7. November 2024 | Bundesamt für Cybersicherheit BACS

Halbjahresbericht 2024/I (Januar – Juni)

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

Der Halbjahresbericht des Bundesamts für Cybersicherheit (BACS) präsentiert die wichtigsten Cyberphänomene, welche die Bedrohungslandschaft der Schweiz aktuell prägen. Anhand von Cybervorfällen und Entwicklungen der ersten Jahreshälfte 2024 in der Schweiz und international wird aufgezeigt, wie verschiedene Bedrohungsakteure im Cyberraum mit unterschiedlichen Methoden versuchen, ihre Ziele zu erreichen.
Das BACS hat im ersten Halbjahr 2024 34'789 Meldungen zu Cybervorfällen erhalten. Im Vergleich zur Vorjahresperiode entspricht dies einem signifikanten Anstieg um 15'740 Meldungen. Diese beinahe Verdoppelung ist vor allem auf die Zunahme der Phänomene «gefälschte Anrufe im Namen der Polizei», «betrügerische Gewinnspiele», «Abofallen» und «Phishing» zurückzuführen. Rund 90 % der Meldungen an das BACS erfolgten durch Privatpersonen, 10 % von Unternehmen. Wie in den Vorjahren wurden die meisten Meldungen zu den Kategorien «Betrug», «Phishing» und «Spam» erstattet.

Betrug – am häufigsten gemeldet

Mit 23’104 Meldungen ist Betrug nach wie vor das am häufigsten gemeldete Phänomen und macht zwei Drittel aller Meldungen im ersten Halbjahr 2024 aus. Im Vergleich zur Vorjahresperiode (11’174) hat sich diese Zahl mehr als verdoppelt. Von diesen Meldungen sind 13’730, also fast 60 %, auf gefälschte Behördenanrufe zurückzuführen. Bei diesem Phänomen werden in grosser Anzahl zufällige Nummern angerufen und den Opfern vorgegaukelt, sie seien in ein Strafverfahren verwickelt und sollen für das weitere Vorgehen die Taste «1» drücken. Anschliessend werden die Opfer mit einem Betrüger verbunden und von diesem dazu gedrängt, eine Fernzugriffs-Software herunterzuladen, die es den Betrügern erlaubt, auf deren Computer zuzugreifen und ungewollte Zahlungen im E-Banking auszulösen.

Markanter Anstieg der Phishing-Meldungen

Im ersten Halbjahr 2024 erhielt das BACS 6'643 Meldungen zu Phishing, was einem markanten Anstieg um rund 2'800 Meldungen im Vergleich zur Vorjahresperiode entspricht (3'879 Meldungen). Nach wie vor betrafen die meisten Phishing-Versuche gefälschte Paketbenachrichtigungen sowie Rückerstattungs-E-Mails im Namen von Lieferanten, der SBB respektive SwissPass sowie verschiedener Steuerverwaltungen. Insbesondere Phishing-Versuche gegen Microsoft-365-Konten werden dem BACS immer wieder gemeldet. Eine aktuell verbreitete Vorgehensweise beinhaltet eine schneeballartige Verteilung von Phishing-E-Mails, das sogenannte «Chain Phishing», bei dem nach der Kompromittierung des E-Mail-Postfachs sofort Phishing-Nachrichten an das gesamte Adressbuch versendet werden.

DDoS-Angriffe im Rahmen von Grossanlässen und internationalen Konferenzen

Bei Angriffen auf die Verfügbarkeit von Websites und -diensten – auch bekannt als «Distributed Denial of Service» (DDoS) – versuchen Angreifer, eine Website oder einen Internetdienst mithilfe von zahlreichen Anfragen für die Nutzung vorübergehend unzugänglich zu machen. Im Berichtshalbjahr wurden insbesondere drei DDoS-Kampagnen beobachtet: Im April 2024 meldeten verschiedene Schweizer Organisationen aus dem Finanzsektor DDoS-Angriffe, die mit einer Erpressung gekoppelt waren. Zu diesen Angriffen bekannte sich angeblich die Gruppe «Armada Collective» respektive «Alpha Jackal». Neben finanziellen Motiven setzten Bedrohungsakteure erneut DDoS-Angriffe mit politischen Absichten im Umfeld von internatio-

nalen Grossveranstaltungen und Konferenzen in der Schweiz ein. Das pro-russische Hacktivisten-Kollektiv «NoName057(16)» zielte im Januar 2024 auf Websites im Zusammenhang mit dem Weltwirtschaftsforum (WEF) und im Juni 2024 auf Websites von Organisationen mit Verbindungen zur «Konferenz zum Frieden in der Ukraine» auf dem Bürgenstock. Insgesamt lagen die Angriffe jeweils im erwarteten Rahmen und führten nur zu geringfügigen Beeinträchtigungen der IT-Infrastruktur. Zu keinem Zeitpunkt waren die IT-Systeme und Daten dieser Veranstaltungen oder der beteiligten Organisationen ernsthaft gefährdet.

Ransomware – eine nationale und globale Herausforderung

Der Meldeeingang beim BACS zu Ransomware-Angriffen auf Unternehmen ist leicht rückläufig. Dabei verantworten die drei Ransomware-Gruppen «Akira», «8Base» und «Black Basta» im Berichtszeitraum mehrere Angriffe auf Schweizer Unternehmen. Opfer von Ransomware-Angriffen finden sich in allen Branchen und Unternehmensgrössen. Bei Privatpersonen setzt sich der bisherige Trend fort, dass sie immer weniger im Fokus der Cyberkriminellen stehen. Wegen des typischen opportunistischen Verhaltens von Ransomware-Gruppen könnten vermehrt gezielte Angriffe auf sehr lukrative Opfer diese Entwicklung beeinflusst haben. Auch international stellen Ransomware-Angriffe Unternehmen und Behörden vor Herausforderungen.

Weitere Phänomene

Der Bericht beleuchtet ferner die Trends und Entwicklungen in Bezug auf Schwachstellen, Schadsoftware bei Mobilgeräten und initialem Zugang. Auch der Umgang mit Daten erfordert die Aufmerksamkeit. Nach Datenlecks werden abgeflossene Daten häufig zur Kompromittierung von IT-Systemen und für Social-Engineering-Angriffe in Betrugsfällen genutzt. Schliesslich gibt der Bericht einen Überblick über die Cyberspionage- und Sabotageaktivitäten im Kontext von geopolitischen Spannungen und des Rekordwahljahres 2024. Dieses Kapitel beruht zwar mehrheitlich auf Beobachtungen aus dem Ausland, ist aber für eine umfassende Beurteilung der Schweizer Bedrohungslage zentral.

Inhalt

Editorial **4**

1 Cyberbedrohungen in der Schweiz – ein Überblick **6**

2 Phishing **8**

2.1 Chain Phishing etabliert sich ***11***

2.2 Der zweite Faktor rückt ins Visier ***11***

3 Schadsoftware **13**

3.1 Initialer Zugang mit Schadsoftware ***13***

3.2 Ransomware ***16***

3.2.1 Ransomware-Aktivitäten in der Schweiz *16*

3.2.2 Ransomware als globale Herausforderung *18*

3.3 Schadsoftware auf Mobilgeräten ***20***

4 Schwachstellen **22**

5 Betrug und Social Engineering **23**

5.1 Methoden der künstlichen Intelligenz bei Betrugsversuchen ***24***

5.2 Werbung für Investmentbetrug ***25***

6 Störung der Verfügbarkeit von Websites und -diensten (DDoS) **26**

7 Datenmanagement, -abflüsse und -erpressung **28**

7.1 Datenabflüsse bei Zulieferern ***28***

7.2 Legaler und illegaler Datenhandel ***30***

8 Cyberspionage und -sabotage **33**

8.1 Cyberspionage ***34***

8.1.1 Politische Institutionen unter Druck *34*

8.1.2 Internationale Entwicklungen in der Cyberspionage *35*

8.2 Bedrohung Industrieller Kontrollsysteme und operativer Technologie ***37***

Editorial

Das Bundesamt für Cybersicherheit BACS blickt auf die ersten 182 Tage seiner Tätigkeit zurück. Es waren spannende sechs Monate mit einigen herausfordernden Projekten, richtungsweisenden Entscheiden sowie einer Konsolidierung von neuen Strukturen mit solchen, die sich bereits bewährt haben. Der eingeschlagene Weg ist nicht immer einfach, aber das Ziel, die Schweiz resilienter vor Cyberbedrohungen zu machen, steht für alle Mitarbeitenden des BACS im Fokus.

Die Weiterentwicklung des BACS ist ein stetiger Prozess und einige Meilensteine wurden bereits erreicht. So hat das BACS Mitte Juni anlässlich der «Hochrangigen Konferenz zum Frieden in der Ukraine» bewiesen, dass es über die Fähigkeiten verfügt, zusammen mit seinen Partnern in kurzer Zeit besondere Leistungen zu bringen. Unser Amt hatte im nationalen Cyberlageverbund die Gesamtkoordination inne und konnte die (Cyber-)Sicherheit aller Beteiligten und der für die Durchführung der Konferenz notwendigen Infrastrukturen jederzeit gewährleisten. Der Schlüssel, um in kurzer Zeit einen so exponierten Anlass abzusichern, war eine konsequente risikobasierte Planung und das Sicherstellen, dass alle Einsatzkräfte die gleichen Ziele verfolgen. Dies integrierte auch, dass die beteiligten Organisationen jederzeit über den notwendigen Informationsstand verfügten und entsprechend abgestimmt agieren konnten. Dies war möglich, da die Mitarbeitenden des BACS dank fundiertem Fachwissen und Verständnis über die Cyberrisiken mit allen Partnern und Stakeholdern national und international auf Augenhöhe diskutieren konnten. Neben der Koordination war das BACS im Vorfeld auch für das «Attack Surface Management» bedrohter Infrastrukturen und die Sensibilisierung potenziell betroffener Organisationen verantwortlich und kam bei der Vorfallbewältigung zum Einsatz. An dieser Stelle möchte ich mich bei allen Partnern für die vorbildliche Zusammenarbeit bedanken. Ein besonderer Dank gilt der Kantonspolizei Luzern und Nidwalden, welche unsere Mitarbeitenden in ihre Einsatzorganisationen integriert haben. Meine Mitarbeitenden und ich freuen uns, dass wir durch dieses Erlebnis nochmals näher zusammenwachsen konnten. Denn nur gemeinsam erhöhen wir die Cybersicherheit in der Schweiz.

In meinem letzten Editorial habe ich unter anderem die hohe Verwundbarkeit von IT-Systemen und die vielerorts noch schwach ausgeprägte Reaktionsfähigkeit bei systemrelevanten Cybervorfällen angesprochen. Anfang Juni 2024 wurde die Firma Synnovis, ein Dienstleister mehrerer Londoner Krankenhäuser, Opfer eines Ransomware-Angriffes. Aufgrund der damit einhergegangenen Systemausfälle mussten während rund fünf Wochen mehr als 6'000 Termine für Operationen und Bluttransfusionen verschoben werden. Dies zeigt einmal mehr, wie wichtig die Cybersicherheit einzustufen ist. Es müssen jedoch nicht immer derart gewaltige Ausfälle sein, die grosse Probleme verursachen. Schon Cybervorfälle, die für sich alleine genommen keine direkte Gefährdung des Staates bewirken, können bei Betroffenen grosse Ängste und finanzielle Verluste auslösen und in Einzelfällen ein betroffenes Unternehmen in den Konkurs treiben. Eine Häufung solcher Vorfälle kann dazu führen, dass durch die Masse dann doch eine nationale Bedrohung entsteht. Deshalb ist es betreffend Cybersicherheit wichtig, nicht nur an kritische Infrastrukturen zu denken, sondern einen Beitrag dafür zu leisten, dass alle Unternehmen in der Schweiz, angefangen beim Einmann-Betrieb bis hin zu Betreibenden in systemkritischen Sektoren, so uneingeschränkt wie möglich ihre Arbeit erledigen können.

Ich freue mich auf die Herausforderungen im zweiten Halbjahr 2024 und wünsche Ihnen beim Lesen des aktuellen Halbjahresberichts viele neue Erkenntnisse, wie Sie Ihre Cybersicherheit noch weiter erhöhen können.

Florian Schütz, Direktor Bundesamt für Cybersicherheit

1 Cyberbedrohungen in der Schweiz – ein Überblick

Cyberbedrohungen sind zu einem integralen Bestandteil der Bedrohungslandschaft in der Schweiz aber auch international geworden. Während die bekannten Phänomene wie Phishing, die Verteilung von Schadsoftware oder auch Spionageaktivitäten im Cyberraum über die Jahre hinweg konstant zu beobachten waren, entwickeln Bedrohungsakteure die eingesetzten Methoden und Taktiken innerhalb der Phänomene kontinuierlich weiter. Dieses dynamische Umfeld zeigte sich im ersten Halbjahr 2024 beispielsweise im verstärkten Einsatz von maschinellem Lernen (ML)[1] bei Betrugsversuchen[2] oder bei Phishing[3]. Auch erweitern Bedrohungsakteure stetig ihre Palette der genutzten Kanäle, um ihre Angriffe auszuführen. So wurden z. B. vermehrt Dienste wie Google Ads für Investmentbetrug missbraucht. Je nach Nutzen-Kosten-Kalkül manifestieren sich diese beobachteten Erneuerungen oder bleiben ein einmaliges Experiment.

Im ersten Halbjahr 2024 sind beim BACS gesamthaft 34'789 Meldungen eingegangen, was einen signifikanten Anstieg von 15'740 Meldungen zur Vergleichsperiode im Vorjahr bedeutet. Diese beinahe Verdoppelung ist vor allem auf die Zunahme der Phänomene «gefälschte Anrufe im Namen der Polizei»[4], «betrügerische Gewinnspiele»[5], «Abofallen»[6] und «Phishing» zurückzuführen. Zu den gefälschten Anrufen im Namen der Polizei[7] haben sich die Meldungen besonders ab Kalenderwoche 10 bis 18 stark erhöht, was zu klar erkennbaren Spitzenwerten bei den Gesamtmeldungen führte (vgl. Abb. 1). Dank Massnahmen seitens der Telekommunikationsanbieter konnte die Welle an solchen gefälschten Anrufen bis Juni 2024 gebrochen werden, weshalb auch die Gesamtzahl der Meldungen am Ende der Berichtsperiode kontinuierlich zurückging.
Die Mehrheit der Meldungen erfolgt durch die Bevölkerung (90 %). Die restlichen 10 % der Meldungen werden von Unternehmen[8] getätigt. Deshalb ist es auch wenig verwunderlich, dass die meisten Meldungen Betrugsfälle, Phishing und Spam betreffen (vgl. Abb. 2). Leicht rückläufig war dabei die Zahl der Meldungen zu Ransomware-Angriffen[9] auf Unternehmen. Während im zweiten Halbjahr 2023 beim BACS 56 Meldungen eingingen, waren es in der aktuellen Berichtsperiode noch 39 Meldungen. Ransomware bei Privatpersonen hat sich in den letzten Monaten auf niederem, einstelligem Niveau stabilisiert. Obwohl eine Diskrepanz zwischen der Anzahl Meldungen von Vorfällen und der Realität nicht ausgeschlossen werden kann, scheinen sich Ransomware-Akteure von vielen, weniger gewinnbringenden zu ein paar wenigen, aber höchst lukrativen Zielen wegzubewegen.

---

1 Maschinelles Lernen (wikipedia.org)

2 Siehe Betrügerische Gewinnspiele (ncsc.admin.ch), Betrügerische Jobangebote (ncsc.admin.ch), Fake-Support (ncsc.admin.ch), oder auch CEO-Betrug (ncsc.admin.ch)

3 Phishing, Vishing, Smishing (ncsc.admin.ch)

4 Anrufe im Namen von Fake-Behörden (Polizei, Zoll) (ncsc.admin.ch)

5 Betrügerische Gewinnspiele (ncsc.admin.ch)

6 Abofallen (ncsc.admin.ch)

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

8 Die Kategorie «Unternehmen» integriert auch Vereine und Behörden.

9 Ransomware (ncsc.admin.ch)

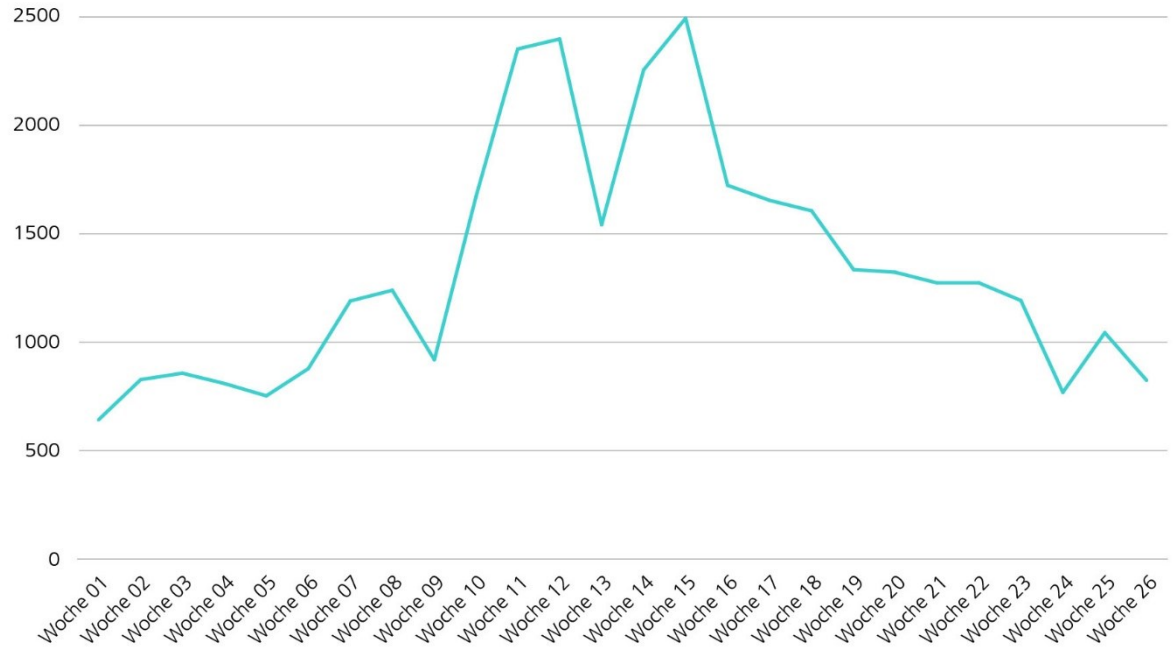

Abb. 1: Anzahl Meldungen pro Woche an das BACS im ersten Halbjahr 2024, vgl. Aktuelle Zahlen (ncsc.admin.ch).

