 CEO-Betrug bei Gemeinden, Schulen und Kirchen

Im zweiten Halbjahr gab es einen Anstieg an Meldungen zu CEO-Betrug. Während im Jahr 2023 noch 487 Meldungen eingegangen waren, waren es im letzten Jahr bereits 719. Beim klassischen CEO-Betrug wird häufig eine E-Mail des angeblichen CEOs an die Finanzabteilung oder eine E-Mail des vermeintlichen Vereinspräsidenten an den Kassierer geschickt. Durch eine glaubwürdige Geschichte soll die angeschriebene Person dazu bewegt werden,

74 Woche 39: Schon wieder neue Fake-Sextortion-Variante: Nun wissen die Betrüger, wo das Opfer wohnt (ncsc.admin.ch)

eine Zahlung zu tätigen. In vielen Fällen soll auch eine Geschenkkarte gekauft und anschliessend deren Code an die Betrüger übermittelt werden.

Besonders auffällig ist, dass von diesem Phänomen bestimmte Sektoren überdurchschnittlich stark betroffen sind. Eine bemerkenswerte Anzahl an Gemeinden, Schulen und Kirchen haben im zweiten Halbjahr 2024 solche betrügerischen Anfragen erhalten. Eine Erklärung dafür ist, dass bei CEO-Betrug die Betrüger die Informationen meist aus öffentlichen Quellen zusammentragen, um die Hierarchie in Firmen, Organisationen oder Vereinen herauszufinden. Viele Unternehmen stellen ihr gesamtes Team inklusive Funktion und E-Mail-Adresse auf der Webseite öffentlich vor. Allerdings bei weitem nicht so transparent wie Gemeinden, Schulen oder Kirchen. Gerade in diesen Bereichen ist eine einfache Kontaktaufnahme seitens Bevölkerung ein zentrales Anliegen. Deshalb werden Kontaktdaten veröffentlicht, wobei teilweise ganze Mitarbeitendenverzeichnisse im Internet zugänglich sind. Was auf der einen Seite die Nähe zur Bevölkerung fördert, ist auf der anderen Seite ein profitables Geschäft für die Betrüger und wird von ihnen auch intensiv genutzt.[75]

Empfehlungen

Sensibilisieren Sie alle Mitarbeitenden bezüglich CEO-Betrug. Insbesondere diejenigen in den Finanzabteilungen und in Schlüsselpositionen sind über diese möglichen Angriffsweisen zu informieren. Bei Vereinen sind alle Mitglieder mit einer Funktion im Vorstand zu schulen. Etablieren Sie klare Prozesse für die Zahlungsabwicklung und setzen Sie deren Einhaltung durch (z. B. Vier-Augen-Prinzip, Unterschrift kollektiv zu zweien usw.).

5.4 Das Ausnützen rechtlicher Grauzonen

Bei vielen Websites, die dem BACS gemeldet werden, ist der Betrug klar ersichtlich. So sind beispielsweise Phishing-Seiten leicht als solche zu erkennen. Es gibt in den wenigsten Fällen Interpretationsspielraum. Dementsprechend einfach ist es auch, diese Webseiten vom Netz nehmen zu lassen. Anders lässt sich zwar bei vielen anderen eine betrügerische Absicht vermuten, beweisen lässt sich dies aber nur selten. Dementsprechend schwierig oder unmöglich ist es für Behörden, eine solche Website offline zu nehmen. Zudem versuchen Betrüger immer häufiger, bewusst in der rechtlichen Grauzone zu operieren, was z. B. bei Abofallen ausgenutzt wird. Diese Websites werben mit einem Gratisprodukt, erwähnen aber nur im Kleingedruckten, dass das Gratis-Abo ohne Reaktion, nach wenigen Tagen in ein kostenpflichtiges umgewandelt wird. Ist die Frist verstrichen, wird sogleich eine Jahres- oder eine Zwei-Jahresgebühr abgebucht. Solche Abofallen gelten als der Ursprung aller Grauzonenbetrügereien.

Ein anderes, vermehrt gemeldetes Beispiel des zweiten Halbjahrs sind Webshops, die vorsätzlich falsche Ware von minderer Qualität liefern. Bei einer Reklamation muss die Ware auf eigene Kosten an den Verkäufer – häufig mit Sitz in Fernost – zurückgesendet werden. In diesen Fällen übersteigen die Versandkosten den Wert des Artikels um ein Vielfaches, was

[75] Woche 49: Kirchen, Schulen, Vereine und politische Parteien vermehrt Opfer von CEO-Betrug (ncsc.admin.ch)

eine Rücksendung unwirtschaftlich macht. Da aber die Möglichkeit der Rücksendung bestanden hätte, ist es unklar, ob dieses Vorgehen als Betrug klassifiziert werden kann.

Noch dreister wird es bei Websites, auf denen angeblich Strafregisterauszüge bestellt werden können. Nach der Bestellung und Bezahlung der geforderten CHF 20 wird anstelle des Auszugs allerdings nur eine Anleitung geliefert, wie ein solcher gekauft werden kann. Diese Information ist insofern nutzlos, weil eine einfache Suchmaschinenanfrage dasselbe Resultat generiert. Auf der Website findet sich ebenfalls im Kleingedruckten der Hinweis, dass es sich nur um eine Wegleitung für die Bestellung handelt und nicht um die eigentliche Bestellung. Die Betreiber spekulieren darauf, dass die Opfer diese Zeilen überlesen, was eine strafrechtliche Verfolgung der Anbieter schwierig gestaltet. Ein ähnliches Vorgehen nutzen auch verschiedene Websites, die Reisende beim Visumsantrag unterstützen wollen. Sowohl der Aufwand des Anbieters als auch der Aufwand der offiziellen Websites für den Visumsantrag des jeweiligen Staates sind praktisch identisch. Nur ist das Angebot auf den angeblichen Hilfe-Websites überteuert.
Vermeintliche Angebote für einen Eintrag in einem mehr oder weniger bekannten Branchenbuch gehören ebenfalls in diese Kategorie. Diese Angebote werden oft als offizielle Rechnung getarnt per E-Mail oder Brief den Unternehmen zugestellt. Im Kleingedruckten wird jedoch darauf hingewiesen, dass erst mit der Bezahlung der Rechnung der eigentliche Vertrag abgeschlossen wird. Auch hier spekulieren die Rechnungssteller darauf, dass das Unternehmen nicht mehr so genau weiss, ob es sich um eine Offerte oder um einen bereits bestehenden Vertrag handelt, der verlängert werden soll.

