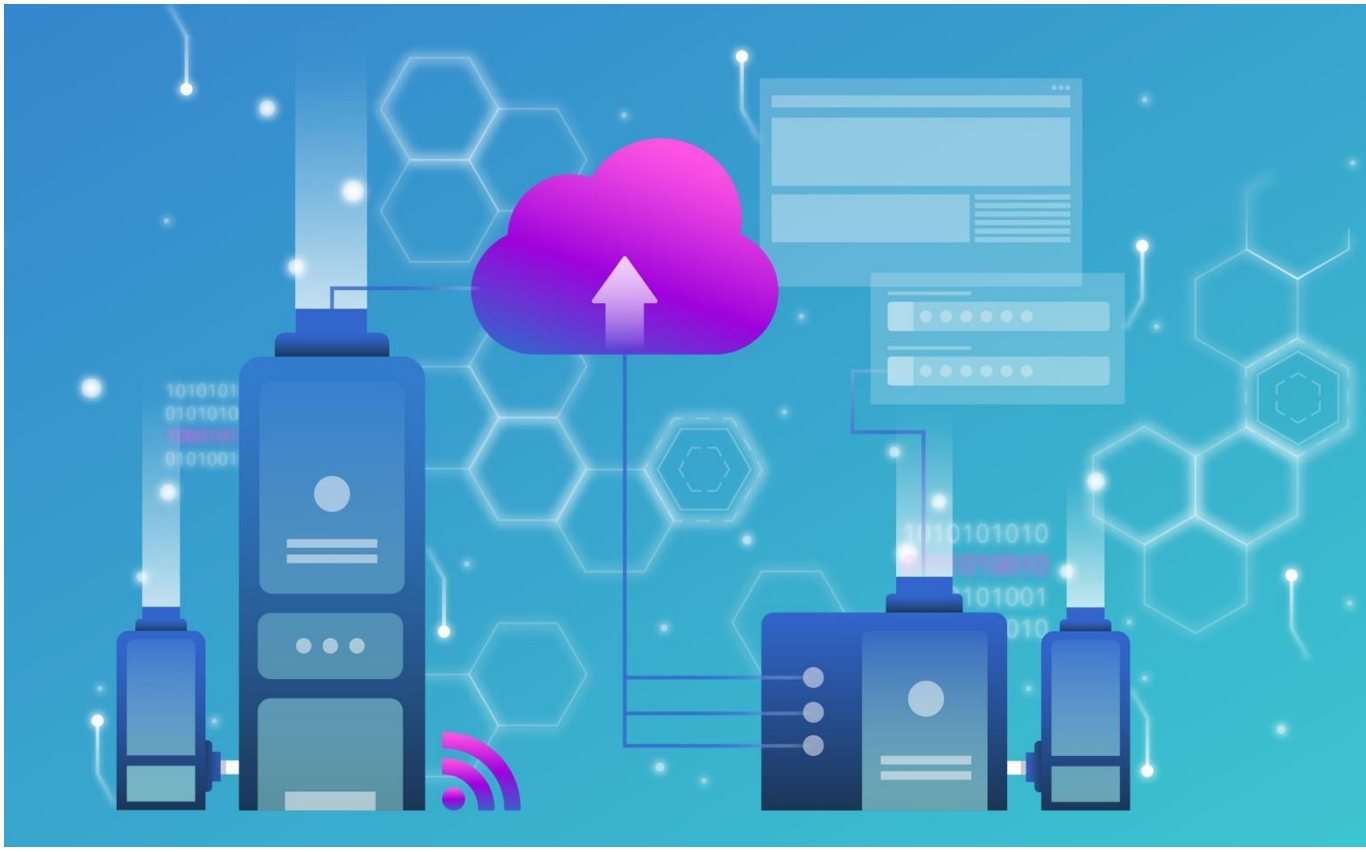
5. Mai 2022 | Nationales Zentrum für Cybersicherheit NCSC



Halbjahresbericht 2021/II (Juli – Dezember)

Informationssicherung

Lage in der Schweiz und International

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

1 Übersicht / Inhalt

Management Summary

Der vorliegende Halbjahresbericht des NCSC befasst sich mit den wichtigsten Cybervorfällen der zweiten Jahreshälfte 2021 in der Schweiz und international. Die Angriffe auf die Supply Chain von IT-Produkten bilden das Schwerpunktthema.