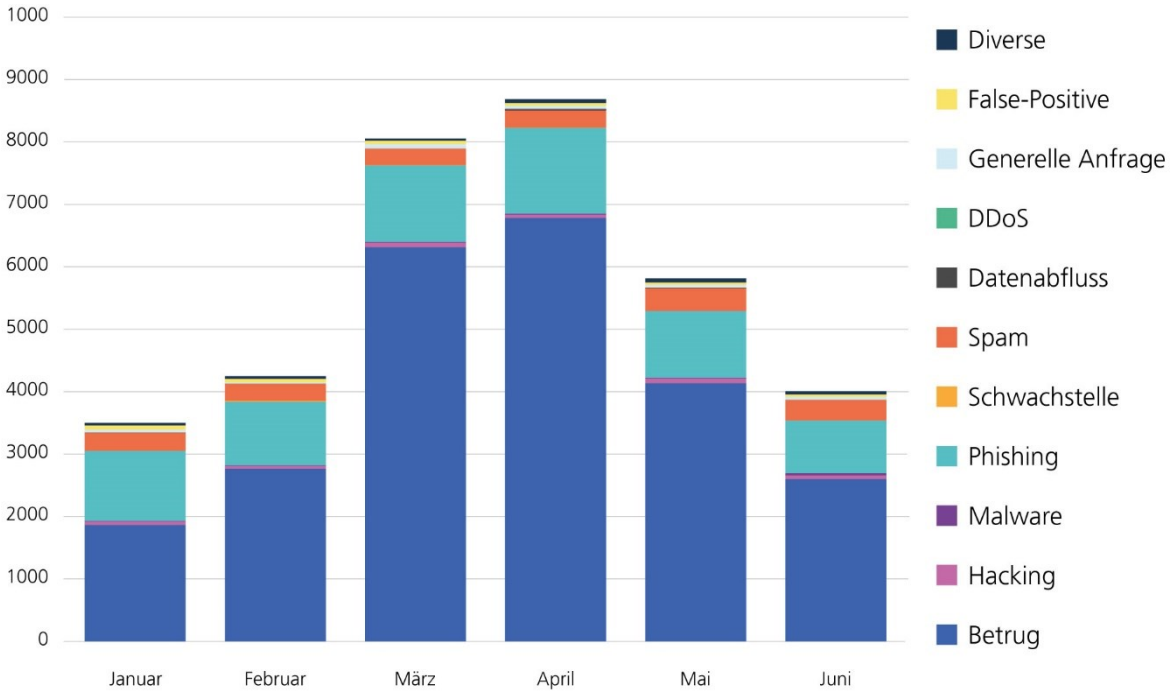

Abb. 2: Meldungen an das BACS im ersten Halbjahr 2024 nach Kategorien, vgl. Aktuelle Zahlen (ncsc.admin.ch).

Die Statistik verdeutlicht, dass die Cybersicherheit und der Schutz der Schweiz vor Cyberrisiken eine immerwährende Herausforderung für Wirtschaft, Staat und Gesellschaft darstellt. Mit der Schaffung des Bundesamts für Cybersicherheit (BACS) am 1. Januar 2024 wurde auch

der zwei Mal jährlich erscheinende Halbjahresbericht in seiner Struktur überarbeitet.[10] Demnach thematisiert der Halbjahresbericht in jedem Kapitel verschiedene Kernphänomene, die die Bedrohungslandschaft in der Schweiz wesentlich prägen: Dies beinhaltet Phishing, Schadsoftware, Schwachstellen, Betrugsfälle und Social-Engineering[11], Angriffe auf die Verfügbarkeit von Internet-exponierten Diensten (DDoS), Datenabflüsse sowie Cyberspionage und -sabotage. Das Hauptziel, die Öffentlichkeit zum Thema Cybersicherheit zu informieren, bleibt bestehen. Der Halbjahresbericht soll anhand von Vorfällen aktuelle Cyberbedrohungen und Herausforderungen aufzeigen und Empfehlungen für die Bevölkerung ableiten. Denn alle sind nach dem Prinzip der Eigenverantwortung gefordert, im Sinne ihrer Fähigkeiten und Möglichkeiten für eine sichere Schweiz im digitalen Raum beizutragen.

2 Phishing

Phishing-Seiten gehören neben Betrugsfällen zu den am häufigsten gemeldeten Cyber-Vorfällen ans BACS. Spezifisch ermöglicht es Bedrohungsakteuren das Sammeln von Zugangsdaten, Finanzinformationen und anderen vertraulichen Daten von ahnungslosen Nutzerinnen und Nutzern im Cyberraum. Typisch an Phishing ist, dass das Austricksen der Nutzerinnen und Nutzer (Social-Engineering) im Zentrum steht und Schadsoftware dabei nicht in erster Linie zur Anwendung kommt.[12] Während Phishing für einen grossen Empfängerkreis via E-Mail noch immer zur gängigsten Methode gehört, nutzen andere Ansätze die Stimme (Voice-Phishing oder Vishing) oder SMS (Smishing), um an sensitive Informationen zu gelangen.

Das BACS erhielt im ersten Halbjahr 2024 mehr Meldungen[13] zu Phishing-Seiten (6'643) über sein Meldeformular, als im Vergleich zum Vorjahr (3’879). Die am häufigsten gemeldeten Phishing-Versuche blieben dabei unverändert. Immer noch werden gefälschte Paketbenachrichtigungen zu Tausenden versendet. Auch angebliche Rückerstattungs-E-Mails im Namen von Lieferanten, der SBB respektive SwissPass oder auch verschiedener Steuerverwaltungen gehören zum Standardrepertoire der Phisher. Ähnliches widerspiegelt sich auch in anderen statistischen Werten, die Phishing-Kampagnen in der Schweiz dokumentieren. Bei der Anzahl der durch das BACS überprüften und bestätigten Phishing-URLs zeigte sich ebenfalls ein Anstieg. Während letztes Jahr im ersten Halbjahr noch 4'765 einzigartige Phishing-URLs rapportiert wurden, verdoppelten sich diese auf 11'505 einzigartige URLs im gleichen Zeitraum im Jahr 2024. Die wöchentliche Entwicklung ist in Abbildung 3 illustriert. Um die Phishing-Seiten so glaubhaft wie möglich zu gestalten, missbrauchen Kriminelle immer wieder bekannte Marken und Unternehmen. Am häufigsten wurden in dieser Berichtsperiode der Finanzsektor (26 %), Postdienste (24 %), der öffentliche Verkehr (23 %), die Telekommunikation (11 %) und der IT-Sektor (8 %) für Phishing unrechtmässig benutzt. Dieses Verhältnis blieb über die verschiedenen Monate vergleichsweise konstant (vgl. Abb. 4).

---

[10] Weitere Halbjahresberichte finden Sie unter Lageberichte (ncsc.admin.ch)

[11] Social Engineering (ncsc.admin.ch)

[12] 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.

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

Um möglichst viele potenzielle Opfer vor Phishing zu schützen, ist das BACS bestrebt, solche Webauftritte so schnell wie möglich deaktivieren zu lassen. Im Gegensatz dazu setzen die Betrüger alles daran, eine rasche Deaktivierung der Seiten zu verhindern. Die Phisher suchen deshalb immer wieder nach neuen Methoden, damit Sicherheitsbehörden möglichst lange nichts von den Phishing-Seiten erfahren und diese abschalten können. Mittlerweile können etliche Phishing-Seiten nur mit spezifischen Nutzerkonfigurationen aufgerufen werden. Eine beliebte Variante dabei ist, Zugriffe auf betrügerische Webseiten nur via Smartphones zuzulassen. Alle anderen Zugriffe von PCs oder anderen internetfähigen Geräten werden dagegen auf legitime Webseiten umgeleitet. Hintergrund ist, dass die meisten Internetnutzer nur noch mit Smartphones unterwegs sind, die Sicherheitsbehörden aber mit PCs.
Ein anderer Ansatz mit einem Selbstselektionsmechanismus zeigte sich in dieser Berichtsperiode.[14] Anstatt direkt eine Phishing-E-Mail mit dem Link zu einer Phishing-Seite zu versenden, wird das Opfer in einer unverfänglichen E-Mail aufgefordert, auf diese zu antworten. Erst in einem zweiten Schritt, nachdem eine Antwort des Opfers eingegangen ist, wird der Phishing-Link per E-Mail zurückgeschickt. Es handelt sich dabei um eine vorgefertigte E-Mail, die unabhängig von der eingegangenen Kommunikation, automatisiert an den Sender zurückgeschickt wird. Mit dieser Herangehensweise soll vor allem verhindert werden, dass der Link zur Phishing-Seite durch einen zu grossen Empfängerkreis zu schnell an Sicherheitsbehörden – wie z. B. an das BACS – weitergeleitet werden. So erhalten nur diejenigen den Link, die den Betrugsversuch nicht erkennen und ihn wahrscheinlich auch nicht melden. Es erhöht die Wahrscheinlichkeit, dass die Seite länger online bleibt und mehr potenzielle Opfer erreicht werden können, um Kreditkartendaten oder Passwörter zu beschaffen.
Nicht zuletzt erlangte eine Phishing-Kampagne gegen PostFinance-Kunden die Aufmerksamkeit der Medien, da diese einen selten benutzen Verteilungskanal nutzte.[15] Bei dieser versendeten die Phisher im Mai 2024 Briefe per Post, die einen QR-Code zu einer Phishing-Seite beinhalteten. Sie behaupteten, dass eine Reaktivierung des E-Banking-Zugangs für die weitere, sichere Verwendung notwendig sei. Die PostFinance erklärte in ihrer Kommunikation, dass sie nie solche Briefe versendet und daher die Briefe ignoriert werden sollten.[16]

Empfehlungen

Melden Sie dem BACS verdächtige Phishings via reports@antiphishing.ch oder direkt per 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 Spezialisten melden. Mit Ihrer Hilfe kann das BACS gezielt warnen und Massnahmen einleiten, damit die Webseiten vom Internet genommen werden.

14 Woche 11: Recycling ist gut, aber nicht bei Passwörtern (ncsc.admin.ch)

15 Siehe u. a. Phishing: Brief von Postfinance entpuppt sich als Betrugsversuch (srf.ch), Phishing: Postfinance warnt vor neuer Masche (blick.ch)

16 Phishing-Briefe mit gefälschtem QR-Code im Umlauf (postfinance.ch)

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

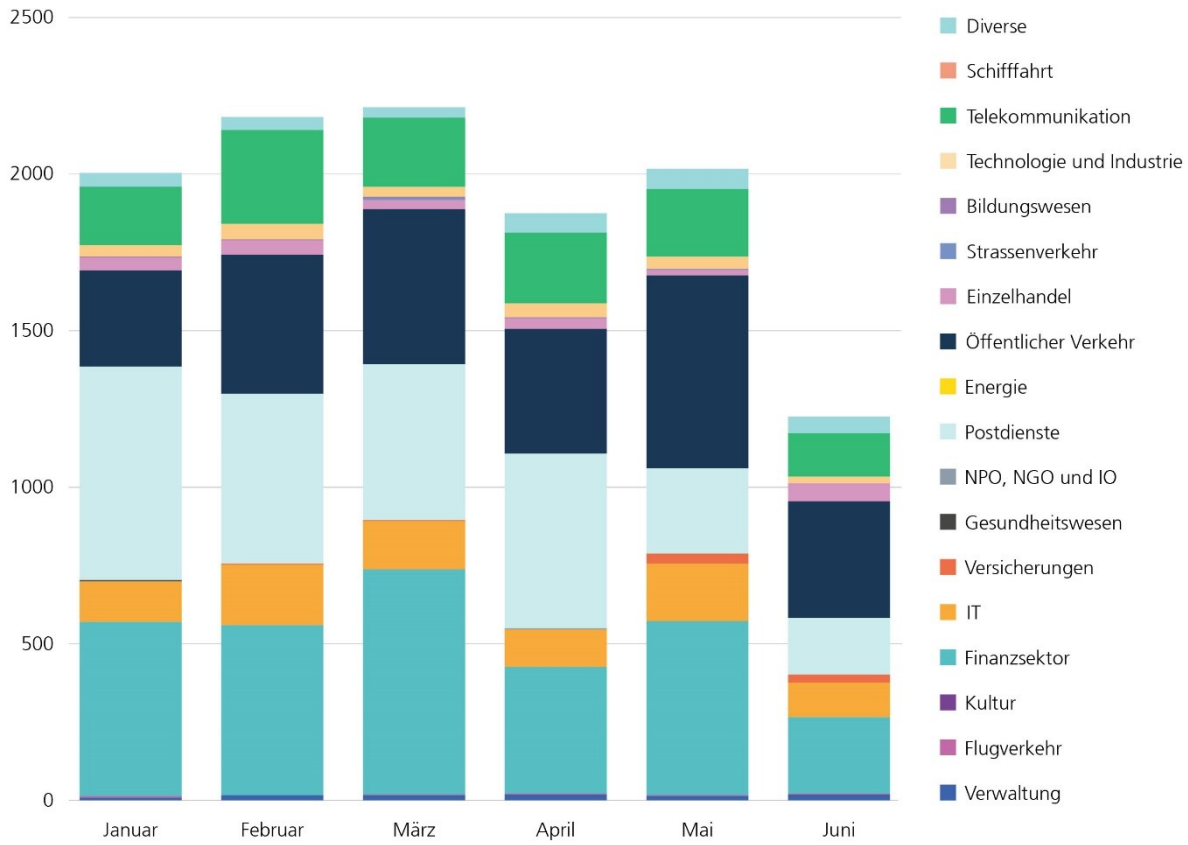

Abb. 4: Anzahl der durch das BACS überprüften und bestätigten Phishing-URLs im ersten Halbjahr 2024 nach Sektoren von missbrauchten Marken.

2.1 Chain Phishing etabliert sich

Phishing-Versuche gegen Microsoft-365-Konten werden dem BACS immer wieder gemeldet. In vielen Fällen wird dabei eine Vorgehensweise beobachtet, die einem Schneeballsystem ähnelt. Sobald ein Opfer auf einer Phishing-Webseite sein Passwort angegeben hat, hacken die Kriminellen das Konto und versenden die gleiche Phishing-E-Mail an alle Kontakte des gehackten Kontos. Fällt einer der Empfänger erneut auf den Phishing-Versuch herein, beginnt das Ganze von vorne. Dies führt innert kurzer Zeit zu einer Vielzahl von gehackten Konten, weshalb das Vorgehen auch als «Chain Phishing» bekannt ist. Das primäre Ziel solcher Phishing-Versuche ist jedoch nicht in allen Fällen klar, denn auf den ersten Blick ist kein direkter Schaden sichtbar. Da mit dem gehackten Konto alle Kontakte im Adressbuch angeschrieben werden, ist es wahrscheinlich, dass einer dieser Empfänger die Kompromittierung erkennt, das Opfer informiert und die Phishing-Kampagne gemeldet wird. Das Opfer kann nun umgehend die Passwörter zurückzusetzen und der Wert des gehackten Kontos scheint für die Kriminellen verloren. Dennoch kann dieses Vorgehen für die Angreifer lukrativ sein, wenn unmittelbar nach dem Hacken des Kontos automatisch alle E-Mails des Opfers von den Angreifern heruntergeladen werden. Diese werden dann nach brauchbarem Material durchsucht, welches für weitere gezielte Angriffe verwendet werden kann. So kommt es immer wieder zu gezielten E-Mail-Angriffen, die sich auf eine vorangegangene E-Mail-Korrespondenz beziehen. Es ist auch möglich, dass die Angreifer die erbeuteten E-Mail-Daten auf kriminellen Foren zum Verkauf anbieten (vgl. Kap. 7.2). Eine andere Möglichkeit ist die Einrichtung einer Weiterleitungsregel, so dass alle eingehenden E-Mails an die Betrüger weitergeleitet werden. Diese Regel bleibt auch bei einer Passwortänderung aktiv und wird häufig nicht entdeckt. Die Betrüger können so zu einem späteren Zeitpunkt über die Passwortrücksetzungsfunktion Zugriff auf weitere Konten – meist von sozialen Netzwerken – erhalten.