Empfehlungen

Lesen Sie Rechnungen, die Sie nicht erwarten, genau durch, auch das Kleingedruckte. Klären Sie im Zweifelsfall ab, ob die Rechnung gerechtfertigt ist. Lesen Sie, bevor Sie sich bei etwas registrieren oder die Kreditkartendaten angeben, die damit verknüpften Bedingungen durch. Besonders bei angeblichen Gratisangeboten ist grosse Vorsicht geboten. Überprüfen Sie den Dienstleister anhand von Erfahrungsberichten im Internet.

6 Angriffe auf die Verfügbarkeit von Websites und -diensten sowie Störung der Infrastruktur

Bei Angriffen auf die Verfügbarkeit von Websites und -diensten – meistens in Form von «Distributed Denial of Service» (DDoS)[76] – versuchen Angreifer, einen aus dem Internet zugänglichen Dienst mithilfe einer grossen Anzahl von Anfragen für die Nutzung temporär unzugänglich zu machen. Solche Angriffe führen weder zum unberechtigten Zugriff auf Daten, zu einem Informationsabfluss noch zur nachhaltigen Beschädigung von Systemen.
Infrastruktur kann aber auch gestört werden, wenn Aktualisierungen oder Änderungen an der Konfiguration den Betrieb beeinträchtigen. Beispielsweise waren durch eine mutmasslich bösartige Manipulation an den Systemen des Login-Tools der Schweizer Medienhäuser OneLog

[76] Angriff auf die Verfügbarkeit (DDoS) (ncsc.admin.ch)

im Herbst 2024 die Anmelde- und Registrierungsdienste nicht mehr verfügbar. Dies beeinträchtigte abhängige Funktionen wie die Bezahlschranke oder die Kommentarfunktion der betroffenen Publikationen[77] (vgl. Kap. 7). Abgesehen von bösartigen Manipulationen können auch Auswirkungen einer fehlerhaften Aktualisierung einer Komponente zu Störungen führen. Eine solche wird im zweiten Teil dieses Kapitels anhand des Sicherheitsdienstleisters CrowdStrike beleuchtet.

6.1 DDoS-Angriffe

Temporäre Ausfälle bei Finanzdienstleistungen[78] und kantonalen Webseiten[79] waren Auswirkungen von DDoS-Angriffen auf Systeme von Schweizer Organisationen im zweiten Halbjahr 2024. Nur leicht zugenommen haben die direkten Meldungen an das BACS zu Angriffen dieser Art von 41 im Jahr 2023 auf 48 im Jahr 2024. Dabei ist die Zunahme vor allem auf das zweite Halbjahr zurückzuführen. Hier stieg die Zahl von 17 auf 25.

DDoS-Angriffe werden häufig durch Angriffsinfrastruktur ermöglicht, welche Cyberkriminelle bei entsprechender Bezahlung auf die Ziele ihrer Wahl richten können. Im September 2024 verzeichnete das BACS vermehrt DDoS-Angriffe, welche von einem Botnetz namens «Gorilla» ausgeführt wurden. Dabei handelt es sich um einen auf Telegram angebotenen «DDoS-as-a-service»-Dienst, welcher für entsprechendes Entgelt gemietet werden kann. Da eine Betreiberin einer kritischen Infrastruktur in der Schweiz betroffen war, hat das BACS die technischen Erkenntnisse in einem Bericht[80] veröffentlicht. Bei jenen DDoS-Angriffen gegen Schweizer Infrastrukturen handelte es sich um DNS-Amplifikations-Angriffe. Bei diesen werden unter Missbrauch des «Domain Name Systems» (DNS) ausserordentlich grosse Datenströme auf die Infrastruktur des Opfers gelenkt, um diese zu überlasten.

Am Abstimmungssonntag des 24. November 2024 war die Website des Kantons Schwyz Ziel eines DDoS-Angriffs.[81] Der Angriff dauerte über längere Zeit an und führte dazu, dass auch Websites von diversen Gemeinden verschiedener Kantone sowie verschiedene kantonale Websites für einige Stunden nicht verfügbar waren.[82] Alle betroffenen Websites wurden vom selben Anbieter betrieben und so kollateral in Mitleidenschaft gezogen. Über die Motivation des Angriffs wurde nichts bekannt. Auch konnte kein direkter Zusammenhang mit dem Abstimmungssonntag hergestellt werden.

Die Schweiz war nicht übermässig von DDoS-Angriffen betroffen, wenn man die Beobachtungen hierzulande mit den internationalen Vorkommnissen vergleicht.[83] Neben den stetig andauernden Angriffen von Hacktivisten im Umfeld von internationalen Konflikten können auch Einzelereignisse DDoS-Kampagnen provozieren. So löste die Verhaftung des Gründers und

---

77 OneLog Update: Login-Service wieder verfügbar (onelog.ch)

78 DDoS-Angriff trifft Swisscom und legte Twint lahm (inside-it.ch)

79 Informatique: l'Etat de Vaud victime d'attaques «très virulentes» (24heures.ch), Revue des cybermenaces : Septembre 2024 (vd.ch)

80 Siehe Technische Kurzanalyse zum Botnetz «Gorilla» (ncsc.admin.ch)

81 DDoS-Angriff auf Webseite des Kanton Schwyz führt zu Ausfällen verschiedener Webseiten von Kantonen und Gemeinden (ncsc.admin.ch)

82 Cyber-Angriff: Websiten von Gemeinden nicht mehr erreichbar (luzernerzeitung.ch)

83 Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4 (cloudflare.com)

CEOs der Messaging-Applikation Telegram, Pavel Durov, in Frankreich eine teilweise koordinierte Reaktion mehrerer Hacktivisten-Kollektive unter dem Hashtag #FreeDurov aus. Über 50 französische Organisation wurden in dieser Kampagne Ziele von DDoS-Angriffen.[84]
Teilweise gelingt es der Strafverfolgung, Angreifer zu identifizieren und festzunehmen oder die Angriffsinfrastruktur unschädlich zu machen. So verhaftete die spanische Polizei Personen, die sich am «DDoSia»-Botnet der pro-russischen Gruppe «NoName057(16)»[85] beteiligt und Geräte für Angriffe zur Verfügung gestellt hatten.[86] Weiter konnte die US-amerikanische Justiz zwei zentrale Mitglieder der Hacktivisten-Gruppe «Anonymous Sudan» anklagen und deren Angriffsinfrastruktur zu grossen Teilen beschlagnahmen.[87] Derweil nahm die deutsche Strafverfolgung im Rahmen der Operation «PowerOff» 27 Stresser-Dienste vom Netz. Stresser-Dienste sind DDoS-Angebote, welche sich von Drittparteien für Angriffe auf beliebige Ziele mieten lassen. Dabei wurden auch über 300 Nutzer dieser Angebote identifiziert, von denen bereits einzelne Personen festgenommen werden konnten.[88]

Trotz dieser Erfolge der internationalen Strafverfolgung bleiben DDoS-Angriffe ein beliebtes Mittel verschiedenster Akteure, um kurzfristig die Verfügbarkeit von Zielen einzuschränken und dadurch unter anderem Aufmerksamkeit zu erzielen. Die Medien können durch eine zurückhaltende Berichterstattung diesem Ziel entgegenwirken. Die laufend weiter ausgebauten Angriffsinfrastrukturen wie Botnetze und deren weiterentwickelten Methoden fordern Netzwerkbetreiber, ihre Abwehrmassnahmen ständig aktuell zu halten.