An der Produktion von Gütern und Dienstleistungen sind heute verschiedene Lieferanten und Drittanbieter beteiligt. Werden diese angegriffen, kann dies zu weitreichenden Problemen in der ganzen Supply Chain führen, wie beispielsweise einem Produktionsstopp. Für internationale Schlagzeilen sorgte der Supply Chain-Angriff auf das Software-Unternehmen Kaseya Mitte 2021. Ausserdem waren in der Schweiz die Internetseiten der Stadt und des Kantons St. Gallen infolge eines DDoS-Angriffs auf einen Hosting-Provider längere Zeit nicht verfügbar.

Betrugsfälle am häufigsten gemeldet

Im Berichtszeitraum erhielt das NCSC insgesamt 11'480 Meldungen zu Cybervorfällen. Am häufigsten gingen dabei Hinweise zu verschiedenen Betrugsformen ein. Insbesondere E-Mails, die angeblich von Strafverfolgungsbehörden stammen, wurden sehr häufig gemeldet. Weitere Meldungen betrafen Vorschussbetrug, Investment-Betrug, CEO-Betrug und Kleinanzeigen-Betrug. Bei Betrug zeichnet sich bei einigen Täterschaften ein Trend zu aufwändigerem, individualisierten Vorgehen ab. Sie bearbeiten Opfer über längere Zeit, um Vertrauen aufzubauen, bevor der eigentliche Betrugsversuch stattfindet.

Ransomware und Datenabfluss

Auch in der zweiten Jahreshälfte 2021 gab es zahlreiche Angriffe mit Verschlüsselungstrojanern, sogenannter Ransomware, bei denen Daten verschlüsselt und anschliessend Lösegeld gefordert wurde. Immer öfter gehen die Angreifer zur doppelten Erpressung über. Sie kopieren die Daten, bevor diese verschlüsselt werden. So verfügen die Angreifer über ein zusätzliches Druckmittel. Falls das Opfer nicht zur Zahlung des geforderten Lösegeldes bereit ist, drohen sie mit der Veröffentlichung der Daten.

Schwachstellen in Software-Komponenten

Häufig werden in der Software-Entwicklung bereits bestehende Komponenten wie Bibliotheken oder Open Source Code verwendet. Diese können jedoch auch Schwachstellen aufweisen. Wird eine solche Schwachstelle bekannt, muss sie in allen Produkten, in denen die Komponente mit der Schwachstelle integriert wurde, behoben werden. Diese Problematik zeigte sich im Dezember 2021 bei der kritischen Schwachstelle in der weit verbreiteten Java-Programmbibliothek «Log4j».

Phishing weiterhin im Trend

Seit Beginn der Pandemie werden dem NCSC viele Phishing-Angriffe mit vermeintlichen Paketankündigungen oder Zustellproblemen gemeldet. Neben E-Mails versenden die Angreifer auch regelmässig SMS, um ihre Opfer zu erreichen. Andere Meldungen betrafen Phishing-Versuche in Zusammenhang mit Webmail und Office365. Die so gephishten Zugangsdaten werden in der Folge oft für Rechnungsmanipulationsbetrug verwendet. Ein weiterer Dauerbrenner sind Phishing-Mails bezüglich angeblich doppelt bezahlter Rechnungen von Internetprovidern.

2 Editorial

No man is an island

Der englische Schriftsteller John Donne hat in seinem 1624 erschienenen «Devotions»-Werk die Phrase «no man is an island» geprägt. Der Poet wollte damit zum Ausdruck bringen, dass jeder von uns Teil eines grossen Ganzen ist und sein Schicksal mit jenem seiner Mitmenschen teilt.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid AG

Unser wirtschaftliches Umfeld ist geprägt von anhaltender Spezialisierung und damit verbundener Reduktion der Fertigungstiefe zwecks Effizienzsteigerung und Kostenreduktion durch Skaleneffekte. Dadurch wird die Wertschöpfungskette von Unternehmen zunehmend von Zulieferern, Dienstleistern und Partnern abhängig – auch wenn uns die Corona-Pandemie die Grenzen und Risiken dieser globalen Arbeitsteilung vor Augen geführt hat.