2.2 Der zweite Faktor rückt ins Visier

«Wenn immer möglich, aktivieren Sie in Zukunft die Multi-Faktor-Authentifizierung.» Dies ist ein Präventionstipp, den das BACS bei jedem gemeldeten Phishing-Vorfall gibt. Der Begriff Multi-Faktor-Authentifizierung (MFA) bezeichnet eine Authentifizierungsmethode, bei der die Anwenderin oder der Anwender zwei oder mehr Authentifizierungsfaktoren angeben muss, bevor er oder sie Zugriff auf die gewünschte Ressource erhält.[17] Typische Faktoren sind spezifisches Wissen (z. B. ein Passwort), der Besitz eines Gerätes (z. B. ein Smartphone oder ein Hardware-Token[18]) oder das Vorweisen von bestimmten körperlichen Merkmalen (z. B. biometrische Daten wie Fingerabdruck oder Gesichtserkennung).

Die Aktivierung von MFA erhöht die Sicherheit eines Kontos um ein Vielfaches. Dies bedeutet aber nicht, dass damit der Zugriff endgültig abgesichert ist. Auch nach der MFA-Aktivierung ist bedachtes Verhalten der Nutzerinnen und Nutzer im Netz erforderlich. Wenn Nutzerinnen und Nutzer auf gefälschte Anfragen, E-Mails oder Telefonanrufe reagieren und Angaben der zusätzlichen Faktoren preisgeben, kann auch MFA ausgehebelt werden. So beobachtete das BACS in der ersten Jahreshälfte 2024 zunehmend, dass verschiedene Phishing-Seiten nun

---

17 S-U-P-E-R.ch – Sichern Sie Ihre Zugänge doppelt (ncsc.admin.ch)

18 Ein «Token» umschreibt ein Sicherheitselement zur Authentifizierung einer Nutzerin oder eines Nutzers, vgl. Security-Token (wikipedia.org).

versuchen, in einem weiteren Schritt den zusätzlichen Sicherheitsfaktor – z. B. das Einmalpasswort – abzugreifen. Auch mittels betrügerischer Telefonanrufe wird versucht, den zusätzlichen Faktor auszuhebeln (vgl. Kap. 5). Wenn sich das Opfer in dessen Konto einloggt, haben die Angreifer simultan Zugriff auf dessen Computer und damit auch auf das Konto. Dies geschieht, indem die Kriminellen das Opfer überzeugen, eine Fernzugriffs-Software herunterzuladen. Mit dieser verfolgen sie die Handlungen des Opfers am Computer mit und können verdeckt Manipulationen am Computer vornehmen. Solche Fälle zeigen exemplarisch, dass der zusätzliche Faktor nicht generell vor ungewollten Zugriffen schützen kann. Er schränkt vor allem das Zeitfenster des Angreifers ein, indem dieser aktiv werden kann. Ist MFA implementiert, kann der Angreifer nur im unmittelbaren Moment auf das Konto zugreifen oder wenn das Opfer selbst eingeloggt ist. Ein späterer Zugriff ist nicht mehr möglich. Im Gegensatz dazu kann ein Angreifer ein Konto, das nur mit einem Passwort geschützt ist, so lange für seine Zwecke nutzen, bis das Passwort geändert wird.

Obwohl im Alltag auf eine Vielzahl digitaler Dienste zugegriffen wird – von E-Mail und Bankkonten bis hin zu sozialen Netzwerken – ist MFA für viele immer noch ein notwendiges Übel. Je häufiger Nutzerinnen und Nutzer aufgefordert werden, zusätzliche Authentifizierungsoptionen zu aktivieren, desto grösser wird bei einigen der Frust aufgrund des gefühlten Mehraufwands. Dies kann dazu führen, dass diese weniger vorsichtig werden und sinnvolle Sicherheitspraktiken vernachlässigen. Diese Entwicklung ist auch bekannt als «MFA-Fatigue». Die ständigen Aufforderungen, Authentifizierungs-Apps zu öffnen, SMS-Codes einzugeben oder Hardware-Token zu verwenden, können auf Dauer ermüdend sein. Hinzu kommt, dass manche MFA-Methoden unzuverlässig sein können.[19] Beispielsweise können SMS-Codes verspätet ankommen oder Authentifizierungs-Apps technische Probleme haben. Leider nutzen Betrüger MFA-Ermüdung mittlerweile für ihre kriminellen Interessen aus. Dabei bombardieren sie Kontoinhaber mit Verifizierungsanfragen, um Ermüdungseffekte auszulösen. Ziel ist es, die Betroffenen so lange zu stressen, bis sie die Anmeldung der Betrüger aus Frust oder in der Eile versehentlich bestätigen.

Empfehlungen

Aktivieren Sie **Multi-Faktor-Authentifizierung (MFA)** als zusätzliche Sicherheit Ihrer Konten, wo immer möglich. Obwohl MFA das Risiko für eine Kompromittierung enorm reduziert, kann MFA durch Social-Engineering[20]-Techniken ausgehebelt werden. Seien Sie deshalb wachsam vor gefälschten Anfragen – insbesondere via E-Mail und SMS, wenn Sie Zugriffe bestätigen oder Ihre Sicherheits-Token an jemand anderes weiterleiten sollen. Bedenken Sie auch, dass E-Mail-Absender und Telefonnummern leicht gefälscht werden können.

19 Siehe Zweiter Faktor SMS: Noch schlechter als sein Ruf (ccc.de)

20 Social Engineering (ncsc.admin.ch)

3 Schadsoftware

Das BACS erhielt im Vergleich zu anderen Quellen für Malware-Verteilung in der Schweiz[21] relativ wenig Meldungen (92) mit einem direkten Bezug zu Schadsoftware (Malware)[22]. Schadsoftware wird entwickelt, um mit Programmen unerwünschte und meist schädliche Funktionen auf IT-Systemen auszuführen. Dies geschieht dann in der Regel ohne das Wissen des Benutzers.[23] Dieser Umstand erklärt auch die eher niedrige Anzahl Meldungen – insbesondere bei Schadsoftware im Zusammenhang mit E-Mail-Versand – durch die Bevölkerung. Wer sich nicht bewusst ist, dass das System von einer Malware infiziert ist, wird auch nichts melden. Andererseits sind die Filtermethoden der Software-Hersteller mittlerweile auf einem so guten Stand, dass nur noch ein geringer Prozentsatz von E-Mails mit böswilligen Inhalten die Empfänger erreicht. Auch sind die Sicherheitsvorkehrungen auf den Endgeräten in den letzten Jahren so stark verbessert worden, dass mehrere Benutzerinteraktionen notwendig sind und mehrfach gewarnt wird, bevor eine schädliche Datei installiert werden kann. Es ist davon auszugehen, dass Angreifer sich auf neue Wege fokussieren, um Schadsoftware auf Geräten zu installieren. Beispielsweise werden entsprechende Schadprogramme in Freeware, Plugins oder Applikationen versteckt, die für den Nutzer weniger transparent sind und daher auch zu weniger Meldungen führen. Gleichwohl wurde während des Berichtszeitraums mit «Poseidon Stealer» eine grosse Malware-Welle beobachtet, die auf MacOS-Benutzende abzielte (vgl. Kap. 3.1). Ende Juni 2024 erhielten viele Schweizerinnen und Schweizer eine E-Mail mit dem Betreff «Ab Juli 2024 wird der AGOV-Zugang für alle öffentlichen Online-Dienste obligatorisch».[24] Die E-Mail forderte die Empfänger zur Installation einer Software auf, da nur damit ein vermeintlich nahtloser Zugang zur öffentlichen Verwaltung gewährleistet sei. Ähnlich wie Phishing hängt das erfolgreiche Verteilen von Schadsoftware häufig vom Faktor Mensch ab. Je glaubhafter der Vorwand erscheint, desto grösser sind die Erfolgschancen für die Bedrohungsakteure, dass sie ihre Malware breit verteilen können.

3.1 Initialer Zugang mit Schadsoftware

Um sich einen ersten Zugang zu einem IT-System zu verschaffen, greifen Cyberkriminelle häufig auf Schadsoftware wie z. B. Trojaner zurück. Diese erfordern in der Regel eine Aktion des Benutzers, wobei auf verschiedene Täuschungsmechanismen zurückgegriffen wird. Beispielsweise kann die Schadsoftware in einem anderen Programm oder in einem per E-Mail erhaltenen Anhang oder Link versteckt sein, der für einen unaufmerksamen Benutzer harmlos erscheint. Viele der international beobachteten Schadsoftwares werden auch in der Schweiz beobachtet, darunter «AgentTesla», «DarkGate», «FakeUpdates», «Formbook», «Gootloader», «GuLoader», «PikaBot» oder auch «Poseidon Stealer»[25]. Im Folgenden werden die beiden Letzteren näher erläutert, da sie die Verbreitungsmethoden und Einflussfaktoren auf die erzielte Wirkung in der Schweiz exemplarisch aufzeigen.

---

21 Siehe Statistics (abuse.ch)

22 Schadsoftware (ncsc.admin.ch)

23 BSI - Malware (bsi.bund.de)

24 Cyberkriminelle verbreiten im Namen von AGOV Schadsoftware für macOS (ncsc.admin.ch)

25 Technische Kurzanalyse zur Schadsoftware «Poseidon Stealer» (ncsc.admin.ch)

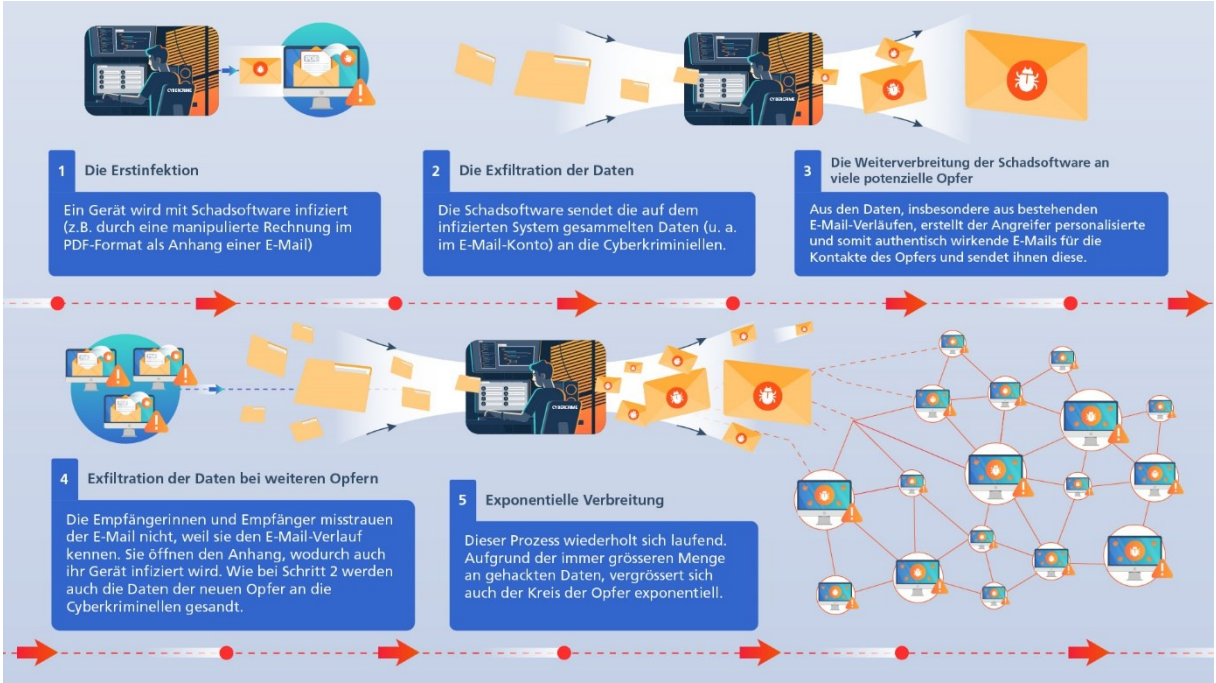

Abb. 5: Kapern von E-Mail-Konversationen für die Verbreitung von Schadsoftware

Anfang Jahr wurden Fälle beobachtet, in denen versucht wurde, die Schadsoftware «PikaBot» durch das Kapern von E-Mail-Konversationen (engl. e-mail thread hijacking) zu verbreiten. Die Kriminellen nutzten dabei alte, zuvor aus den Postfächern anderer Opfer gestohlene E-Mail-Korrespondenzen (vgl. Kap. 2.1), um das Opfer zu täuschen (vgl. Abb. 5).

Beim angefügten Dokument handelte es sich z. B. um eine Excel-Datei, die die Nutzerin oder den Nutzer darauf hinweist, dass bestimmte Dateien online zu finden seien und zum Anzeigen dieser Dateien auf eine Schaltfläche in dieser Datei geklickt werden müsse.[26] Hinter dieser Schaltfläche verbirgt sich aber ein Skript, welches zu einer PikaBot-Infektion führt. Eine PikaBot-Infektion kann zu beträchtlichen Folgen führen, insbesondere da diese Schadsoftware in Verbindung mit Ransomware-Gruppen vermehrt zum Einsatz seit dem zweiten Halbjahr 2023 kam.[27] Um dem entgegen zu treten, gelang es im Rahmen der internationalen Zusammenarbeit den Strafverfolgungsbehörden mit der Operation «Endgame» im Mai 2024, die Infrastruktur mehrerer krimineller Dienstleister von Erstzugängen und Schadsoftware (Malware-as-a-Service) zu stören.[28] Dieser Schlag richtete sich ebenfalls gegen PikaBot-Infrastruktur. Kurzfristig ist zwar anzunehmen, dass die Operation die Aktivitäten dieser Bedrohungen in der Schweiz reduziert. Langfristig hingegen halten diese Effekte nur selten an, da die Urheber solcher Schadsoftware – sofern sie nicht verhaftet wurden – ihre Infrastruktur neu aufbauen und Kriminelle, die diese Dienste nutzen, sich rasch anderen Anbietern zuwenden.

26 TA577 introduced a rather interesting new approach to distribute their Pikabot malware (x.com)

27 The Emerging Threat of PikaBot Malware (flashpoint.io)

28 Largest ever operation against botnets hits dropper malware ecosystem (europol.europa.eu)

Ende Juni 2024 kommunizierte das BACS, dass eine Malspam-Kampagne[29] mit «Poseidon Stealer» auf MacOS-Nutzerinnen und -Nutzer in der Schweiz abzielte, indem AGOV als Täuschung verwendet wurde.[30] Der Link in der E-Mail leitete auf eine Website weiter, die die Empfänger dazu aufforderte, eine .dmg-Datei herunterzuladen. Diese gab vor, eine Desktop-Anwendung von AGOV zu sein. In Wirklichkeit handelte es sich bei dem angebotenen Programm jedoch um die Schadsoftware Poseidon Stealer. Sobald die Schadsoftware ausgeführt war, stahl sie Informationen vom Computer des Opfers und leitete sie an die Cyberkriminellen weiter. Interessanterweise deckte sich die Kampagne in der Schweiz mit einer anderen im Ausland. Einige Tage zuvor wurde eine internationale Verteilungskampagne mit derselben Schadsoftware beobachtet, bei der die Verteilmethode des «Malvertising»[31] in Verbindung mit dem Internetbrowser «Arc» eingesetzt wurde.[32] Dieser Angriff zielte primär auf Internetnutzer, die über eine Suchmaschine nach der Software Arc suchten, um sie zu einem Klick auf das «gesponserte» Ergebnis der Kriminellen anstelle des legitimen Links für die Produktinstallation zu verleiten.

Empfehlungen

Klicken Sie in verdächtigen E-Mails nicht auf Links und öffnen Sie keine angefügten Dateien. Fragen Sie im Zweifelsfall beim vermeintlichen Absender über andere Kanäle nach, ob die E-Mail 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 Webseite als bezahlte Werbung deklariert ist oder nicht.

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.

29 Was ist Spam? Seine Arten und wie Sie sich schützen (avast.com)

30 Cyberkriminelle verbreiten im Namen von AGOV Schadsoftware für macOS (ncsc.admin.ch)

31 «Malvertising» beschreibt die Technik von Bedrohungsakteuren, wenn sie als Verteilmethodik Online-Werbung als böswillige Aktivitäten nutzen, vgl. NCSC For Startups: taking on malvertising (ncsc.gov.uk).