Empfehlungen

Die Website des BACS bietet unter der Rubrik Angriff auf die Verfügbarkeit (DDoS-Angriff) (ncsc.admin.ch) verschiedene Informationen und Massnahmen zur Prävention und Abwehr solcher Angriffe an. Bereiten Sie sich in Kooperation mit Ihrem Dienstleister oder Hoster auf einen potenziellen Angriff vor, um die Auswirkungen abzumildern. Für kritische Systeme kann es sinnvoll sein, einen kommerziellen DDoS-Schutz zur Unterstützung hinzuzuziehen.

Bei DDoS-Angriffen im Zusammenhang mit Erpressung empfiehlt das BACS, nicht auf die Forderungen einzugehen. Die Betrüger können nach einer ersten Zahlung mehr Geld verlangen und die Angriffe danach trotzdem fortführen. Stattdessen sollten Sie den Fall dem BACS melden und mit der Polizei in Kontakt treten, um eine Strafanzeige zu erstatten. Im Falle eines Angriffs finden Sie Empfehlungen auf DDoS-Angriff - Was nun? (ncsc.admin.ch).

6.2 Vorfall CrowdStrike

Am 19. Juli 2024 kam es zu einer weltweiten Störung von Windows-Systemen, die als bisher weitreichendster IT-Ausfall der Geschichte bezeichnet wird. Diese Störung war nicht auf einen Cyberangriff zurückzuführen, sondern wurde durch eine fehlerhafte Aktualisierung des CrowdStrike-Falcon-Schutzmoduls ausgelöst, das der Erkennung und Abwehr ebensolcher

84 Hacktivists Call for Release of Telegram Founder with #FreeDurov DDoS Campaign (blog.checkpoint.com)
85 Detaillierter Analysebericht zu den DDoS-Angriffen «NoName057(16)» (ncsc.admin.ch)
86 Tres detenidos por delitos de daños informáticos con fines terroristas (interior.gob.es)
87 Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks (justice.gov)
88 Operation „Power OFF“: weltweiter Schlag gegen Cybercrime-Infrastruktur (bka.de)

Cyberangriffe dient. Durch die erwähnte Aktualisierung kam es bei einer Vielzahl von Windows-Computern zum sogenannten «Blue Screen of Death», welcher mit einem Absturz des Geräts sowie dessen Funktionsunfähigkeit einher geht.[89] CrowdStrike gelang es, den Fehler innerhalb weniger Stunden zu identifizieren und die Verteilung des fehlerhaften Updates umgehend zu unterbinden. In der Folge veröffentlichten CrowdStrike und Microsoft Anweisungen zur Behebung des Problems.[90] Die Behebung erforderte den Start jedes betroffenen Systems im abgesicherten Modus und die manuelle Entfernung einer spezifischen Datei. Da der Start im abgesicherten Modus in der Regel nicht für normale Benutzer verfügbar ist und die erforderlichen Bitlocker-Schlüssel sich zum Teil auf anderen vom Vorfall betroffenen Systemen befanden, kam es in bestimmten Organisationen zu erheblichen Verzögerungen bei der Behebung des Problems. Schätzungen zufolge waren weltweit über 8,5 Millionen Systeme von dem Vorfall betroffen, wobei die Gesamtschadenssumme auf mehrere Milliarden US-Dollar geschätzt wird.[91]

Die Auswirkungen manifestierten sich zunächst in Australien, anschliessend in Indien, Europa und den USA, abhängig davon, zu welchem Zeitpunkt der Arbeitstag nach dem fehlerhaften Update begann. Unter den betroffenen Organisationen befanden sich zahlreiche Grossunternehmen, Regierungsbehörden und öffentliche Einrichtungen, wobei die Konsequenzen insbesondere in der Luftfahrt deutlich spürbar waren. Dieser Umstand ist auch auf die hohe Komplexität des Flugverkehrs sowie die eng getakteten Flugpläne zurückzuführen. Der Vorfall ereignete sich zudem an einem Freitag im Juli, einem Zeitraum mit besonders hohem Flugaufkommen in Europa. In der Folge kam es zu vielen Verzögerungen oder Streichungen von Flügen an zahlreichen Flughäfen. Besonders betroffen waren zentrale internationale Flughäfen wie Heathrow in London sowie Fluggesellschaften wie Delta Airlines, welche Tausende von Flügen verschieben oder absagen mussten. Auch in der Schweiz kam es am Flughafen Zürich zu Verzögerungen und Stornierungen.[92]

Der Sicherheitsvorfall wurde zeitnah von Kriminellen instrumentalisiert, um betrügerische Aktivitäten zu initiieren. Zu den von den Kriminellen genutzten Angriffsmethoden zählten Phishing-E-Mails, die Supportangebote von CrowdStrike vortäuschten, sowie bösartige Skripte, die eine automatisierte Wiederherstellung der betroffenen Systeme in Aussicht stellten. CrowdStrike reagierte auf diese Vorfälle mit öffentlichen Berichterstattungen und Stellungnahmen und empfahl insbesondere den Nutzern, ausschliesslich Updates von offiziellen Quellen herunterzuladen.[93] Darüber hinaus gaben sich opportunistische Betrüger als Kundendienstmitarbeiter von Fluggesellschaften aus. Zudem durchsuchten Betrüger die soziale Medien nach Beiträgen verärgerter Reisender, deren Flüge verspätet waren oder gestrichen wurden. Im weiteren Verlauf kontaktierten die Kriminellen die Betroffenen über gefälschte Konten und baten sie um die Herausgabe sensitiver Informationen wie etwa ihrer Personaldaten, ihrer Buchungsbestätigungsnummer oder ihrer Kreditkartendaten.[94]