32 'Poseidon' Mac stealer distributed via Google ads (malwarebytes.com)

3.2 Ransomware

Ransomware-Angriffe[33] sind immer wieder Thema der Schlagzeilen, aber auch von Untersuchungen.[34] 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. In der Regel exfiltrieren die Kriminellen zugleich die Daten. Im Anschluss fordern sie vom Opfer ein Lösegeld für ein Entschlüsselungstool (Dekryptor) und für die Nicht-Veröffentlichung oder den Nicht-Weiterverkauf der gestohlenen Daten. Die Erfahrung zeigt, dass das Schadensausmass variiert. Während die Angriffe bei einigen Opfern dank vorhandener Cyberhygiene kaum zu Schäden führt, können bei anderen Opfern existenzbedrohende Auswirkungen resultieren.[35] Neben den Wiederherstellungskosten müssen Unternehmen mehrere Tage oder Wochen mit eingeschränkten oder komplett ausgefallenen IT-Diensten auskommen. Zudem besteht beispielsweise die Gefahr eines Reputationsschadens nach der Publikation der Daten.

3.2.1 Ransomware-Aktivitäten in der Schweiz

Der Meldeeingang beim BACS bezüglich Ransomware-Angriffe auf Unternehmen ist leicht rückläufig. Im ersten Halbjahr des Jahres 2024 gingen beim BACS 39 Meldungen zu Ransomware ein. Im Vergleichszeitraum des Vorjahres verzeichnete das BACS noch 56 Ransomware-Angriffe. Bei Privatpersonen setzt sich der bisherige Trend fort, dass sie immer weniger im Fokus der Cyberkriminellen stehen. Während aktuell nur fünf Meldungen von Privatpersonen stammten, waren es in der Vorjahresperiode noch acht. Eine bessere Sensibilisierung der Nutzerinnen und Nutzer und die Einrichtung von (Offline-)Backups könnten zu diesem Rückgang beigetragen haben. Auch ist es möglich, dass mehr gezielte Angriffe auf sehr lukrative Opfer einen Einfluss hatten. Wenn die Zielsetzung ist, möglichst hohen Druck zur Zahlung des Lösegelds zu erzeugen, können Kriminelle bei dem so entstehenden Mehraufwand mit den gleichen Ressourcen tendenziell weniger Ziele angreifen. Opfer, die nicht als interessant eingeschätzt werden, aber bei denen sich die Angreifer trotzdem z. B. Zugang zu den Systemen verschafft haben, können sie mit dem Verkauf der Informationen auf Schwarzmärkten zusätzlich monetarisieren (vgl. Kap. 3.2).

Die drei Ransomware-Gruppen «Akira», «8Base» und «Black Basta» verantworten im Berichtszeitraum mehrere Angriffe gegen Schweizer Unternehmen. Augenfällig war dabei der

---

33 Ransomware (ncsc.admin.ch)

34 Vgl. Kolumne der Neue Zürcher Zeitung (NZZ) zum Play-Ransomware-Vorfall im Jahr 2023: Kriminelle Hacker greifen die NZZ an: das Protokoll der Krise (nzz.ch),
Interview mit Geschäftsführer der Xplain AG zum Play-Ransomware-Vorfall im Jahr 2023: Xplain-CEO: «Es war nicht vorgesehen, dass wir produktive Daten bei uns haben» (inside-it.ch),
Bericht des BACS zur Datenanalyse im Kontext des Play-Ransomware-Vorfalls der Xplain AG im Jahr 2023: Hackerangriff auf Firma Xplain: Bericht des Bundesamtes für Cybersicherheit zur Datenanalyse publiziert (ncsc.admin.ch)
Abschlussbericht der Administrativuntersuchung zum Play-Ransomware-Vorfall im Jahr 2023: Abschluss der Administrativuntersuchung zum Hackerangriff auf die Xplain AG: Bundesrat beschliesst Massnahmen (admin.ch)
Untersuchungsbericht des Schweizer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) zum Play-Ransomware-Vorfall im Jahr 2023: EDÖB schliesst Untersuchungen gegen das Unternehmen Xplain und die Bundesämter fedpol und BAZG ab (edoeb.admin.ch)

35 Siehe u. a. Akumin Inc., CloudNordic, KNP Logistics, MediSecure, Travelex, United Structures

relativ hohe Meldeeingang von neun Ransomware-Infektionen mit «Akira» bei Schweizer Unternehmen, wobei allein im März drei Meldungen erfolgten. Die Ransomware-Gruppe charakterisiert sich durch ein opportunistisches Angriffsverhalten wegen der verhältnismässig hohen Anzahl Opfer, die verschiedene Sektoren und Grössen von Unternehmen miteinbeziehen. Obwohl die Gruppe erst seit März 2023 aktiv ist, hatte sie bis Anfang 2024 in Europa, Nordamerika und Australien bereits schätzungsweise 250 Organisationen angegriffen.[36] Akira zeigt dabei Innovation in ihrem Vorgehen: Die Gruppierung nutzt beispielsweise gemäss dem finnischen NCSC eine CISCO-VPN-Schwachstelle aus, um NAS-Systeme (Netzwerkspeicher) und Backups von Backups systematisch zu verschlüsseln.[37]

Im Gegensatz zu Akira war der Meldeeingang für die 8Base-Ransomware mit drei Meldungen etwas tiefer. In der Schweiz wurde 8Base bekannt, nachdem es der Gruppe im November 2023 gelang, das Schweizer IT-Unternehmen Concevis AG zu kompromittieren.[38] 8Base nutzt die Datenverschlüsselung in Verbindung mit «Name-and-shame»-Erpressertechniken, um Opfer verschiedener Branchen zur Zahlung von Lösegeld zu nötigen.[39] Muster dieser Ransomware zeigen, dass sie eine adaptierte Version der Ransomware «Phobos v2.9.1»[40] verwendet, die über die Schadsoftware «SmokeLoader» geladen wird.[41] Zwei der Schweizer Opfer wurden ebenfalls öffentlich diskutiert, da gestohlene Daten auf der Datenleckseite der Gruppe publiziert wurden. Einerseits betraf dies das Telekomunternehmen Nexus Telecom Switzerland AG.[42] Die Auswirkungen der 23 Gigabyte (GB) an veröffentlichen Daten waren begrenzt, da vor allem Archivdaten abgeflossen sind und das Unternehmen keine Schweizer Kunden hatte. Andererseits griff 8Base die Firma Mikrona an, einen Zulieferer für Kieferorthopäden, Zahnärzte und Zahntechniker. Nach Angaben von Mikrona gab es keine Unterbrechung der Produktion durch den Vorfall. Da Sicherheitskopien vorhanden waren, konnten betroffene operative Systeme innerhalb von wenigen Tagen wieder komplett funktionsfähig gemacht werden. Trotz Mikronas schnellem Handeln muss davon ausgegangen werden, dass Daten kompromittiert wurden.[43]

Die Ransomware-Gruppe Black Basta[44] fiel besonders von Februar bis April 2024 mit Operationen in der Schweiz auf: Gleich drei grössere Schweizer Unternehmen – darunter ein Zulieferer u. a. für kritische Infrastrukturen – wurden Opfer der Kriminellen. Black Basta listete das Personalunternehmen Das Team AG und den Spielwarenhändler Franz Carl Weber auf ihrer Datenleckseite im Februar und März 2024 auf. Nachdem offenbar beide Unternehmen nicht gewillt waren, sich erpressen zu lassen, wurden deren – teilweise sensitiven – Daten publiziert.[45] Anders als z. B. Akira oder 8Base wendet Black Basta häufig ein selektiveres Verfahren

---

36 #StopRansomware: Akira Ransomware (cisa.gov)

37 Finland warns of Akira ransomware wiping NAS and tape backup devices (bleepingcomputer.com)

38 Hackerangriff auf die Firma Concevis: Auch die Bundesverwaltung ist betroffen (ncsc.admin.ch)

39 Ransomware Spotlight: 8Base (trendmicro.com)

40 #StopRansomware: Phobos Ransomware (cisa.gov)

41 8Base (sentinelone.com)

42 Daten von Nexus Telecom im Darkweb veröffentlicht (inside-it.ch)

43 Cyberangriff auf Schweizer Medtech-Firma (inside-it.ch)

44 #StopRansomware: Black Basta (cisa.gov)

45 Haufenweise Kundendaten von Schweizer Personalvermittler gestohlen (inside-it.ch), Cyberkriminelle stehlen schützenswerte Daten von Franz Carl Weber (inside-it.ch)

bei seiner Zielauswahl an. Black Basta Ransomware kompromittiert immer wieder hochkarätige Unternehmen und Organisationen, bei denen hohe Lösegeldforderungen gestellt werden können. Dies zeigte sich auch beim Angriff im April 2024 auf ein drittes Opfer, die swisspro Gruppe.[46] Black Basta bekannte sich zum Angriff und veröffentlichte nach eigenen Angaben 700 GB an Daten, nachdem swisspro nicht auf die Erpressung eingegangen war und die Zahlung verweigerte hatte. Da der Angriff auf eine alte IT-Infrastruktur erfolgte, blieben die negativen Konsequenzen gering und swisspro konnte ihre Dienstleistungen jederzeit erbringen.[47]

3.2.2 Ransomware als globale Herausforderung

Auch kritische Infrastrukturen stehen immer wieder im Fokus von Ransomware-Gruppierungen. Ihre hohe Relevanz für das tägliche Leben einer Gesellschaft und das Risiko bei Systemausfällen, Kaskadeneffekte auf andere kritische Funktionalitäten hervorzurufen, erhöht den Druck für eine schnelle Lösung zusätzlich. Diese Beobachtung machte auch das Federal Bureau of Investigation (FBI), wobei es eine generelle Zunahme von Ransomware-Angriffen auf kritische Infrastrukturen feststellte.[48] Während einige Gruppen behaupten, gewissen ethischen Standards bei ihrer Opferauswahl zu folgen, greift die Mehrheit der Gruppen bewusst kritische Infrastrukturen an, um die Zahlungsbereitschaft bei den Opfern maximal abzuschöpfen. So waren beispielsweise in der Wasserversorgung und -entsorgung tätige Unternehmen Veolia North America[49] sowie Southern Water[50] von Ransomware-Angriffen betroffen. Ebenso wurde ein deutscher Software-Entwickler für Kontrollsysteme von kritischen Infrastrukturen Opfer eines Verschlüsselungsangriffs.[51] Abgesehen davon war auch der Gesundheitssektor ein beliebtes Ziel für Kriminelle. Die US-Behörden warnten spezifisch den amerikanischen Gesundheitssektor vor Phobos und Akira Ransomware-Aktivitäten (vgl. Kap. 3.2.1).[52]

Ein aufsehenerregender und disruptiver Fall betraf Anfang Juni 2024 mehrere Londoner Krankenhäuser, nachdem Synnovis – einer ihrer Dienstleister – Opfer eines «Qilin» Ransomware-Angriffs wurde. Aufgrund des Cyberangriffs und den resultierenden IT-Systemausfällen mussten die Spitäler rund 6'000 Termine wie Operationen und Bluttransfusionsverfahren innerhalb der nächsten fünf Wochen verschieben.[53] Der Notfallbetrieb blieb aber jederzeit operativ. Die Ransomware-Gruppe publizierte wenige Wochen später 400 GB an sensitiven Gesundheitsdaten.[54] In einem späteren Interview erklärten die Kriminellen, dass sie sich den Konsequenzen ihres Handelns bewusst seien und nichts bereuen.[55]

---

46 Basta bekennt sich zum Angriff auf BKW-Tochter Swisspro (inside-it.ch)

47 Russischer Hackerangriff: Attacke auf Schweizer Stromkonzern wirft Fragen auf (bernerzeitung.ch)

48 Federal Bureau of Investigation: Internet Crime Report 2023 (ic3.gov)

49 Veolia Responds to Cyber Incident (mywater.veolia.us)

50 Black Basta claims hack on Southern Water (computing.co.uk)

51 Critical infrastructure software maker confirms ransomware attack (bleepingcomputer.com)

52 Siehe CISA, FBI, and MS-ISAC Release Advisory on Phobos Ransomware (cisa.gov), Feds Warn Health Sector About Akira Again, Amid New Attacks (bankinfosecurity.com)

53 NHS Trusts cancelled over 6,000 appointments after Qilin cyber attack (computerweekly.com), Cyber-attack on London hospitals declared critical incident (bbc.com)

54 NHS England confirm patient data stolen in cyber attack (bbc.com)

55 Qilin has 'no regrets' over the healthcare crisis it caused (theregister.com)

Als Antwort auf die wachsende, globale Bedrohung durch Ransomware-Aktivitäten führten verschiedene Strafverfolgungsbehörden mehrere mitigierende Massnahmen aus. Erwähnenswert ist insbesondere «Operation Cronos» Mitte Februar 2024. Unter der Führung der britischen National Crime Agency (NCA) führten Polizeibehörden ein Störmanöver gegen die damals noch einflussreiche Ransomware-Gruppe «LockBit» aus.[56] LockBit war z. B. im Jahr 2023 für rund 25 bis 33 % aller Ransomware-Angriffe weltweit verantwortlich.[57] Nebst der Verhaftung einiger Gruppenmitglieder[58] und der Beschlagnahmung von Kryptogeld, entwickelten die beteiligten Strafverfolgungsbehörden einen Dekryptor, mit dem Opfer ihre verschlüsselten Dateien kostenlos wiederherstellen konnten. Der zentralste Aspekt der Operation betraf die Übernahme der Server der Cyberkriminellen und die Beschlagnahmung ihrer Datenleckseite. Letztere wurde dann sogleich von der Polizei als Kommunikationsplattform genutzt, um Updates über den Fall – wie z. B. die Identität eines Administrators von LockBit[59] – zu veröffentlichen.[60] Durch die Polizeiaktion verlor die Führung von LockBit das Vertrauen vieler ihrer Partner (engl. Affiliate),[61] wodurch LockBit zu einem Schatten seiner selbst wurde. Trotzdem wurden auch nach «Operation Cronos» immer noch Fälle von LockBit-Infektionen verzeichnet. Auch das BACS erhielt drei Meldungen von Schweizer Opfern, welche alle nach der internationalen Operation erfolgten.

Die Cyberbedrohungslandschaft ist auch bei Ransomware-Gruppen dynamisch und untersteht regelmässigen Veränderungen. Dies zeigt sich einerseits anhand der LockBit-Gruppe, die durch eine gezielte Operation der Strafverfolgung de facto in die Irrelevanz verbannt wurde. Andererseits wählen Gruppen immer wieder freiwillig den Ausstieg, wenn sich für sie ein Ausstiegsbetrug (Exit-Scam) oder eine Neuausrichtung mehr lohnt als die Fortsetzung der Aktivität. Für ein solches Vorgehen entschied sich im ersten Halbjahr 2024 die Ransomware-Gruppe «BlackCat» – auch bekannt als «ALPHV». Nachdem BlackCat im Dezember 2023 im Visier einer Strafverfolgungsoperation war,[62] behielten die Administratoren das gezahlte Lösegeld von 22 Millionen US-Dollar im März 2024 komplett für sich und zahlten dem Partner seinen Anteil nicht aus.[63] Dies bedeutet dann auch das endgültige, endogene Ende dieser Ransomware-Aktivität. Andere Ransomware-Gruppen wie Black Basta, Akira, Hunters International oder BianLian profitierten von der Lücke und konnten danach das Volumen ihrer Aktivitäten erhöhen. Es ist anzunehmen, dass viele der Partner von BlackCat sich auf andere Gruppen umorientierten. Weiter ist zu erwarten, dass destabilisierte Ransomware-Gruppen sich neu erfinden, um wieder unter neuem Namen aktiv zu werden. Es ist zudem möglich, dass grosse Ransomware-Gruppen nach und nach verschwinden und stattdessen viele kleinere Gruppen entstehen werden. Entwickler von Ransomware könnten dadurch abwechselnd oder sogar gleichzeitig für mehrere Ransomware-Operationen arbeiten.

---

56 The NCA announces the disruption of LockBit with Operation Cronos (nationalcrimeagency.gov.uk)
57 Auswirkungen der Operation Cronos auf LockBit (trendmicro.com)
58 LockBit administrator sentenced to almost four years in prison after guilty plea (therecord.media)
59 LockBit leader unmasked and sanctioned (nationalcrimeagency.gov.uk)
60 Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption (trendmicro.com)
61 Ransomware Talent Surges to Akira After LockBit's Demise (bankinfosecurity.com)
62 Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant (justice.gov)
63 BlackCat ransomware turns off servers amid claim they stole $22 million ransom (bleepingcomputer.com)

Empfehlungen

Erstellen Sie regelmässig Sicherungskopien Ihrer Daten (auch) auf einem externen Medium.[64] Folgen Sie dabei für sehr wichtige Daten der altbekannten **3-2-1 Regel**: Halten Sie mindestens drei Sicherheitskopien in zwei verschiedenen Lokalitäten, wobei mindestens eine davon komplett offline gelagert werden sollte.[65] Modernere Backup-Strategien basieren zwar auf dieser Regel, aber verbessern die Dimensionen Redundanz, Zugriff und geografische Entfernung. Dies integriert u. a. Cloud-Anbieter, die entsprechende Cloud-Dienstleistungen anbieten.[66]

Auf der Website des BACS finden Sie eine Auflistung von weiteren präventiven Massnahmen zum Schutz vor Ransomware sowie auch Handlungsanweisungen für den Ereignisfall. Generell rät das BACS den Opfern von Ransomware ab, Lösegeld zu zahlen. Es besteht keine Garantie, dass Cyberkriminelle ihr Wort halten. Mit einer Lösegeldzahlung steigt vor allem die Attraktivität für weitere Ransomware-Operationen.