---

89 CrowdStrike oopsie crashes Windows workstations across the world (therecord.media)

90 KB5042421: CrowdStrike issue impacting Windows endpoints (microsoft.com), Falcon Content Update Remediation and Guidance Hub (crowdstrike.com)

91 What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk (hbr.org)

92 CrowdStrike-Softwarefehler - Der Tag, an dem die IT weltweit verrückt spielte (srf.ch)

93 Falcon Sensor Issue Likely Used to Target CrowdStrike Customers (crowdstrike.com)

94 Scammers impersonate airline customer service representatives (ftc.gov)

Als Konsequenz des zuvor geschilderten IT-Ausfalls hat CrowdStrike eine Überprüfung und Optimierung der internen Testprozesse für Software-Aktualisierungen vorgenommen und eine Funktion hinzugefügt, mit der Kunden wählen können, ob sie Inhaltsaktualisierungen sofort oder verzögert erhalten möchten. Das Ziel besteht darin, das Risiko zukünftiger Vorfälle dieser Art zu minimieren. Eine Besonderheit von Windows-Systemen, die einen solchen Ausfall ermöglichte, sind die erweiterten Zugangsrechte, welche die Software von Sicherheitsanbietern wie CrowdStrike auf Kernel-Ebene benötigen. Microsoft hat hierzu Stellung genommen und betont, dass der Zugriff von Sicherheitslösungen auf Kernel-Ebene zwar notwendig sei, aber besseren Richtlinien unterliegen müsse und Innovationen diesen Zugriff in der Zukunft einschränken sollten. Zudem kündigte Microsoft an, die Zusammenarbeit mit Partnern wie CrowdStrike zu intensivieren, um solche Risiken künftig einzuschränken.[95]

Empfehlungen

Ein effektives Patch-Management ist für die Aufrechterhaltung von Sicherheit und Stabilität von entscheidender Bedeutung. Organisationen müssen abwägen zwischen einer sofortigen Installation, die Schwachstellen schnell behebt, aber das Risiko ungetesteter Störungen mit sich bringt, und einer verzögerten Installation, die zwar gründliche Tests ermöglicht, die Systeme aber länger ungeschützt lässt. Eine gestaffelte Aktualisierung basierend auf der Exponiertheit und Kritikalität der Systeme kann eine geeignete Strategie zur Risikominimierung darstellen.

Die Schulung und das Training der Mitarbeitenden in Bezug auf IT-Ausfälle sind essenziell, um im Ernstfall eine schnelle und effektive Reaktion zu gewährleisten.

7 Datenmanagement, -abflüsse und -erpressung

Datenlecks und ungewollte Datenexpositionen waren auch in der zweiten Jahreshälfte des Jahres 2024 sowohl in der Schweiz als auch international ein Thema. Eine sichere und intakte Datenhaltung kann aber nur erreicht werden, wenn Zugriffsschutz und Datenmanagement bei Behörden, Unternehmen und Privaten Priorität erhalten. Dieser Umstand zeigte sich eindrücklich beim Cybervorfall der Schweizer «Single-Sign-On»-Plattform OneLog Ende Oktober 2024. Ein Abfluss der Nutzerdaten bei der Medienplattform konnte nach einer forensischen Untersuchen zwar ausgeschlossen werden,[96] trotzdem mussten verschiedene Medien ihre Inhalte während zehn Tagen ohne Bezahlschranke anbieten.[97] Dies war notwendig, denn der Bedrohungsakteur löschte die Daten der Nutzerinnen und Nutzer für die Authentifizierung bei OneLog, womit die zahlenden Kunden nicht mehr identifiziert werden konnten.[98] Andere Cy-

[95] CrowdStrike tells Congress of two process changes to address July outage incident (therecord.media), Windows Security best practices for integrating and managing security tools (microsoft.com)

[96] Siehe Pressemitteilung OneLog informiert über weitere Erkenntnisse nach Sicherheitsvorfall: Keine Hinweise auf Datendiebstahl, Untersuchungen dauern an (ringier.com)

[97] Ein Super-GAU für die Schweizer Medienwelt (republik.ch)

[98] OneLog informiert über weitere Erkenntnisse nach Sicherheitsvorfall: Keine Hinweise auf Datendiebstahl, Untersuchungen dauern an (ringier.com)

bervorfälle verdeutlichten ebenfalls den Wert von Daten, insbesondere dann, wenn die Integrität oder die Verfügbarkeit der Daten in Zweifel gezogen wird. Beim Cybervorfall bei der Praxisgruppe VidyMed im Dezember 2024 war die Verfügbarkeit der Daten nicht mehr gegeben, weshalb die vier Praxisstandorte für die Weiterführung der medizinischen Versorgung temporär auf Stift und Papier wechseln mussten.[99] Ähnlich erging es zahlreichen Schulen in Europa, Nordamerika und Singapur, die eine digitale Plattform zur Verwaltung des Schulunterrichts nutzten. Nachdem sich ein unautorisierter Nutzer Anfang August Zugriff auf die Plattform verschafft hatte, löschte dieser bei mindestens 13'000 Geräten von Schülerinnen und Schülern die Daten.[100] Nur wenige Monate später erlebte ein anderer, globaler Anbieter von Unterricht-Software einen vergleichbaren Cybervorfall: Der Bedrohungsakteur gab in einer Erpressernachricht an, die Daten von rund 62 Millionen Schulkindern und 10 Millionen Lehrpersonen abgegriffen zu haben.[101] Hier führte der Vorfall zwar zu keiner Datenlöschung auf den Geräten der Schulkinder und Lehrpersonen oder zu einer Verschlüsselung der Systeme, jedoch kann das immense Volumen der abgeflossenen Daten als Grundlage für künftige Straftaten im digitalen aber auch im physischen Raum dienen. Denn auch bei diesem Fall konnten sensitive Personendaten exfiltriert werden.[102]

Eine sichere Datenhaltung ist besonders bezüglich Datenabflüssen relevant, bei denen die abgeflossenen Daten ein nachgelagertes Risiko für weitere Organisationen und Privatpersonen bedeuten. Während Unternehmen nach einem Datenabfluss bei einem Zulieferer gegebenenfalls ihre Zugänge zur eigenen IT-Infrastruktur überwachen müssen, steigt auch das Risiko, Opfer eines Betrugsversuch zu werden (vgl. Kap. 5). Ähnlich können bei Privatpersonen sensitive Informationen für Kontoübernahmen, Phishing (vgl. Kap. 2), Identitätsdiebstahl oder Finanzbetrug missbraucht werden. Dabei spielen besonders Bedrohungsakteure im Ransomware-Umfeld eine bedeutende Rolle, da sie beim Ausbleiben der Lösegeldzahlung die Daten in der Regel veröffentlichen und/oder z. B. durch deren Verkauf monetarisieren (vgl. Kap. 3.2). Nebst den Aktivitäten von Bedrohungsakteuren begründen auch andere Ursachen wie ein unzureichendes Datenmanagement in der eigenen Infrastruktur, vorhandene Schwachstellen oder technische Fehlkonfigurationen eine Datenexposition. Dies kann dann in einem zweiten Schritt wiederum durch Bedrohungsakteure ausgenutzt werden.

Dedizierte Marktplätze im Internet und im Darkweb – wie beispielsweise «BreachForums» – offerieren Cyberkriminellen die Möglichkeit, gestohlene Daten zu verkaufen und damit Profit zu erwirtschaften.[103] Die Firma Temenos, eine Schweizer Anbieterin von Banken-Software, wurde im November 2024 Opfer eines solchen Vorfalls.[104] Der Hacker behauptete, die Daten würden nebst Angaben über Mitarbeitende auch Details zu Applikationen und Webdiensten für Banken und weitere Kunden enthalten. Um den Behauptungen zusätzliche Glaubwürdigkeit zu verschaffen, fügte der Hacker Screenshots hinzu. Teilweise bieten Hacker auch an, dass die bestohlenen Organisationen sich die Daten wieder zurückkaufen könnten, um die

---

99 Groupe Vidymed: actualites (vidymed.ch); vgl. Pressemitteilungen vom 7. Dezember 2024, 20. Dezember 2024 und 14. Januar 2025.

100 Mobile Guardian: Security Incident Report (mobileguardian.com), Hacker wipes 13,000 devices after breaching classroom management platform (bleepingcomputer.com)

101 PowerSchool starts notifying victims of massive data breach (bleepingcomputer.com)

102 Powerschool hat offenbar Daten von 62 Millionen Schülern verloren (inside-it.ch)

103 Siehe auch Halbjahresbericht 2024/1; Kap. 7.2.

104 Hacker verkaufen Daten von Temenos Quantum Fabric (inside-it.ch)

Publikation oder den Weiterverkauf zu verhindern. Problematisch daran ist, dass sich Opfer bei einem solchen Angebot nie sicher sein können, inwiefern die Cyberkriminellen ihr Wort halten werden.

Hacktivisten nutzen sensitive Daten von Zielen, um ihre sozialen, politischen oder ideologischen Interessen zu verbreiten. Ein von diesen Gruppierungen beliebtes Vorgehen ist das Hacken von IT-Systemen, um anschliessend die erbeuteten Personendaten und Informationen zu veröffentlichen. Diese Vorgehensweise ist auch bekannt als «Hack-and-Leak». So publizierte beispielsweise eine pro-palästinensische Hacktivistengruppe während den Olympischen Sommerspielen in Frankreich persönliche Informationen von israelischen Athleten auf sozialen Medien. Neben Namen, Telefonnummern, Adressen, Passwörtern oder Fotografien wurden auch medizinische Informationen wie z. B. die Blutgruppe veröffentlicht.[105] Problematisch werden solche Informationen für Personen und Unternehmen dabei besonders, wenn sie als strukturierte Daten für Bedrohungsakteure einfach zugänglich werden. Dadurch wird das Risiko erhöht, dass diese Informationen systematisch für Betrug oder andere unlautere Aktivitäten ausgenützt werden. Mitte November veröffentlichte der Nutzer «Nam3L3ss» auf der Darkweb-Plattform BreachForums verschiedene Datensätze von 25 Konzernen. Unter den Opfern befanden sich auch zwei Schweizer Unternehmen.[106] Nach einem Monat weiterer Aktivitäten stieg die Zahl bereits auf rund 100 Datensätze an, die vom selben Nutzer veröffentlicht worden waren.[107] Anders als andere Plattformnutzer behauptete dieser, dass er die Daten nicht durch Hacking, sondern rein durch von den Unternehmen ungewollte Datenexposition gesammelt und bereinigt habe. Dies war beispielsweise gegeben, wenn Daten bei einer Übertragung unverschlüsselt gesendet oder online Datenspeicher ohne Passwörter geschützt wurden. Auch Daten, die Ransomware-Gruppen zur Erpressung nutzten, sind Teil dieser Datensätze. Zwar bezweckte Nam3L3ss nach eigenen Angaben nicht den Verkauf der Daten, aber er wollte mit der Verteilung der bereinigten Datensets seine politischen Vorstellungen nach mehr Verantwortung in der Datenhaltung unterstreichen. In der Schweiz verstösst ein solches Vorgehen gegen das Datenschutzgesetz, weil ein privater Akteur wie Nam3L3ss das Sammeln, Bearbeiten und Veröffentlichen von Personendaten nur mit der Einwilligung der Betroffenen ausführen darf.[108] Dies umfasst insbesondere Personendaten, die als besonders schützenswert gelten.

Empfehlungen

Die verschiedenen Vorfälle im zweiten Halbjahr des Jahres 2024 verdeutlichen, dass die Sicherung sensitiver Daten Priorität haben muss: Wenn Inhalte einmal im Internet veröffentlicht worden sind, ist eine endgültige Löschung kaum mehr durchführbar. Daher gilt im Allgemeinen:

Legen Sie gemäss den 5Ws der Datenhaltung fest, wer welche Daten, in welcher Form, wo abspeichert und bearbeitet und mit wem diese geteilt werden. Nebst einer konservativen Speicherung sollten Sie Daten in regelmässigen Abständen überprüfen und nicht mehr benötigte

105 Israeli athletes doxed at Olympic Games by Zeus hacking group (bitdefender.com)
106 Amazon, UBS und Firmenich von Breach betroffen (inside-it.ch)
107 Conversation with a “Nam3L3ss” Watchdog: Preface (databreaches.net)
108 Siehe auch Art. 31 DSG (Datenschutzgesetz)

Daten löschen. Archivieren Sie aufbewahrungswürdige aber nicht mehr aktiv genutzte Daten offline. Etablieren Sie klare, umsetzbare Prozesse für Datenbearbeitung und Datenschutz und kontrollieren Sie die Implementation. Schützen Sie ferner Zugänge zu Systemen, Konten und Daten mit starken Passwörtern und wo immer möglich mit einer Multi-Faktor-Authentifizierung (MFA).[109] Gewähren Sie den Zugriff nur Personen, die diesen auch wirklich benötigen.