3.3 Schadsoftware auf Mobilgeräten

Seit einigen Jahren sind Mobilgeräte – Smartphones und Tablets – zu alltäglichen Begleitern geworden. Tragbar, leistungsstark und ständig verbunden enthalten sie immer mehr persönliche Daten wie Fotos, Kontakte und E-Mails sowie Anwendungen mit sensitiven Inhalten. Dies kann z. B. E-Banking- und MFA-Software sein. Um diese Funktionalitäten zu ermöglichen, verwenden die meisten Mobilgeräte die Betriebssysteme Android oder iOS. Aus diesen Gründen gibt es eine eigene Kategorie von Schadsoftware, die auf Betriebssysteme von Mobilgeräten abzielt, sogenannte «Mobile Malware». Im Berichtszeitraum wurden in diesem Bereich verschiedene Vorfälle und Entwicklungen beobachtet, wobei keine davon einen exklusiven Bezug zur Schweiz hatte.

In Finnland warnte die Agentur Traficom im Mai 2024 vor einer Kampagne zur Verbreitung von Schadsoftware, die auf die Online-Banking-Konten von Android-Nutzern abzielte.[67] Betrügerische SMS verleiteten die Opfer dazu, eine gefälschte Antivirenanwendung zu installieren. Um die Empfänger zu täuschen, kündigte die SMS eine verdächtige Bankaktivität oder eine Inkassoforderung an und gab vor, von Banken oder Zahlungsdiensten zu stammen. Die Angreifer verschickten SMS in Finnisch und nutzten Spoofing[68], um den Anschein zu erwecken, dass sie von lokalen Telekommunikationsanbietern stammten. Zusätzlich forderten sie die Empfänger auf, eine Nummer anzurufen. Bei dem Anruf wurden die Opfer dazu gebracht, eine gefälschte Antivirenanwendung ausserhalb des offiziellen App-Stores zu installieren. Bei dieser

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

65 O. Hönö zit. in Finland warns of Akira ransomware wiping NAS and tape backup devices (bleepingcomputer.com)

66 What's the Diff: 3-2-1 vs. 3-2-1-1-0 vs. 4-3-2 (backblaze.com)

67 The National Cyber Security Centre Finland's weekly review – 18/2024 (kyberturvallisuuskeskus.fi)

68 Spoofing (ncsc.admin.ch)

handelte es sich in Wirklichkeit um die Mobilgeräte-Schadsoftware «Vultur».[69] Einmal installiert, ermöglicht die Schadsoftware u. a. den Zugriff auf Anwendungen auf dem infizierten Telefon. Darunter waren auch E-Banking-Anwendungen. Diese ermöglichte es den Kriminellen, die Bankkonten der Opfer zu leeren.

Neben Vultur gibt es noch eine Vielzahl anderer Schadsoftwares, die auf Betriebssysteme von Mobilgeräten abzielen und ständig weiterentwickelt werden. Beispielsweise analysierten Sicherheitsforscher im April 2024 eine neue Mobilgeräte-Schadsoftware mit dem Namen «Brokewell». Diese Schadsoftware zielt auf Android-Betriebssysteme und ab, indem sie als Update für Google Chrome getarnt von einer Internetseite ausserhalb des offiziellen App-Stores heruntergeladen wird. Nach der Installation ermöglicht sie Cyberkriminellen das Stehlen sensitiver Informationen, indem sie gefälschte Anmeldefenster über E-Banking-Apps legen und so die Zugangsdaten der Nutzerinnen und Nutzer abgreifen. Darüber hinaus kann Brokewell weitere Interaktionen der Nutzerinnen und Nutzer mit deren Geräten aufzeichnen, wie z. B. Tastatureingaben und Gespräche über das Mikrofon. Sie ist zudem in der Lage, Daten wie den geografischen Standort, den Anrufverlauf und technische Details des Geräts zu sammeln und weiterzugeben.[70]

Auch iOS-Nutzerinnen und -Nutzer bleiben von dieser Bedrohungsart nicht verschont. Im Februar 2024 entdeckten Sicherheitsforscher eine Schadsoftware mit dem Namen «GoldPickaxe.iOS», die speziell auf das Betriebssystem iOS abzielte. Diese Schadsoftware kann u. a. Gesichtserkennungsdaten und Identitätsdokumente sammeln sowie SMS abfangen. Gemäss dem Bericht hatten Kriminelle die gestohlenen biometrischen Daten verwendet, um ein Deepfake[71] zu erstellen. In Kombination mit gestohlenen Identitätsdokumenten und der Möglichkeit, Telefonanrufe und SMS abzufangen, ermöglichte es diesen, auf die Bankkonten ihrer Opfer zuzugreifen. So können sie Transaktionen mit hohen Geldbeträgen bestätigen, bei denen die Gesichtserkennung eingesetzt wird. Die Entwickler von GoldPickaxe.iOS nutzten Social-Engineering-Techniken[72], um ihre Opfer zur Installation der Mobilgeräte-Schadsoftware zu verleiten. Dabei kamen zwei Kanäle zur Verteilung zum Einsatz: Zunächst streuten sie die Schadsoftware über die TestFlight-Plattform von Apple, auf der Nutzerinnen und Nutzer Apps vor der offiziellen Veröffentlichung testen können. Als die Schadsoftware von der TestFlight-Plattform entfernt wurde, änderten die Kriminellen die Methodik, indem ein Profil für die Verwaltung von Mobilgeräten (MDM)[73] über eine bösartige Website installiert wird. Nach der Installation durch das Opfer ermöglichte das Profil den Kriminellen die vollständige Kontrolle über das Gerät, so dass sie die Schadsoftware hinzufügen können.[74]

Empfehlung

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

69 Android Malware Vultur Expands Its Wingspan (fox-it.com)
70 Brokewell: do not go broke from new banking malware! (threatfabric.com)
71 Deepfake (wikipedia.org)
72 Social Engineering (ncsc.admin.ch)
73 Mobile-Device-Management (wikipedia.org)
74 Face Off: Group-IB identified iOS trojan stealing facial recognition data (group-ib.com)

4 Schwachstellen

Wer das Geschehen um publizierte Beiträge und Warnungen rund um Schwachstellen aktiv verfolgt, könnte den Eindruck erhalten, dass Produkte prominenter Software-Hersteller – wie beispielsweise Cisco, Citrix, Fortinet, Ivanti und VMware – auffällig oft von Schwachstellen betroffen zu sein scheinen. Etliche Male pro Jahr stehen sie in der Fachpresse, weil schwerwiegende Sicherheitslücken gefunden werden. Ein Beispiel hierbei war eine Sicherheitslücke in der Firewall-Lösung des Software-Herstellers Palo Alto, die im April 2024 bekannt wurde. Die Schwachstelle ermöglichte es Angreifern, bei verwundbaren Geräten aus der Ferne Code auszuführen, was zur Kompromittierung der Systeme ausgenutzt werden konnte.[75]

Abgesehen von dieser Schwachstelle hat das BACS in der aktuellen Berichtsperiode die Betreiber kritischer Infrastrukturen gleich mehrfach vor verschiedenen Schwachstellen in Produkten gewarnt. In 85 % der Fälle, in denen das BACS Meldungen bezüglich Sicherheitslücken in Produkten erstellte, betraf es einen global agierenden Hersteller. Nur gerade 15 % der getätigten Schwachstellenwarnungen handelten mit einer wesentlich kleineren Anzahl an Warnungen von Sicherheitslücken in Anwendungen von weniger bekannten – und damit in der Schweiz auch viel weniger weit verbreiteten – Lieferanten. Generell ist aber festzuhalten, dass Schweizer Unternehmen sich grundsätzlich mit denselben Schwachstellen auseinandersetzen und sicherstellen müssen, dass diese behoben werden, wie ihre internationalen Mitbewerber. Gründe, weshalb Schwachstellen bei Produkten solcher namhaften Lieferanten regelmässig – und teilweise mit sehr hoher Kritikalität – immer wieder publiziert werden, sind im Folgenden beschrieben.

Zum einen sind umfangreiche Software-Produkte grundsätzlich sehr komplex. Sie enthalten zahlreiche Funktionen und Abhängigkeiten im Code und innerhalb der Software, aber auch ausserhalb wie mit dem Betriebssystem. Diese Komplexität kann zu Fehlern im Code führen, die schwer zu erkennen und zu beheben sind. Jede neue Funktion oder Integration kann, zunächst unbemerkt, neue Schwachstellen einführen. Hinzu kommt, dass grosse Software-Anbieter ihre Produkte stetig weiterentwickeln müssen, um auf dem Markt konkurrenzfähig zu bleiben. Die kontinuierliche Weiterentwicklung ist häufig auch gepaart mit dem Druck, neue Produkte und Updates rasch zur Marktreife zu bringen. Dieser Umstand kann ebenfalls dazu führen, dass Schwachstellen im Rahmen des Entwicklungsprozesses vorerst unentdeckt bleiben. Zum anderen wird kommerziell weit verbreitete Software von einer sehr grossen Anzahl von Benutzern eingesetzt. Das macht sie grundsätzlich zu einem attraktiven Ziel für Cyberkriminelle. Ein erfolgreicher Angriff auf eine populäre Software kann potenziell Millionen von Geräten und Benutzern treffen, was das Schadenspotenzial eines Angriffs erheblich erhöht. Diese und weitere Faktoren tragen massgeblich dazu bei, dass die Namen grosser und namhafter Software-Anbieter im Kontext des Schwachstellenmanagements häufig fallen und scheinbar unablässig neue Schwachstellen für deren Produkte bekannt werden.

---

75 CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect (paloaltonetworks.com), Kritische Sicherheitslücke in Firewalls von Palo Alto (ncsc.admin.ch)

Schlussfolgerung / Empfehlungen

Für weit verbreitete und vielfach genutzte Software ist die Wahrscheinlichkeit erheblich höher, dass in regelmässigen Abständen neue Schwachstellen gefunden werden. Dies ist u. a. auf die grosse Nutzerbasis und die Komplexität der Software zurückzuführen.

Hersteller von kommerziell weit verbreiteter Software müssen deshalb ihrerseits eine starke Sicherheitskultur pflegen und Verantwortung für die Sicherheit ihrer Produkte übernehmen. Diverse Massnahmen seitens Software-Lieferanten tragen dazu bei, dass ein möglichst sicheres Produkt zur Verfügung gestellt werden kann. Dies integriert z. B. die Durchführung von Sicherheitstests, die Implementierung von Best Practices für die sichere Entwicklung und insbesondere auch eine rasche und effiziente Reaktion nach neu entdeckten Schwachstellen.

Wenn Sie Software von globalen und renommierten Anbietern einsetzen, bedeutet dies nicht zwingend, dass diese sicherer in der Anwendung und im Betrieb als ein weniger bekanntes Produkt sind. Auch Software-Produkte von namhaften Herstellern weisen Sicherheitslücken auf.

Kürzlich geschlossene Sicherheitslücken bieten keine Gewähr dafür, dass Sie nun für längere Zeit ein sicheres Produkt einsetzen können. Neue Schwachstellen können **jederzeit**, auch **unmittelbar** nach dem letzten Patching ihrer Systeme, auftreten. Seien Sie sich deshalb der Notwendigkeit regelmässiger Updates bewusst.

Daher gilt: Verlieren Sie keine Zeit – **aktualisieren** Sie Ihre Software, wenn Sicherheits-Updates verfügbar sind. Antizipieren Sie das **Ende des Lebenszyklus** einer Software und ersetzen Sie diese rechtzeitig.

5 Betrug und Social Engineering

Mit 23’104 Meldungen ist Betrug nach wie vor das häufigste gemeldete Phänomen und macht zwei Drittel aller Meldungen im ersten Halbjahr 2024 aus. Im Vergleich zum Vorjahreszeitraum (11’174) hat sich die Zahl mehr als verdoppelt. Von diesen Meldungen sind 13’730, also fast 60 %, auf gefälschte Behördenanrufe zurückzuführen. Noch vor einem Jahr war dieses Phänomen inexistent und hat sich erst in der zweiten Hälfte des Jahres 2023 etabliert. Auch wenn die Meldungen zu diesem Phänomen in der zweiten Hälfte der Berichtsperiode wieder deutlich abgeflacht sind, machen sie immer noch die Mehrheit der Meldungen aus. Bei diesem Phänomen ruft ein Roboter eine grosse Anzahl zufälliger Rufnummern an. Nimmt das Opfer den Anruf entgegen, wird eine Bandansage in Englisch abgespielt. Demnach sei der Angerufene in ein Strafverfahren verwickelt. Um das weitere Vorgehen mit einem vermeintlichen Polizisten zu besprechen, soll die Taste «1» gedrückt werden. Erst danach werden die Opfer mit einem

Betrüger verbunden. Dieser überzeugt dann das Opfer mithilfe von Social-Engineering-Techniken[76], eine Fernzugriffs-Software herunterzuladen, wodurch die Betrüger dann auf deren Computer zugreifen und ungewollte Zahlungen im E-Banking auslösen.[77]

An zweiter Stelle in der Kategorie Betrug folgen mit 2'252 Meldungen gefälschte Droh-E-Mails im Namen von Behörden. In der Vorjahresperiode lag diese Kategorie mit über 5'500 Meldungen noch an der Spitze dieser Kategorie. Die Vorgehensweise ähnelt den vorgängig beschriebenen Drohanrufen. Auch in diesen Fällen wird dem Opfer eine Straftat vorgeworfen. Die Kommunikation erfolgt hier jedoch nicht per Telefon, sondern schriftlich. Das Opfer wird aufgefordert, an eine E-Mail-Adresse zu antworten. Anschliessend wird versucht, das Opfer zur Zahlung einer Kaution zu bewegen.
Abgesehen vom klassischen Vorschussbetrug[78], der mit 1'135 Meldungen an dritter Stelle der Betrugsmeldungen steht, fallen vor allem betrügerische Gewinnspiele auf. 1'111 Meldungen erhielt das BACS in der Berichtsperiode. Im Vorjahreszeitraum waren es noch 281 Meldungen. Vor allem gegen Ende der Berichtsperiode wurde dieses Phänomen überdurchschnittlich häufig gemeldet. Inzwischen werden fast alle Namen bekannter Firmen aus der Lebensmittel- und Technikbranche für das Vorgaukeln von Gewinnspielen missbraucht. Die Urheber wollen möglichst viele Teilnehmerinnen und Teilnehmer anwerben, weshalb die Beantwortung der Fragen sehr einfach ist. Um an den vermeintlichen Gewinn zu kommen, müssen auf einer gefälschten Website persönliche Daten wie Kreditkartendaten, Namen, E-Mail-Adresse oder Handy-Nummer angegeben werden. Mit dem Absenden der Informationen wird dann unwissentlich ein mehrjähriges Abonnement abgeschlossen. Die Gebühr wird unverzüglich der Kreditkarte belastet.

Eine Zunahme ist auch bei den Angriffen auf Konten sozialer Medien zu verzeichnen. Waren es im Vorjahreszeitraum noch 101 Meldungen, so sind es nun bereits 178 Meldungen. Erschwerend kommt in diesen Fällen hinzu, dass es schwierig ist, ein einmal gehacktes Konto wieder zurückzuerlangen. Dies zeigen diverse Erfahrungsberichte von Opfern. Das BACS erhält immer wieder Meldungen, dass trotz Ausfüllen der entsprechenden Formulare bei den Betreibern von sozialen Netzwerken nicht oder ablehnend reagiert wird. Oft erhalten die Opfer auch nach mehrmaligen Anfragen ihren gehackten Account nicht zurück.