Daten aus älteren Datenabflüssen können für spätere Angriffe wiederverwendet werden. Überprüfen Sie periodisch, ob Ihre Zugangsdaten in einem Datenleck auftauchen, etwa auf der Website Have I Been Pwned (haveibeenpwned.com) oder dem Identity Leak Checker des Hasso Plattner Instituts (hpi.de).

8 Cyberspionage und -sabotage

Staatliche oder staatsnahe Akteure stellen eine besondere Art der Bedrohung im Cyberraum dar. Die oft auch als «Advanced Persistent Threat» (APT)[110] bezeichneten Gruppen führen Spionage oder seltener Sabotageangriffe durch, wenn es ihren Interessen dient. Im Gegensatz zu finanziell motivierten Cyberkriminellen wählen sie dabei ihre Ziele spezifisch aus und betreiben einen hohen Aufwand, um an die gewünschten Informationen zu kommen oder die beabsichtigte Wirkung zu erzielen. Dementsprechend robuster müssen potenziell betroffene Organisationen auch das Abwehrdispositiv gegen diese Art Bedrohung gestalten.

8.1 Cyberspionage

Die Taifun-Saison

Ende September 2024 berichtete das Wall Street Journal, dass eine Gruppe namens «Salt Typhoon», die mutmasslich für die chinesischen Behörden operierte, mehrere US-amerikanische Telekommunikationsanbieter kompromittiert habe.[111] Nach diesen ersten Enthüllungen gaben die US-Behörden CISA und das Federal Bureau of Investigation (FBI) am 25. Oktober 2024 bekannt, dass sie den unerlaubten Zugriff auf Telekommunikationsinfrastrukturen durch Akteure, die mit der Volksrepublik China in Verbindung stehen, untersuchen.[112] Diese Meldung fiel damals mit mehreren Medienberichten zusammen, denen zufolge Salt Typhoon durch Zugang zu den US-Telekommunikationsriesen gezielt Daten von Telefonen abgriff, die vom ehemaligen und heutigen Präsidenten Donald Trump und vom US-amerikanischen Politiker J.D. Vance sowie von Mitarbeitenden der damaligen Vizepräsidentin Kamala Harris und anderen Persönlichkeiten der Demokratischen Partei genutzt wurden. Darüber hinaus gab es weitere Enthüllungen über eine mögliche Kompromittierung des Systems, das die US-Regierung für die Beantragung von Telefonüberwachungen verwendet. Das genaue Ausmass dieser Kampagne sei noch schwer abzuschätzen. Im Dezember 2024 erklärte das Weisse Haus, es habe neun Telekommunikationsunternehmen als Opfer identifiziert, über welche die Täter potenziell über einen langen Zeitraum hinweg bestimmte Ziele angreifen konnten. In diesem

[109] Siehe Schützen Sie Ihre Konten / Passwörter (ncsc.admin.ch)
[110] APT - Glossary (csrc.nist.gov)
[111] Chinese-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack (wsj.com)
[112] Joint Statement by FBI and CISA on PRC Activity Targeting Telecommunications (cisa.gov)

Fall ermöglichen privilegierte Zugänge dem Angreifer, Anrufe aufzuzeichnen, Nutzer zu lokalisieren und auf die Metadaten der Mobilgeräte zuzugreifen.[113] Gemäss des Sicherheitsunternehmens Trend Micro besteht zudem die Möglichkeit, dass die Kampagne auch auf Einrichtungen ausserhalb der USA abgezielt hatte. Das Unternehmen sieht Ähnlichkeiten zwischen den Aktivitäten von Salt Typhoon und einem von ihm beobachteten Akteur namens «Earth Estries».[114]
Das Ziel von Salt Typhoon ist höchstwahrscheinlich, Zugang zu besonders schützenswerten Informationen zu erhalten. In diesem Bereich bietet eine Kompromittierung von Telekommunikationsanbietern eine ideale Eintrittspforte zu vielen hochinteressanten Zielen, insbesondere zu hochrangigen Politikerinnen und Politikern. Andere Angriffe, die von den US-Behörden ebenfalls chinesischen staatlichen Akteuren zugeschrieben werden, scheinen jedoch eher die Kontrolle über kritische Infrastrukturen erlangen zu wollen. Dies ist der Fall bei der Gruppe «Volt Typhoon», die im letzten Halbjahresbericht des BACS[115] erwähnt worden ist. Die US-Behörden befürchten, dass diese Zugänge im Krisenfall für Sabotageaktionen auf US-Infrastrukturen genutzt werden könnten.[116]

Die Aufmerksamkeit, welche die Vereinigten Staaten den zugeschriebenen feindlichen Aktivitäten Chinas widmet, zeigt sich auch in offiziellen Reaktionen. So gab das US-Justizministerium am 18. September 2024 die Zerschlagung eines Botnets bekannt, welches im Auftrag der chinesischen APT «Flax Typhoon» operiert haben soll. In ihrer Mitteilung betonten die US-Behörden, dass das Botnetz von der chinesischen Firma Integrity Technology Group betrieben wurde. Daraufhin teilte das US-Finanzministerium am 3. Januar 2025 mit, dass es Sanktionen gegen dasselbe Unternehmen wegen seiner Rolle bei Hackerangriffen auf US-Institutionen, die Flax Typhoon zugeschrieben wurden, verhängt hatte[117]. In einer auffallenden zeitlichen Übereinstimmung hatte das US-Finanzministerium kurz zuvor eine Kompromittierung seiner Informatiksysteme publik gemacht, die ebenfalls von einem Akteur mit mutmasslichen Verbindungen zum chinesischen Staat begangen worden war. Die Angreifer verwendeten einen Support-Schlüssel, der von einem Drittanbieter mit privilegiertem Zugang gestohlen worden war.[118]

Neue APT29-Kampagne

Der Bericht des BACS zum ersten Halbjahr 2024 gab bereits Aufschluss über zahlreiche der Gruppe «APT29» zugeschriebenen Spionageaktivitäten. Die Gruppe operiert mutmasslich für den russischen Auslandsgeheimdienst. APT29 wurde auch für eine gross angelegte Kampagne verantwortlich gemacht, die wahrscheinlich ebenfalls zu Spionagezwecken durchgeführt wurde. Ab dem 22. Oktober 2024 beobachtete Microsoft, wie dieser Akteur, den Microsoft als «Midnight Blizzard» nennt, eine Reihe von sehr gezielten Spear-Phishing-E-Mails mit einer signierten RDP-Verbindungsdatei (Remote Desktop Protocol) verschickte. Diese Verbindungsdatei stellte bei Ausführung eine Verbindung zu einem von dem Akteur kontrollierten