5.1 Methoden der künstlichen Intelligenz bei Betrugsversuchen

Bereits der letzte Halbjahresbericht[79] hat sich mit dem Einsatz von künstlicher Intelligenz (KI) bei Betrugsversuchen eingehend befasst. Die Entwicklung hat sich in den letzten sechs Monaten nicht wesentlich verändert. Im Einzelfall ist es schwierig festzustellen, in welchem Umfang z. B. maschinelles Lernen (ML)[80] und grosse Sprachmodelle (LLM)[81] eingesetzt wurden. So kann in der Regel nur vermutet werden, ob ein Übersetzungstool verwendet wurde oder nicht. In wenigen Fällen ist deren Einsatz hingegen eindeutig. Der bisher offensichtlichste und

---

76 Social Engineering (ncsc.admin.ch)

77 Woche 15: Anrufe von Fake-Behörden auf Rekordhoch – dies ist aber nicht nur ein negatives Zeichen (ncsc.admin.ch)

78 Vorschussbetrug (ncsc.admin.ch)

79 Siehe Halbjahresbericht 2023/2 (ncsc.admin.ch)

80 Maschinelles Lernen (wikipedia.org)

81 Large Language Model (wikipedia.org)

auffälligste Fall, bei dem solche Hilfsmittel zur Anwendung kamen, war ein CEO-Betrug[82]. Bei dieser Betrugsvariante wird eine angeblich dringende Zahlungsaufforderung des CEO an die Finanzabteilung gesendet. Dabei geben sich die Betrüger in der Regel wenig Mühe, das Opfer gezielt anzusprechen und die Anfrage entsprechend zu personalisieren. Die verwendeten Texte sind unspezifisch und meist identisch. Zudem wird in diesen Fällen versucht, das Opfer von einer Kontaktaufnahme mit dem Chef abzuhalten. Nicht so aber in diesem Fall: Zunächst wurde der Finanzverantwortliche von einem Anwalt telefonisch kontaktiert und zu einer Videokonferenz mit seinem Chef eingeladen, die in wenigen Minuten beginnen sollte.[83] Dazu erhielt er eine E-Mail mit den Zugangsdaten zum Meeting. Als sich der Finanzverantwortliche dann in die Online-Konferenz einwählte, konnte er tatsächlich seinen Chef auf dem Bildschirm sehen und mit ihm interagieren. Während des Gesprächs versuchte der vermeintliche Chef, an die Handynummer des Finanzverantwortlichen zu gelangen und ihn zur Auslösung von Finanztransaktionen zu überreden. Das Video des Chefs wurde in diesem Fall von den Betrügern mit Hilfe von Deepfake-Algorithmen erstellt. Woher genau die Angreifer das Ausgangsmaterial für die Erstellung der gefälschten Videos hatten, ist ungeklärt. Das BACS geht davon aus, dass öffentlich verfügbares Videomaterial für die Erstellung des Deepfake-Videos verwendet wurde.

5.2 Werbung für Investmentbetrug

Um Internetnutzende zu einer Investition auf einer dubiosen Webseite[84] zu verleiten, nutzen Kriminelle bekannte Persönlichkeiten zur Werbung für angeblich lukrative Investmentangebote. Denn mit diesen Angeboten hätten diese in kürzester Zeit viel Geld verdient. Schweizer und internationale Prominenz wie Sandra Boner, Beatrice Müller, Roger Federer, Nemo oder Alain Berset finden sich ungewollt als Gesichter von zahlreichen betrügerischen Werbeinseraten wieder. Die zum Teil sehr geschmacklosen Inserate werden immer mehr zum Ärgernis. So erscheinen täglich neue Inserate, die mit falschen Versprechungen locken.
Die Werbung für den Investmentbetrug folgte bisher immer den gleichen Mustern: Es wird behauptet, dass die berühmte Persönlichkeit nicht über eine höchst rentable und sichere Investition sprechen durfte, da es sonst zur Entlassung geführt hätte. Eine andere Variante gibt an, dass versehentlich eine Aussage gemacht wurde, die nie an die Öffentlichkeit hätte gelangen dürfen. Es kommt sogar auch vor, dass der Tod eines Prominenten proklamiert wird. Die erste Investitionssumme ist meist bei 250 CHF angesetzt. Nach den ersten Tagen erhält das Opfer dann Berichte von sich überschlagenden Gewinnen, was das Opfer zu zusätzlichem Investieren anregen soll. Aus den anfänglich überschaubaren 250 CHF können dann schnell mehrere 1’000 oder gar 10'000 CHF werden. Sobald sich das Opfer den investierten Betrag und den Gewinn auszahlen will, wird es hingehalten und teilweise auch noch zur Zahlung zusätzlicher Gebühren aufgefordert. Der Betrug basiert darauf, dass Opfer mit relativ niederen initialen Zahlungen geködert werden und in einem zweiten Schritt eine Vertrauensbeziehung aufgebaut wird. Die spekulativen Angebote richten sich mehrheitlich an Personen, die geringe Kenntnisse im Bereich der Anlageinvestition mitbringen. So gibt es viele, die ihr ganzes Erspartes «investieren» respektive verlieren.

---

82 CEO-Betrug (ncsc.admin.ch)
83 Woche 14: Online-Meeting mit Deep-Fake-Chef: CEO-Betrug 2.0 (ncsc.admin.ch)
84 Investmentbetrug (ncsc.admin.ch)

Schlussfolgerungen / Empfehlungen

Mithilfe von Algorithmen-basierten Anwendungen können Cyberakteure Inhalte für glaubhaft aussehende E-Mails und Kurznachrichten erstellen, die sprachlich und in der Darstellung einem legitimen Schreiben täuschend ähnlich sehen. Sie unterscheiden sich kaum mehr vom Werk eines sprachlich versierten Menschen. Dies erschwert es den Empfängern solcher Inhalte, den Betrugsversuch zu erkennen. Weiter ermöglicht deren Einsatz das Erstellen von täuschend echt aussehenden Fotos und Videos sowie von echt klingenden Stimmen (Deepfakes). Diese können Kriminelle für Social-Engineering-Angriffe verwenden. Stimmimitationen können Zielpersonen überzeugen, dass sie mit einer bekannten Person sprechen, die Geld oder andere Hilfe benötigt.

Betrüger sind kreativ im Ausdenken neuer Szenarien, um Opfer zu unbedachten Handlungen zu verleiten. Mithilfe von KI-generierten Inhalten und Social-Engineering erreichen sie, dass die Opfer von der Täterschaft gesteuerte Handlungen ausführen, ohne Verdacht zu schöpfen. Lassen Sie sich deshalb nicht täuschen. Denken Sie erst in Ruhe nach und fragen Sie im Zweifelsfall andere Personen oder das BACS, wie sie den Sachverhalt beurteilen.

6 Störung der Verfügbarkeit von Websites und -diensten (DDoS)

Bei Angriffen auf die Verfügbarkeit von Websites und -diensten – auch bekannt als «Distributed Denial of Service» (DDoS)[85] – versuchen Angreifer, einen dem Internet zugänglichen Dienst oder System mithilfe einer grossen Anzahl von Anfragen für die Nutzung temporär unzugänglich zu machen. Solche Angriffe beinhalten weder den unberechtigten Zugriff auf Daten noch die nachhaltige Beschädigung von Systemen. Erfolgreiche DDoS-Angriffe haben daher in der Regel nur zur Folge, dass der anvisierte Dienst – meistens eine Website – der betroffenen Organisation vorübergehend nicht verfügbar ist. Dieses Kapitel geht auf drei DDoS-Kampagnen ein, die im Berichtshalbjahr beobachtet wurden. Während eine der Kampagnen sich durch eine finanzielle Motivation charakterisierte, ordnen sich die beiden anderen dem Aktivismus im Cyberraum (Hacktivismus)[86] zu.

Im April 2024 meldeten verschiedene Schweizer Organisationen aus dem Finanzsektor DDoS-Angriffe, die mit Erpressung gekoppelt waren.[87] Diese Angriffe, zu denen sich angeblich die Gruppe «Armada Collective»[88] respektive «Alpha Jackal» bekannte, wendeten das folgende Muster an: Zunächst erhält die Zielorganisation per E-Mail eine Drohung, dass ihre Online-Dienste gestört werden, wenn sie kein Lösegeld zahlt. Auf diese Drohung folgt unmittelbar ein

---

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

86 Siehe Fokusthema im Halbjahresbericht 2023/01: NCSC-Halbjahresbericht mit Fokusthema «Hacktivismus» (ncsc.admin.ch)

87 DDoS Angriffe und Erpressung: eine äusserst aktuelle Kombination (ncsc.admin.ch)

88 Die Gruppe Armada Collective wurde 2015 und 2016 von MELANI, einer Vorgängerorganisation des BACS, mit demselben Modus Operandi beobachtet. Es gibt jedoch keine technischen Hinweise, die bestätigen, dass es sich bei dieser Aktivität im Jahr 2024 wiederum um dieselben Akteure handelt.

kurzer DDoS-Angriff, der jedoch bereits zu einer Überlastung und Unterbrechung dieser Dienste führen kann. Anschliessend setzt der Angreifer die Zielorganisation weiter unter Druck, das Lösegeld zu zahlen und droht per E-Mail, seine Angriffe zu intensivieren. Bei einem Teil der gemeldeten Fälle wurde die Drohung wahr gemacht und die Dauer sowie die Intensität der Angriffe nahmen zu. Bei einigen Angriffen wurden dazu noch legitime Quell-IP-Adressen von Finanzorganisationen missbraucht und zur Durchführung von Angriffen auf andere Institutionen verwendet. In der überwiegenden Mehrheit der gemeldeten Fälle waren jedoch die Auswirkungen begrenzt und konnten durch gängige Massnahmen zur Eindämmung von DDoS-Angriffen abgewehrt werden. Die letzte Aktivität des Armada Collective – oder von jemandem, der behauptet, Teil der Gruppe zu sein – wurde in der Schweiz im Jahr 2020 verzeichnet.

Neben finanziellen Gründen haben Bedrohungsakteure erneut DDoS-Angriffe mit politischen Absichten[89] im Kontext von grossen internationalen Veranstaltungen und Konferenzen in der Schweiz eingesetzt. Das pro-russische Hacktivisten-Kollektiv «NoName057(16)» zielte im Januar 2024 auf Websites im Zusammenhang mit dem Weltwirtschaftsforum (WEF) und im Juni 2024 auf Websites von Organisationen mit Verbindungen zur «Konferenz zum Frieden in der Ukraine» auf dem Bürgenstock. Im Vorfeld hatte das BACS ein Merkblatt mit Empfehlungen für Organisatoren mit besonders exponierten Infrastrukturen veröffentlicht.[90] Während beider Veranstaltungen analysierte das BACS die Zielauswahl der Hacktivisten und arbeitete mit den Betreibern der betroffenen Infrastrukturen eng zusammen. Insgesamt lagen die Angriffe im erwarteten Bereich und führten nur zu geringfügigen Beeinträchtigungen der IT-Infrastruktur. Zu keinem Zeitpunkt waren die IT-Systeme und Daten dieser Veranstaltungen oder der beteiligten Organisationen ernsthaft gefährdet.[91] Diese DDoS-Angriffe bestanden hauptsächlich aus Angriffen auf der Anwendungsebene des OSI-Modells (sog. «Layer 7»)[92], was im Detail Überflutungen von HTTP/s GET-Anfragen sind.[93] Die meisten der verwendeten IP-Adressen gehörten zu privaten VPN-Dienstleistern, die von NoName057(16) für den DDoS-Angriff missbraucht worden waren.

Empfehlungen

Die Website des BACS bietet unter der Rubrik Angriff auf die Verfügbarkeit (DDoS-Angriff) (ncsc.admin.ch) verschiedene 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.

89 Siehe Halbjahresbericht 2023/2, Kap 3.6.1; Halbjahresbericht 2023/1, Kap 2.

90 Massnahmen zur Cyberresilienz im Kontext von Grossveranstaltungen und internationalen Konferenzen (ncsc.admin.ch)

91 Hochrangige Konferenz zum Frieden in der Ukraine: Erste Bilanz des BACS zu den Arbeiten des Cyberlageverbunds (ncsc.admin.ch)

92 Application layer DDoS attack (cloudflare.com)

93 HTTP flood DDoS attack (cloudflare.com)

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).

7 Datenmanagement, -abflüsse und -erpressung

Datenlecks und ungewollte Datenexposition sind immer wieder Teil der Schlagzeilen: Beispielsweise waren rund 500 GB biometrische und andere sensitive Daten von indischen Bürgerinnen und Bürgern, inklusive Militärangehörigen und Polizisten, im Mai 2024 öffentlich zugänglich. Die betreffende Datenbank war falsch konfiguriert und ohne ein Passwort geschützt.[94] Ein effektives Zugriffsschutz- und Datenmanagement ist daher sowohl für Unternehmen als auch für Behörden und Privatpersonen unabdingbar, um eine sichere Datenhaltung zu gewährleisten. Dies zeigt sich insbesondere im Kontext von Datenabflüssen, die nicht nur Konsequenzen für die direkt-betroffenen Organisationen, sondern auch ein Angriffspotential auf weitere Organisationen entfalten. Sensitive Informationen von Privatpersonen rücken dabei gleichwohl in den Fokus von Bedrohungsakteuren. Denn nach einem Datenabfluss steigt für Betroffene das Risiko von Folgeangriffen, wie beispielsweise durch Kontoübernahmen, Phishing (vgl. Kap. 2), Identitätsdiebstahl oder Finanzbetrug (vgl. Kap. 5). Die aktuelle Cyberbedrohungslage in Bezug auf Datenlecks zeigt, dass ein Grossteil der ungewollt veröffentlichten Daten durch Ransomware-Gruppierungen für die Datenerpressung genutzt werden (vgl. Kap. 3.2). Gleichzeitig sind auch andere Ursachen wie ein unzureichendes Datenmanagement in der eigenen Infrastruktur oder bei Zulieferern zu identifizieren. Vorhandene Schwachstellen und technische Fehlkonfigurationen können zudem zu einer ungewollten Datenexposition führen und durch Bedrohungsakteure ausgenutzt werden.

7.1 Datenabflüsse bei Zulieferern

Datenabflüsse gehören national und international zu einer für die Öffentlichkeit immer sichtbareren Problematik – insbesondere, wenn Lieferketten bei Vorfällen involviert sind. Einer der bekannteren Vorfälle in der Schweiz ist der Play Ransomware-Angriff auf das Software-Unternehmen Xplain AG im Jahr 2023. Die von den Kriminellen veröffentlichten Kundendaten beinhalteten auch solche der Schweizer Bundesverwaltung, u. a. im Bereich der inneren Sicherheit. Anfang März 2024 publizierte das BACS einen Bericht, in dem die Vorfallsbewältigung seitens Bundesverwaltung zusammengefasst, die veröffentlichten Daten analysiert und Schlussfolgerungen einer solchen Datenüberprüfung abgeleitet wurden.[95] Aus der Triage ging hervor, dass rund 5 % des gesamthaft veröffentlichten Datenvolumens von etwa 1.3 Millionen Objekten für die Bundesverwaltung relevant waren. Obwohl die Mehrheit der Daten der Xplain

94 Data Leak Exposes 500GB of Indian Police, Military Biometric Data (hackread.com)

95 Hackerangriff auf Firma Xplain: Bericht des Bundesamtes für Cybersicherheit zur Datenanalyse publiziert (admin.ch)

AG selbst gehörten, waren 9'040 (rund 14 %) dieser Objekte der Bundesverwaltung zuzuweisen. Etwas mehr als die Hälfte der Objekte enthielten sensitive Inhalte wie Personendaten, technische und/oder klassifizierte Informationen. Die getätigte Triage und Analyse verdeutlichte, dass nach einem Datenabfluss eine exakte Analyse der abgeflossenen Daten – insbesondere bei unstrukturierten[96] Daten – einen verhältnismässig hohen Aufwand impliziert. Dabei war eine erste Herausforderung die schnelle Bereitstellung der geeigneten Instrumente für die Aufbereitung und Analyse der Daten sowie personellen Ressourcen, die die aufwändige, manuelle Sichtung und Kategorisierung der Daten durchführen konnten. Dieses Vorgehen ist ressourcenintensiv und entsprechend kostspielig, besonders wenn die Sichtung nicht komplett maschinell automatisiert werden kann.
Der Vorfall zog weitere Untersuchungen auf Bundesebene nach sich: Einerseits eröffnete die Bundesanwaltschaft (BA) zwei Strafverfahren im Zusammenhang mit dem Cyberangriff. Andererseits leitete der Schweizer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) seinerseits eine unabhängige Untersuchung zum Datenabfluss ein.[97] Diese stellte fest, dass unzureichende Abmachungen zwischen dem Lieferanten und zweier Bundesämter dazu führten, dass eine unverhältnismässig hohe Anzahl an Personendaten durch Unterstützungsprozesse an den Lieferanten gelangten und dort gespeichert wurden. Ferner beschloss der Bundesrat im Sommer 2023 einen politisch-strategischen Krisenstab «Datenabfluss» (PSK-D) sowie eine Administrativuntersuchung ins Leben zu rufen.[98] Basierend auf den Schlussfolgerungen der Administrativuntersuchung[99] leitete der Bund verschiedene Massnahmen zur nachhaltigen und systematischen Verbesserung der Datensicherheit ein. Das per 1. Januar 2024 in Kraft getretene Informationssicherheitsgesetz (ISG) widerspiegelt und ergänzt das Massnahmenpaket.[100]

Vorfälle ähnlicher Natur lassen sich auch auf internationaler Ebene beobachten. Eine breit angelegte, gezielte Angriffskampagne gegen Kunden des global agierenden Unternehmens Snowflake nutzte bewusst den grossen Kundenstamm von Snowflake in Verbindung mit ungenügend gesicherten Konten aus. Das Kerngeschäft von Snowflake besteht in der Bereitstellung einer Cloud-basierten[101] Plattform für strukturierte und unstrukturierte Daten. Diese ermöglicht es Kunden, Daten zu speichern und für vertiefte Analysen mit Methoden des maschinellen Lernens weiterzuverarbeiten. Integriert in dieser Plattform ist zudem ein Marktplatz, auf dem Daten verkauft und getauscht sowie Daten von Dritten gratis genutzt werden können. Ende Mai 2024 verkündete die Hackergruppe «ShinyHunters», Daten des Unternehmen Ticketmaster mithilfe einer Schadsoftware für die Beschaffung von Daten (Infostealer) exfiltriert zu haben.[102] Die rund 1.3 Terabyte (TB) an Daten, die von rund 560 Millionen Nutzerinnen und Nutzern von Ticketmaster stammten, griffen die Kriminellen über die Plattform von Snowflake

---

96 Unstrukturierte Daten (wikipedia.org)

97 Ein Bericht mit den Ergebnissen zur Untersuchung betreffend Datenbearbeitung seitens Xplain AG und abgeleitete Empfehlungen wurde am 1. Mai 2024 veröffentlicht, vgl. EDÖB schliesst Untersuchungen gegen das Unternehmen Xplain und die Bundesämter fedpol und BAZG ab (edoeb.admin.ch).

98 Hackerangriff auf Firma Xplain: Bundesrat mandatiert politisch-strategischen Krisenstab «Datenabfluss» (admin.ch)

99 Die Resultate der Administrativuntersuchung wurden am 1. Mai 2024 publiziert, vgl. Abschluss der Administrativuntersuchung zum Hackerangriff auf die Xplain AG: Bundesrat beschliesst Massnahmen (admin.ch)

100 Bundesrat setzt das Informationssicherheitsgesetz in Kraft (admin.ch)

101 Cloud Computing (wikipedia.org)

102 Live Nation confirms Ticketmaster breach after hackers hawk stolen info of 560 million (therecord.media)

ab. Der finanzgetriebene Bedrohungsakteur ging dabei ähnlich wie Ransomware-Gruppierungen vor (vgl. Kap. 3.2), ohne aber eine Verschlüsselung der Daten beim Opfer durchzuführen. Damit stand der Vorfall bei Ticketmaster aber nicht für sich allein. Auch viele weitere Unternehmen – u. a. AT&T[103] und Santander[104] – wurden Opfer dieser Datenerpressungskampagne durch dieselben Akteure. Eine eingehende Untersuchung in Zusammenarbeit mit der IT-Sicherheitsfirma Mandiant schlussfolgerte, dass die unautorisierten Zugriffe auf die Datenbanken bereits im April 2024 anfingen. Weiter fand Mandiant keine Hinweise, dass die Datenexfiltrationen von Snowflake-Instanzen wegen einer Fehlkonfiguration, einer Schwachstelle oder eines anderen Verstosses bei der generellen Snowflake-Infrastruktur ermöglicht wurde, sondern aufgrund von vorgängig abgeflossenen Zugangsdaten von Kunden durch Infostealer.[105] Abgeflossene Passwörter reichten dabei teilweise zurück ins Jahr 2020. In Kombination mit fehlender Zwei-Faktor-Authentifizierung (2FA) der Benutzerkonten konnten sich die Kriminellen systematisch Zugriff auf Snowflake-Instanzen ergaunern. Das Ausmass der Kampagne und auch das mögliche Schadenspotential werden insbesondere in Anbetracht dessen ersichtlich, dass Mandiant und Snowflake rund 165 mögliche Opfer über exponierte Snowflake-Infrastruktur informieren musste.[106]

Empfehlungen

Speichern Sie nur Daten, die Sie wirklich benötigen (Datensparsamkeit). **Löschen** Sie nicht mehr benötigte Daten **zeitnah** beziehungsweise **archivieren** Sie aufbewahrungswürdige aber nicht mehr aktiv gebrauchte Daten **offline**. Vereinbaren Sie verbindlich mit Zulieferern und Partnern, unter welchen Voraussetzungen mit welchen Daten wie umgegangen werden kann und darf. Implementieren Sie Kontrollmechanismen, damit diese Abmachungen eingehalten werden. Schützen Sie ferner Zugänge zu Systemen, Konten und Daten mit starken Passwörtern und wo immer möglich mit einer **Multi-Faktor-Authentifizierung (MFA)**.[107]

7.2 Legaler und illegaler Datenhandel

Daten sind das Gold der Digitalisierung. Sie sind ein wertvolles Gut, was sie sowohl für legale als auch für illegale Geschäfte interessant macht. Infolgedessen nutzen beispielsweise Cyberkriminelle für die Beschaffung von Daten Phishing (vgl. Kap. 2), Infostealer und illegale Platt-

[103] Siehe Toll of Snowflake Widens With Theft of AT&T Text, Calling Data (bloomberg.com), AT&T Addresses Illegal Download of Customer Data (att.com)
[104] More than 12,000 Santander employees in US affected by Snowflake customer breach (therecord.media)
[105] Detecting and Preventing Unauthorized User Access (snowflake.discourse.group)
[106] UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion (cloud.google.com)
[107] Siehe Schützen Sie Ihre Konten / Passwörter (ncsc.admin.ch)

formen für den Ankauf. Durch die stetige Nachfrage hat sich ein eigenes Ökosystem an illegalen Marktplätzen im Deep- und Darkweb[108] aufgebaut, die teilweise bis ins Clearweb[109] reichen. Sie ermöglichen den Kriminellen Austausch, Arbeitsteilung und Spezialisierung.[110] Während beispielsweise die einen vor allem mit Chain Phishing (vgl. Kap. 2.1) oder mit einer Schadsoftware alte E-Mail-Verläufe sammeln und verkaufen, kaufen andere diese Informationen, um auf deren Grundlage Betrügereien durchzuführen.
Einer der aktuell in der Öffentlichkeit und den Medien präsentere Markt ist «BreachForums». Die englisch sprachige Plattform entstand, nachdem verschiedene bei Hackern beliebte Vorgängermarktplätze wie z. B. «RaidForums» durch Polizei-Operationen im Jahr 2022 geschlossen worden waren.[111] Jedoch verhafteten die US-Strafverfolgungsbehörden den Gründer schon ein Jahr später und schlossen die neu erstellte Plattform sogleich wieder.[112] Dennoch konnte «BreachForums» unter der Führung der Gruppe ShinyHunters wieder neu aufgesetzt werden und die Plattform etablierte sich zu einer der Kernforen für den Verkauf und das freie Teilen von gestohlenen Daten und Zugangsinformationen. Gehandelte Daten reichen dabei von öffentlich zugänglichen bis hin zu sehr sensitiven Inhalten: Ein erschreckendes Beispiel ist hierfür der im April 2024 versuchte Verkauf von rund 5 Millionen hochauflösenden Passfotos – mit Beschriftungen ihrer Identitätsnummern – von Bürgerinnen und Bürgern von El Salvador. Ergänzend erhielt der Käufer dann auch noch einen Datensatz mit persönlichen Informationen wie Name, Identitätsnummer, Geburtstag und Kontaktinformationen. Es ist damit anzunehmen, dass rund 80 % der salvadorianischen Bevölkerung in diesem Datenleck enthalten sind.[113]

Im Mai dieses Jahres holten die Strafverfolgungsbehörden erneut zum Schlag gegen «BreachForums» aus. Mit Beteiligung der Kantonspolizei Zürich gelang es dem FBI, die Domains temporär zu übernehmen.[114] Leider konnten sich die ehemaligen Administratoren schon nach zwei Wochen die Seite im Darkweb wieder aufbauen und sich sogar den Zugriff auf die originale Clearweb-Seite zurückholen.[115] Der Domain-Registrator gab anscheinend die vom FBI beschlagnahmte Webseite im Clearweb an die Administratoren zurück.[116] Damit sind die beiden Plattformen wieder vollständig operativ, was besonders durch die Snowflake-Leaks eindrücklich unter Beweis gestellt wurde (vgl. Kap. 7.1). Die Strafverfolgungsbehörden können zwar immer wieder erfolgreich solche Netzwerke und Marktplätze zerlegen und die illegalen Aktivitäten stören, jedoch ist die Nachfrage und Backup-Infrastruktur so robust, dass sich immer wieder neue Plattformen bilden.

---

108 Deep Web (wikipedia.org), Dark web (wikipedia.org)
109 Surface Web (wikipedia.org)
110 Top 10 Deep Web and Dark Web Forums (socradar.io)
111 One of the world's biggest hacker forums taken down (europol.europa.eu)
112 Justice Department Announces Arrest of the Founder of One of the World's Largest Hacker Forums and Disruption of Forum's Operation (justice.gov)
113 Threat Actor Claims to Have Leaked Database Containing Personal Information of 5 Million Salvadoran Citizens (dailydarkweb.net)
114 Breachforum: FBI und Kapo Zürich gelingt Schlag gegen Hacker (nzz.ch)
115 BreachForums returns just weeks after FBI-led takedown (theregister.com)
116 Breach Forums Return to Clearnet and Dark Web Despite FBI Seizure (hackread.com)

Schlussfolgerung / Empfehlungen

Daten sind wertvoll. Daher gibt es auch ein kriminelles Interesse, sich diese mit unehrlichen Mitteln zu beschaffen und zu verkaufen oder die Opfer mit der Drohung einer Veröffentlichung von sensitiven Daten zu erpressen. Nicht zuletzt sollte sich jede Person darüber im Klaren sein, dass Informationen – ob freiwillig oder unfreiwillig – im Netz öffentlich verfügbar sind. Akteure mit böswilligen Interessen können dies ausnutzen und für Social-Engineering verwenden. Aufgrund dessen sollte sich die Diskussion der Datensicherheit von der Frage wegbewegen, ob ein Datenabfluss stattfinden kann, und hin zur Frage, wann dieser geschieht und wie die Daten selbst – im Extremfall eines Abflusses – für den Angreifer nutzlos sind.

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 Daten löschen. Etablieren Sie klare, umsetzbare Prozesse für den Datenumgang und -schutz und kontrollieren Sie die Implementation.

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).

Daten werden aber nicht nur im kriminellen Milieu, sondern auch in der Legalität gehandelt. Datenbroker[117] und -dienstleister wie zum Beispiel Snowflake ermöglichen es Unternehmen, einfach Daten zu kaufen oder gratis zu erhalten. Jedoch besteht bei legalen Plattformen das Problem, dass auch wiederrechtlich gesammelte Datensätze auf diese gelangen können und durch den Betreiber aus dem Verkehr gezogen werden müssen.[118] Grundsätzlich ist die Bearbeitung von Personendaten durch Unternehmen aus der Sicht des Datenschutzes widerrechtlich, wenn diese ohne das explizite Einverständnis der betroffenen Personen erhoben und zu Analysezwecken bearbeitet werden, für die es kein überwiegend öffentliches oder privates Interesse gibt.[119] Ferner ist es für Unternehmen relativ simpel, Daten von Nutzerinnen und Nutzern mit deren Erlaubnis zu sammeln. Dies wird dann besonders in hohem Masse gemacht, wenn es wie beispielsweise bei der Werbebranche zum Kerngeschäft gehört. Mithilfe einzigartiger Werbe-IDs, die einen eindeutigen Identifikator von mobilen Endgeräten darstellt, können Unternehmen das Verhalten von Nutzerinnen und Nutzern in Daten erheben, zusammenfügen, analysieren und personalisierte Werbung für den Endnutzer erstellen. Werbe-IDs sind dabei eine wertvolle Quelle für Informationen für Unternehmen, da sie persistent und über

[117] Datenbroker sind Unternehmen, die Informationen in Datensätzen systematisch sammeln, mit weiteren Informationen anreichern und sie an Dritte weiterverkaufen.

[118] Siehe Databroker: Belgian data marketplace publishes passport data of thousands of people (netzpolitik.org), European data broker: Sensitive passport data of Germans published online (netzpolitik.org)

[119] Siehe hierzu Art. 30 sowie 31 Abs. 1 des Datenschutzgesetzes (DSG; SR 235.1); Sandra Husi/Stämpfli/Anne-Sophie Morand/Ursula Sury, Datenschutzrecht, Zürich 2023, S. 150 ff., N 277 ff.

verschiedene Geräte (interoperabel) einsetzbar sind.[120] Dabei spielen auch Cookies einen integralen Bestandteil in der Analyse des Nutzerverhaltens. Anders aber als Werbe-IDs sind Cookies anonymisierte Besucher-IDs, die nur pro Gerät erhoben werden und das Erstellen eines kompletten Nutzerprofils nicht ermöglichen. Sie protokollieren ebenfalls das Surfverhalten und speichern Präferenzen und Nutzereigenschaften.[121] Abgesehen von Cookies erlauben auch Methoden wie Fingerprinting das Sammeln und Wiederkennen von Nutzerinnen und Nutzern mithilfe von Metadaten.[122] Aber auch durch das Akzeptieren von Berechtigungen bei Applikationen von Mobilgeräten können persönliche Daten – wie Standortinformationen – an Unternehmen weitergegeben werden. Diesen Umstand zeigt eine Analyse des SRF vom Juni 2024 illustrativ auf.[123] Während den Recherchen erhielt SRF Data kostenlos einen Datensatz von Standortdaten von 1.3 Millionen Geräten in der Schweiz während einer Woche des Jahres 2024, die gemäss dem Anbieter anonymisiert sein sollten. Diese Informationen sind wahrscheinlich durch App- und Webseitentracker von verschiedenen Unternehmen zu Werbezwecken erhoben worden. Anders als vom Anbieter versprochen, konnte SRF Data aber nach kurzer Zeit die Daten bestimmten Personen zuordnen, was deren Privatsphäre nachhaltig beeinträchtigt.

Empfehlungen

Achten Sie beim täglichen Gebrauch Ihres Mobilgerätes, dass Sie bei den von Ihnen genutzten Applikationen nur die **Berechtigungen** geben, die Sie auch wirklich erteilen möchten. Akzeptieren Sie im **Cookie**-Banner bei Websites und Applikationen nicht intuitiv alle Cookies. Mit ein paar zusätzlichen Klicks können Sie Cookies, die über die normale Funktionalität hinausgehen, **ablehnen** und so ein ungewolltes Speichern und Weiterverkaufen Ihrer Daten verhindern. Die Anleitung von SRF[124] erklärt Ihnen, wie Sie diese Punkte und weitere Schritte umsetzen können.

8 Cyberspionage und -sabotage

Nebst den nicht-staatlichen Akteuren bewegen sich auch staatliche Bedrohungsakteure in der Cyberbedrohungslandschaft. Diese werden in der Regel als sogenannte «Advanced Persistent Threat» (APT)[125] bezeichnet, da sie aufgrund ihrer zeitlichen, personellen, technischen und finanziellen Ressourcen eine fortgeschrittene und anhaltende Bedrohung darstellen können. Ein APT zeichnet sich dadurch aus, dass er seine Methoden unabhängig der Kosten weiterentwickelt, um massgeschneiderte, auf seine Ziele abgestimmte Angriffe durchzuführen. Sobald APTs entdeckt und aus einem Netzwerk entfernt wurden, versuchen sie erneut, sich

120 Werbewelt ohne Cookies: Mit neuen ID-Technologien in die Zukunft (traffective.com)
121 DSGVO vs. ePrivacy: Datenschutz, einfach erklärt (traffective.com)
122 Browser fingerprinting explained (+7 top techniques) (fingerprint.com)
123 Tracking mit Ortungsdiensten - Der Spion in unseren Handys (srf.ch)
124 Anleitung gegen Tracking - So schützen Sie Ihr Handy vor Tracking (srf.ch)
125 APT (csrc.nist.gov)

Zugang zu diesem zu verschaffen. Obwohl APTs besonders im staatlichen Umfeld agieren, arbeiten sie für ihre Ziele auch mit nicht-staatlichen Akteuren zusammen. Die Interessen sind dabei mannigfaltig. Während einige finanzielle Interessen verfolgen, haben sich die meisten auf Cyberspionage, Sabotage oder beides spezialisiert. Das Kapitel behandelt relevante Themen und Entwicklungen im internationalen Kontext, die für ein verbessertes Verständnis der Schweiz im digitalen Raum unabdingbar sind.