---

113 US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage (reuters.com)
114 Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions (trendmicro.com)
115 Halbjahresbericht 2024/1 (ncsc.admin.ch)
116 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (cisa.gov)
117 Treasury Sanctions Technology Company for Support to Malicious Cyber Group (treasury.gov)
118 US Treasury says Chinese hackers stole documents in 'major incident' (reuters.com)

Server her.[119] Ziel dieser Kampagne waren laut Microsoft Regierungsbehörden, Hochschulen, Verteidigungsorganisationen und Nichtregierungsorganisationen in Dutzenden von Ländern, vorwiegend in Europa, Australien und Asien. Ähnliche Aktivitäten wurden auch vom Computer Emergency Response Team der Ukraine (CERT-UA) unter der Bezeichnung «UAC-0215» sowie von Amazon gemeldet.[120] Die Phishing-E-Mails dieser Kampagne wurden von E-Mail-Adressen legitimer Organisationen versendet. Diese E-Mail-Adressen waren bei früheren Kompromittierungen gesammelt worden.

Weiterentwicklung der Vorgehensweisen

Die raffiniertesten Gruppen, die im Bereich der Cyberspionage aktiv sind, verfügen über die Fähigkeit, ihr offensives Arsenal ständig weiterzuentwickeln und zu verbessern. Dies ermöglicht ihnen, neue Gelegenheiten auszunutzen und bestehende Verteidigungsmassnahmen zu umgehen. Der Berichtszeitraum bot zwei Beispiele für dieses spezifische Können.
Im Oktober 2024 schrieb der Anbieter der Sicherheits-Software ESET eine Reihe von Angriffen auf eine Regierungsorganisation in Europa dem APT-Akteur «GoldenJackal» zu. Laut ESET entwickelte dieser Akteur zwei verschiedene Schritte, um physisch isolierte Systeme (Air Gap) mithilfe eines USB-Sticks zu kompromittieren. In einem ersten Schritt wird der USB-Stick in ein mit dem Internet verbundenes System eingesteckt, das bereits kompromittiert worden ist. Die bei dieser ersten Kompromittierung verwendete Methode ist jedoch noch unbekannt. Der gleiche USB-Stick infiziert anschliessend das isolierte System, sobald er dort angeschlossen wird. Schliesslich werden die Daten erneut über das mit dem Internet verbundene System abgegriffen, sobald der USB-Stick wieder bei diesem System eingesteckt wird. Ein Air Gap wird in der Regel für kritische Netzwerke – wie industrielle Steuerungssysteme oder Hochsicherheitsnetzwerke – eingesetzt. Die für die Entwicklung eines solchen Tools erforderlichen Ressourcen lassen auf die Beteiligung eines Staates schliessen. ESET macht keine eindeutige Zuordnung, sieht aber bei den Vorgehensweisen Ähnlichkeiten mit vermeintlich russischen APTs, insbesondere «Turla».[121]

Im November 2024 beschrieb das Cybersicherheitsunternehmen Volexity eine andere, kreative Vorgehensweise, die von «GruesomeLarch», einer mutmasslich russischen APT (auch bekannt als «APT28» oder «Sofacy»), verwendet wurde. Die Gruppe operiert vermutlich für den russischen Militärgeheimdienst. Zur Erreichung ihrer Cyberspionage-Ziele drang die Gruppe in die Netzwerke ihrer Ziele ein, indem sie sich mit dem Wifi-Netzwerk des Unternehmens verband. Die Strategie des Angreifers bestand darin, in eine andere, dem Ziel benachbarte Organisation einzudringen, sich dann innerhalb dieser Organisation weiter auszubreiten, um Systeme mit dualer Verbindung, sprich Systeme mit einer kabelgebundenen und einer drahtlosen Netzwerkverbindung zu finden und sich von diesem kompromittierten Nachbarsystem aus mit dem Wifi-Unternehmensnetzwerk des Opfers zu verbinden.[122]

---

119 Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files (microsoft.com)
120 Amazon identified internet domains abused by APT29 (aws.amazon.com)
121 Mind the (air) gap: GoldenJackal gooses government guardrails (welivesecurity.com)
122 The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access (volexity.com)

Schlussfolgerungen

Die hohe Bereitschaft solcher Angreifer, Zeit und Ressourcen in Hilfsmittel zu investieren, ermöglicht es ihnen in die sichersten Netzwerke überhaupt einzudringen. Grundlegend sollte es nicht erlaubt sein, dass USB-Sticks in gesicherten und physisch isolierten Systemen auf allen Geräten eingesteckt werden können. Nur bestimmte genau definierte Verbindungen sollten nach aussen möglich sein und diese Verbindungen müssen überwacht werden. Auch die Kompromittierung eines benachbarten Unternehmens kann ein Sicherheitsrisiko darstellen. Beim WLAN ist es zudem wichtig, zwischen dem Gastnetzwerk und dem stärker geschützten Unternehmensnetzwerk zu unterscheiden.

Angebliche IT-Mitarbeitende

Akteure, die wahrscheinlich im Auftrag der nordkoreanischen Regierung arbeiten, nehmen seit längerer Zeit eine Sonderstellung unter den offensiven staatlichen Cyberakteuren ein. Denn sie betreiben nicht nur Cyberspionage, sondern führen einen grossen Teil ihrer Aktivitäten zu finanziellen Zwecken durch. Dieser Trend steht im Einklang mit den Prioritäten des nordkoreanischen Regimes, das aufgrund von zahlreichen Wirtschaftssanktionen Devisen benötigt.

Mit Nordkorea in Verbindung gebrachte Akteure haben häufig Handelsplattformen für Kryptowährungen angegriffen. In den letzten Tagen des Berichtszeitraums machten die US-amerikanischen und japanischen Behörden einen staatlichen Akteur aus Nordkorea dafür verantwortlich, 308 Millionen USD von der Handelsplattform DMM im Mai 2024 gestohlen zu haben.[123] In diesem wie auch in vielen anderen Fällen besteht der Angriffsvektor aus einem angeblichen Rekrutierungsprozess für IT-Mitarbeitende, bei dem versucht wird, dem Ziel einen bösartigen Code zu übermitteln.[124] Die Akteure haben in letzter Zeit jedoch regelmässig auf eine andere Methode zurückgegriffen, bei der sie ihre Agenten als IT-Mitarbeitende in Fernarbeit für westliche Unternehmen vermitteln. Dazu verwenden sie falsche Identitäten sowie technische Hilfsmittel (insbesondere VPN), um ihren Aufenthaltsort zu verschleiern. Sie schrecken auch nicht davor zurück, mithilfe von KI Fotos oder Videos zu generieren.[125] Diese Methode erwies sich als sehr profitabel. So machte das US-Justizministerium in einer am 12. Dezember 2024 veröffentlichten Anklageschrift 14 nordkoreanische Staatsangehörige für einen sechs Jahre dauernden Betrug dieser Art verantwortlich, bei dem 88 Millionen USD an das nordkoreanische Regime geflossen sein sollen.[126]