8.1 Cyberspionage

8.1.1 Politische Institutionen unter Druck

Anfang des Jahres bezeichnete das WEF das Jahr 2024 als Rekordwahljahr, denn in über 50 Ländern weltweit stehen Wahlen an.[126] Die Erfahrung zeigt, dass solche zentralen Ereignisse der politischen Prozesse Opportunitäten für verschiedene Bedrohungsakteure bieten. Während Kriminelle das Thema zur eigenen Bereicherung ausnützen wollen, können Hacktivisten mehr Aufmerksamkeit für ihre Sache erregen. Anders profitieren staatliche Akteure, indem sie Wahlen für das Sammeln von Informationen oder für Beeinflussungsoperationen instrumentalisieren.[127] Im Sinne dieser Erwartungen waren Wahlen, die in dieser Berichtsperiode stattfanden, von erhöhten Cyberaktivitäten betroffen. Dabei standen die Europawahlen unter besonderer Beobachtung. Die sichtbarsten Cyberaktivitäten, über die die Medien berichten, gingen häufig von Hacktivisten aus, sei es in Form von Drohungen oder tatsächlichen Angriffen. So wurde u. a. zu Beginn der Europawahlen von DDoS-Angriffen auf die Websites niederländischer Parteien berichtet, zu denen sich die pro-russische Gruppe «Hacknet» bekannte.[128] Die tatsächlichen, direkten Auswirkungen dieser Aktivitäten scheinen gering zu sein, da nur temporäre Einschränkungen mit DDoS-Angriffen erreicht werden können (vgl. Kap. 6). Dennoch hat die Hacktivistengruppe ihr Hauptziel der Aufmerksamkeit und der erhaltenen Sichtbarkeit erreicht.
Der Kontext von Wahlen und Parlamenten ist auch für Cyberspionage sensibel. Im Hinblick auf dieses Rekordwahljahr und aufgrund der hohen Relevanz eines unabhängigen Wahlprozesses hatte die Agentur der Europäischen Union für Cybersicherheit (ENISA) im März ihr Kompendium über die Sicherheit von Wahlen aktualisiert.[129] Trotzdem war die Christlich Demokratische Union Deutschlands (CDU) eine Woche vor den Europawahlen von einem Cyberangriff betroffen. Das deutsche Bundesinnenministerium bestätigte zwar den Vorfall, jedoch wurden nur wenige der Details veröffentlicht.[130] Bekannt ist, dass sich die Angreifer dank einer Schwachstelle Zugang zu den IT-Systemen verschafft hatten.[131] Es wird weiter angedeutet, dass es sich um einen sehr fähigen Akteur handelte.[132]

Im Gegensatz zu den hacktivistischen Operationen während den Europawahlen sind potenziell schwerwiegendere Cyberangriffe komplexer zu entdecken und werden seltener aufgrund

126 Why 2024 is a record year for elections around the world (weforum.org)
127 Siehe für Überblick: Poll Vaulting: Cyber Threats to Global Elections (cloud.google.com)
128 Dutch political websites hit by cyber attacks as EU voting starts (cloudflare.com)
129 Safeguarding EU elections amidst cybersecurity challenges (enisa.europa.eu)
130 CDU: Cyber-Angriff auf Parteizentrale – Verfassungsschutz eingeschaltet (spiegel.de)
131 Hackerangriff auf CDU: Software wird auch in Mitteldeutschland genutzt (mdr.de)
132 Germany's Christian Democratic party hit by 'serious' cyberattack (reuters.com)

geopolitischer Implikationen offengelegt. Die Schweiz und ihre politischen Institutionen sind davon nicht ausgenommen, wie die Angriffe im Jahr 2021 auf 122 Parlamentarier in der Schweiz und anderen europäischen Staaten im Mai 2024 zeigten.[133] Die Spear-Phishing-Angriffe gegen die Schweizer Parlamentarier waren Teil einer grösseren Kampagne, die sich gegen Mitglieder der Interparlamentarischen Allianz zu China (IPAC) richtete. Sie wurden von den Behörden der USA und Grossbritanniens öffentlich der chinesischen staatlichen Gruppe «APT31» zugeschrieben.[134]

8.1.2 Internationale Entwicklungen in der Cyberspionage

ISoon – ein lehrreiches Datenleck

Im Februar 2024 wurden mehr als 500 – höchstwahrscheinlich authentische – Dokumente der chinesischen Firma ISoon über die kollaborative Entwicklungsplattform GitHub geleakt. Sie enthielten Listen von Angriffszielen, Werkzeugbeschreibungen, aber auch Gespräche zwischen Mitarbeitenden. Die Dokumente werden von vielen Experten als legitim eingestuft. Sie geben Aufschluss über die Aktivitäten des Dienstleisters, der in den Bereichen Überwachung und Cyberangriffe tätig ist und u. a. für das Ministerium für öffentliche Sicherheit, die Staatssicherheit und das chinesische Militär tätig sein soll.[135]

Diese Dokumente veranschaulichen den Stellenwert von Outsourcing-Praktiken in Chinas Cyberoperationen und die Art und Weise, wie dieses Ökosystem funktioniert. Der Rückgriff auf externe Dienstleister birgt für den Auftragnehmer Risiken, da er die Kontrolle über Teile der Angriffskette verlieren kann (vgl. Kap. 7.1). Diese Vorgehensweise hat jedoch den Vorteil, dass der Staat seine Beteiligung abstreiten kann, wenn eine Operation enttarnt wird.

Der Aufschwung der ORB-Netzwerke

Im Januar 2024 gaben die US-Behörden bekannt, dass sie ein Angriffsnetzwerk bestehend aus kompromittierten Routern ausser Betrieb genommen hatten.[136] Dieses Netzwerk soll von der Gruppe «Volt Typhoon»[137] genutzt worden sein, die die US-Behörden mit dem chinesischen Staat in Verbindung bringen. Die USA beschuldigen die Gruppe, kritische Infrastrukturen in den USA und anderen Ländern ins Visier genommen zu haben. Um das Netzwerk funktionsunfähig zu machen, benötigten die US-Behörden Fernzugriff auf kompromittierte Router. Dies war notwendig, um die Schadsoftware von innen zu zerstören und eine weitere Kommunikation mit der Angriffsinfrastruktur zu verhindern.

Die Verwendung von Netzwerken mit kompromittierten Routern oder anderen vernetzten Objekten – sog. ORB-Netzwerke (Operational Relay Boxes) ist ein bekanntes Vorgehen. Neu ist deren Ausmass und erhöhte Nutzung, insbesondere durch chinesische staatliche Akteure. Jedoch verwenden nicht nur chinesische APTs solche Netzwerke. Der dem russischen Militärgeheimdienst (GRU) nahen «APT28» – auch bekannt als «Sofacy» – machte Gebrauch von

---

133 Schweizer Parlamentarier von chinesischen Staatshackern attackiert (watson.ch)

134 Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians (justice.gov); UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity (gov.uk)

135 iSoon leak sheds light on China's use of extensive hacker-for-hire ecosystem (huntandhackett.com)

136 U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure (justice.gov)

137 Siehe Halbjahresbericht 2023/02; Kap. 3.5.

ähnlichen Netzwerken operiert von Kriminellen für Cyberoperationen.[138] Für den Angreifer hat die Nutzung von ORB-Netzwerken viele Vorteile: Es ermöglicht ihm, die eigene Identität zu verschleiern und die Entdeckung eines Angriffs zu erschweren. Bei Bedarf kann auch schnell auf eine neue Infrastruktur umgeschwenkt werden.
Diese Entwicklung demonstriert, dass der bei Cyberkriminellen verbreitete Trend der Arbeitsteilung auch die Methoden staatlicher Akteure beeinflusst. So stellen beispielsweise Dienstleister – auch aus dem kriminellen Milieu – den staatlichen Bedrohungsakteuren solche Netzwerke für deren Cyberoperationen zur Verfügung. Ebenso zeigt dieses Beispiel exemplarisch, wie fliessend die Grenzen zwischen staatlichen und privaten Akteuren im Cyberraum mittlerweile sind.

Schlussfolgerung / Empfehlungen

Nicht nur eigentliche Netzwerkgeräte wie Router, sondern auch andere internetfähige Geräte im Haushalt wie Kameras, Fernseher und Speichergeräte, sind heutzutage vernetzt und konstant online. Häufig sind sie schlecht oder gar nicht geschützt, weshalb sie ein Angriffsziel darstellen und ohne Wissen des Besitzers für böswillige Aktivitäten z. B. im Kontext von ORB-Netzwerken missbraucht werden können. Auch diese Geräte müssen daher adäquat abgesichert und bei Bekanntwerden von Schwachstellen aktualisiert werden. Das BACS veröffentlichte verschiedene Empfehlungen, um die Sicherheit dieser Geräte zu gewährleisten, siehe Cybertipp: Was beim Internet der Dinge zu beachten ist (ncsc.admin.ch).

Coathanger-Kampagne nimmt Edge-Geräte ins Visier

Das niederländische NCSC stellte im Juni 2024 einen Trend hin zu gezielten Angriffen auf Edge-Geräte wie Firewalls, VPN-Server, Routers und E-Mail-Relay-Server fest. Solche Geräte sind direkt mit dem Internet verbunden und daher auch gegenüber Angriffen exponiert. Risiken, die mit Edge-Geräten wie Firewalls oder Routern verbunden sind, wurden im Kontext der Kampagne «Coathanger» veranschaulicht. Laut dem niederländischen NCSC nutzte ein chinesischer, staatlicher Spionageakteur systematisch eine Schwachstelle in FortiGate Firewall aus, womit sich dieser in den Jahren 2022 und 2023 weltweit Zugriff auf mindestens 20'000 Geräten verschaffte. Vor der Publikation der Schwachstelle nutzte der Akteur diese während zwei Monaten als Zero-Day[139]. Abgesehen vom niederländischen Verteidigungsministerium waren mehrere andere westliche Regierungsbehörden und diplomatische Institutionen im Fokus der Kampagne. Wenn ein Ziel als interessant eingestuft wurde, installierte der Bedrohungsakteur eine Schadsoftware, um sich permanent Zugriff zu den Systemen zu verschaffen. Selbst nachdem der Hersteller die Schwachstelle entdeckt und ein Update durchgeführt hatte, erlaubte diese Schwachstelle weiterhin den Zugang.[140]

138 Router Roulette: Cybercriminals and Nation-States Sharing Compromised Networks (trendmicro.com)
139 Zero-day vulnerability (wikipedia.org)
140 Ongoing state-sponsored cyber espionage campaign via vulnerable edge devices (ncsc.nl)

Aktivitäten in Zusammenhang mit APT29

«APT29» ist ein Bedrohungsakteur mit einem breiten Set an Angriffsmöglichkeiten, die seit langem für Cyberspionage-Aktivitäten eingesetzt werden. Die Behörden verschiedener Länder gehen davon aus, dass APT29 im Auftrag des russischen Auslandsgeheimdienstes SVR operiert.[141] Für APTs typisch entwickeln sie ihre Angriffsmethoden kontinuierlich weiter, wie ein Bericht der Five-Eyes-Länder[142] aufzeigt.[143] So attackierte APT29 direkt Cloud-Infrastrukturen, um sich Zugang zu gewünschten Systemen zu verschaffen, anstatt sich vor allem auf Software-Schwachstellen bei lokalen Netzwerken zu konzentrieren. In den letzten sechs Berichtsmonaten war die Gruppe besonders aktiv und griff vor allem Unternehmen im Bereich der Informationstechnologie wie HPE[144], Microsoft[145] und zuletzt Teamviewer[146] an. APT29 hat sich darüber hinaus auf dem Gebiet der politischen Spionage hervorgetan und diplomatische Einrichtungen und Regierungen auf der ganzen Welt sowie politische Parteien ins Visier genommen. Die französische Behörde für die Sicherheit von Informationssystemen (ANSSI) teilte im Juni 2024 mit,[147] dass APT29 in der Kampagne «diplomatic orbiter» mithilfe von Spear-Phishing legitime E-Mail-Konten diplomatischer Einrichtungen kompromittierte. Darüber hinaus waren sie Anfang 2024 aktiv gegen deutsche politische Parteien.[148]

8.2 Bedrohung Industrieller Kontrollsysteme und operativer Technologie

Nicht nur im Umfeld von Daten und Informationen schreitet die Digitalisierung immer weiter voran, auch physische Prozesse und deren Steuerung werden nach und nach digitalisiert und häufig im selben Zug mit den IT-Systemen vernetzt. Die langen Lebenszyklen solcher Systeme erschweren häufig eine nachhaltige, sicher implementierte Integration in die Informations- und Kommunikationstechnologie (IKT-) Landschaft. Unachtsamkeiten bei Anpassungen an industriellen Steuerungen können ungewollt zu neuen Sicherheitsrisiken führen. Da die Manipulation eines cyberphysischen Prozesses Auswirkungen auf mechanische Anlagen bis hin zur Bedrohung von Leib und Leben haben kann, ist besondere Vorsicht geboten.

Sabotageangriffe und -versuche mit störender bis zerstörerischer Absicht werden grossmehrheitlich nur im Umfeld bereits eskalierter Konflikte beobachtet. Trotz anderweitiger Behauptung von Hacktivisten blieb die Schweiz daher – bis auf ein paar kollaterale Querschläger – von

---

141 Siehe Halbjahresbericht 2021/2 ; Kap. 4.7.3.

142 Five Eyes ist ein Sicherheitsverbund in Bezug auf nachrichtendienstliche Arbeit der folgenden fünf Länder: USA, Grossbritannien, Kanada, Australien und Neuseeland. Für mehr Informationen siehe Five Eyes (wikipedia.org) oder Five Eyes Intelligence Oversight and Review Council (FIORC) (dni.gov).

143 SVR cyber actors adapt tactics for initial cloud access (ncsc.gov.uk)

144 Hewlett Packard Enterprise tells SEC it was breached by Russia's 'Cozy Bear' hackers (therecord.media)

145 Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard (msrc.microsoft.com)

146 Teamviewer (teamviewer.com)

147 Malicious activities linked to the *Nobelium* intrusion set (cert.ssi.gouv.fr)

148 APT29 Uses WINELOADER to Target German Political Parties (cloud.google.com)

derartigen Angriffen verschont. Hacktivisten behaupten regelmässig, sie hätten im Internet exponierte industrielle Steuerungssysteme (ICS) manipuliert.[149] Unter solchen Auflistungen fanden sich auch Systeme Schweizer Organisationen, daraus resultierende Störungen sind jedoch keine bekannt.

Im Rahmen der existierenden Konflikte in der Ukraine und in Gaza[150] wurden hingegen durchaus Angriffe mit Sabotagecharakter durchgeführt. Neben destruktiven Angriffen auf verschiedene Internetanbieter in der Ukraine[151] wurden im März auch Organisationen der Energieversorgung, parallel zu Raketenangriffen, mit Cybermitteln[152] an der Bereitstellung ihrer Dienstleistungen gehindert. Um diese Angriffe durchzuführen, werden laufend neue Angriffswerkzeuge entwickelt. So wurde im Umfeld der beschriebenen Sabotagekampagnen die neue zerstörerische Wiper-Schadsoftware «AcidPour»[153] entdeckt. Eine Variante der Hintertür «Kapeka»[154] ermöglichte die Störungen der ukrainischen Energieversorgung. Diese Sabotageangriffe wurden von ukrainischen Behörden dem APT «Sandworm»[155] zugeordnet, der mit dem russischen Militärnachrichtendienst GRU in Verbindung gebracht wird.
Auch Russland war von einigen Cybersabotageakten betroffen. In Moskau wurde beispielsweise das industrielle Sensornetzwerk Moscollector angegriffen. Die Gruppe «Blackjack» nutze dabei die Schadsoftware «Fuxnet»[156], um Geräte zum Netzwerkzugang für Sensoren mit Bezug zur Notrufnummer, Flughäfen oder der Gasversorgung unbrauchbar zu machen.

Die Gefahr, dass Auswirkungen solcher Sabotageaktionen – speziell von angeblichen Hacktivisten im Umfeld von Konfliktparteien – auch ausserhalb der Kampfhandlungen Wirkung zeigen, bleibt bestehen. Dies könnten nebst Kollateralschäden auch zu Angriffen auf europäische Infrastrukturen führen, wenn Bedrohungsakteure ein Land als dem Gegner zugewandt betrachten. So warnten bereits norwegische[157] und tschechische[158] Behörden vor erhöhtem Sabotagerisiko in Europa. Ein weiteres Indiz sind Warnungen von Herstellern[159] industrieller Steuerungssysteme, dass im Internet exponierte Geräte[160] speziell bedroht werden. Sabotage-ähnliche Effekte bewirken auch Ransomware-Angriffe im Umfeld von industriellen Systemen, weshalb der Schutz gegen diese Angriffsformen zentrale Beachtung verdient.

149 Dark Web Profile: Hunt3r Kill3rs (socradar.io)
150 Bad Karma, No Justice: Void Manticore Destructive Activities in Israel (research.checkpoint.com)
151 Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs (cyberscoop.com)
152 Russian hackers target 20 energy facilities in Ukraine amid intense missile strikes (therecord.media)
153 AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine (sentinelone.com)
154 Kapeka: A novel backdoor spotted in Eastern Europe (labs.withsecure.com)
155 APT44: Unearthing Sandworm (services.google.com)
156 Unpacking the Blackjack Group's Fuxnet Malware (claroty.com)
157 Alarm over Russian-directed sabotage operations growing across Europe (therecord.media)
158 Russia is trying to sabotage European railways, Czech minister said (securityaffairs.com)
159 Security Advisory (rockwellautomation.com)
160 It appears that the number of industrial devices accessible from the internet has risen by 30 thousand over the past three years (isc.sans.edu)

Schlussfolgerung / Empfehlungen:

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

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

Um sich Angriffsversuchen durch Hacktivisten im Umfeld von Konflikten abzuwehren, haben mehrere internationale Partner ein gemeinsames Faktenblatt veröffentlicht.