---

123 FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com (fbi.gov)

124 Zu dieser Methode siehe insbesondere die Einzelheiten einer Kampagne mit dem Namen «contagious interview»: Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Install New Variants of BeaverTail and InvisibleFerret Malware (unit42.paloaltonetworks.com)

125 Das Unternehmen Knowbe4 hat in diesem Zusammenhang ein konkretes Beispiel eines Rekrutierungsprozesses mit einem solchen Bewerber mit bösen Absichten geteilt: How a North Korean Fake IT Worker Tried to Infiltrate Us (blog.knowbe4.com)

126 Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions (justice.gov)

Diese Bedrohung hat viele Facetten und der Zugang solcher Mitarbeitenden zu westlichen Unternehmensnetzwerken kann auf verschiedene Weise gewinnbringend genutzt werden. Einerseits verdienen diese Mitarbeitenden Geld in Form des Gehalts, das sie für ihre Arbeit in den Unternehmen erhalten. Andererseits wurden aber auch Fälle beobachtet, in denen sie sensitive Daten entwendeten und anschliessend ihre ehemaligen Arbeitgeber erpressten. Diese Akteure scheinen nicht nur finanzielle Ziele zu verfolgen, ihr Zugang zu Unternehmensnetzwerken kann unter Umständen auch für Spionagezwecke genutzt werden.

Empfehlungen

Die Abwehr dieser Bedrohungsart muss auf mehreren Ebenen erfolgen. In erster Linie geht es darum, auffällige Verhaltensweisen oder Elemente im Anstellungsprozess zu erkennen. Andererseits sollte während des Anstellungsprozesses Überprüfungen vorgenommen werden, um die Identität der Bewerbenden sicherzustellen.[127]

8.2 Bedrohung industrieller Kontrollsysteme und operativer Technologie

Die Digitalisierung führt nicht nur zum Einsatz von mehr und mehr Informationstechnologie im Daten- und Informationsraum, sondern erfasst, respektive steuert, immer mehr auch physische Prozesse. Die dafür eingesetzte, früher meistens isolierte operative Technologie (OT) wie industrielle Steuerungen (ICS) vernetzt sich zunehmend mit der restlichen Systemlandschaft und setzt sich so auch Risiken aus deren Umfeld aus.

Personen, die sich nicht im industriellen Umfeld bewegen, kommen mit dieser Entwicklung wohl am ehesten durch die Fortschritte in der Gebäudeautomatisierung im Rahmen von «Smart Home» Projekten in Kontakt. Nicht verwunderlich ist daher, dass Sicherheitsspezialisten im industriellen Umfeld eine Zunahme der Angriffsversuche auf die Gebäudeautomation beobachteten.[128]

Erfolgreiche Angriffe gegen solch industriell geprägte Systeme mit folgenschweren Auswirkungen in der physischen Welt werden weiterhin fast ausschliesslich im Rahmen bereits eskalierter Konflikte registriert. So wurde Ende Juli 2024 bekannt, dass bei einem zweitägigen Ausfall einer Heizungsanlage für rund 600 Wohngebäude in der Ukraine ein Sabotage-Angriff verantwortlich war. Über das Protokoll Modbus, welches im Umfeld von cyberphysischen industriellen Systemen Anwendung findet, wurde die speziell ausgelegte Schadsoftware «FrostyGoop» eingesetzt.[129] Der zweite Konflikt, in dessen Rahmen auch immer wieder Cyberangriffe eine Nebenrolle einnehmen, liegt im Nahen Osten. So nutzten Akteure, die bereits in früheren Angriffen mit den iranischen Revolutionsgarden in Verbindung gebracht wurden, die Malware «IOCONTROL» um IoT und OT-Geräte zu manipulieren.[130] Auf der Gegenseite behaupteten

---

127 The latest in North Korea's fake IT worker scheme: Extorting the employers (therecord.media)
Dieses umfassende Dokument der britischen Behörden enthält eine Reihe von Empfehlungen: Advisory on North Korean IT Workers (gov.uk)

128 2024 Global Threat Roundup (forescout.com)

129 Impact of FrostyGoop ICS Malware on Connected OT Systems (dragos.com)

130 Inside a New OT/IoT Cyberweapon: IOCONTROL (claroty.com)

Hacktivisten, die sich als «Red Devil» bezeichnen, sie hätten Wasseraufbereitungsanlagen im Südlibanon sabotiert.[131]
Neben Cyberangriffen haben auch physische Interventionen Auswirkungen auf die Informations- und Kommunikationstechnologie. So wurden Pager und Funkgeräte der Hisbollah in der Herstellungs- und Lieferkette manipuliert und nach Auslieferung zur Explosion gebracht.[132] In der Ostsee veranlasste eine Häufung an zerstörten Unterseekabeln die betroffenen Anrainerstaaten zu einer Erhöhung der Sicherheitsmassnahmen zu deren Schutz.[133]

Ausserhalb der Konfliktgebiete verüben mit den Konfliktparteien verbandelte Hacktivisten ebenfalls vereinzelte Sabotageversuche. So machte sich die pro-russische Gruppierung «Z-Pentest» an dänischen Pump-Kontrollsystemen zu schaffen, deren Auswirkungen jedoch unter Kontrolle gebracht werden konnten.[134]

Künftig könnte der auf europäischer Ebene am 10. Dezember 2024 in Kraft getretene «Cyber Resiliency Act» (CRA) einen wichtigen Beitrag leisten, dass OT- und IoT- Systeme besser geschützt werden können, indem Hersteller in die Pflicht genommen werden, ein Mindestmass an Sicherheitsfunktionalitäten bereitzustellen.[135]

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.

131 Israeli Group Claims Lebanon Water Hack as CISA Reiterates Warning on Simple ICS Attacks (securityweek.com)
132 Lebanon pager and walkie-talkie explosions: What we know so far (apnews.com)
133 We assume damage to Baltic Sea cables was sabotage, German minister says (theguardian.com)
134 »Koden var 1234«: For første gang er dansk vandforsyning blevet angrebet af prorussiske hackere (jyllands-posten.dk)
135 Cyber Resilience Act (digital-strategy.ec.europa.eu)