Gerade wenn es um Cyberangriffe gegen Unternehmen geht, teilen alle Beteiligten einer Lieferkette ein gemeinsames Schicksal: Ein Cyberangriff auf einen Zulieferer kann Auswirkungen auf seine Abnehmer und in der Folge wiederum auf die Empfänger von deren Leistungen haben. So musste etwa Toyota im Februar dieses Jahres seine japanischen Fabriken vorübergehend schliessen, nachdem ein Zulieferer aufgrund eines Cyberangriffs ausgefallen war. Die Metapher «no man is an island» lässt sich auch auf Organisationen übertragen.

Die Problematik wird dadurch verstärkt, dass Cyberakteure damit begonnen haben, Lieferketten direkt anzugreifen: Wenn Akteure beispielsweise die Produkte von Anbietern von Netzwerkgeräten mit Backdoors versehen, um durch diese Hintertüren später deren Kunden anzugreifen (wie im Falle des Angriffs auf das texanische Unternehmen SolarWinds unlängst geschehen), erzielen sie damit einen Multiplikationseffekt.

Sich selbst nicht zu schützen, heisst potenziell also auch, andere mit zu gefährden.
In Gesprächen stelle ich immer wieder fest, dass das Risikomanagement der Lieferkette in vielen Unternehmen nur zaghaft angegangen wird.

Wenn man sich das Ausmass der Vernetztheit und der gegenseitigen Abhängigkeiten vergegenwärtigt, dann blicken wir hier womöglich auf das grösste systemische Cyberrisiko unserer modernen Gesellschaft!

Es stellt sich die Frage, warum dieses Thema keine grössere Aufmerksamkeit geniesst. Eine mögliche Erklärung könnte darin liegen, dass Führungsverantwortliche von Unternehmen beim Auslagern von Leistungen versuchen, auch die damit verbundenen Verantwortungen zu übertragen. Daraus ergibt sich ein blinder Fleck: Denn während ich mittels Outsourcings zwar die Verantwortung für die Leistungserbringung (responsibility) auslagern kann, verbleibt die Rechenschaftspflicht (accountability) gegenüber meinen Anspruchsgruppen in jedem Fall bei mir. Und wie kann ich die Rechenschaftspflicht gegenüber meinen Stakeholdern wahrnehmen, wenn ich die durch Auslagerungen entstehenden Risiken meiner Lieferkette nicht kontrolliere?

Aus meiner Sicht muss das Risikomanagement der Lieferkette fester Bestandteil des operativen Managements jedes Unternehmens sein.

Ein systematisches Risikomanagement der Lieferkette fusst darin, die entsprechenden Risiken zu identifizieren und zu verstehen. Hierbei kann eine Analyse der Kernprozesse helfen, kritische Abhängigkeiten zu Drittparteien zu erkennen. Auch können Threat Modeling Methoden wie STRIDE dabei helfen, Bedrohungen und Schwachstellen an Systemübergängen zu ermitteln.

Grosse Bedeutung kommt auch dem Aufbau einer resilienten Organisation zu. Wenn es mir gelingt, meine Kernprozesse mit alternativen Mitteln weiterzuführen, wenn etwa die primäre IT ausfällt (Business Continuity Management) oder wenn ich Vorkehrungen getroffen habe, die Auswirkungen eines Angriffs einzudämmen und nach einem Ausfall von ICT oder OT Mitteln deren Wiederaufbau in kurzer Zeit zu vollziehen (Incident Response und Disaster Recovery), dann leiste ich damit auch einen unmittelbaren Beitrag zur Resilienz der gesamten Lieferkette, in welcher mein Unternehmen eine Rolle spielt.

Diese Vorkehrungen müssen in den Unternehmen regelmässig getestet und mit der Belegschaft wiederkehrend eingeübt werden, sollen sie im Ernstfall wirksam sein.

Auch können branchenweite Normen sowie Zertifizierungen von Produkten und Leistungen einen positiven Beitrag leisten. Hierzu ist es notwendig, dass die Unternehmen einer Branche sich zusammenschliessen, um solche Normen und Vorgaben gegenüber ihren Zulieferern auch durchsetzen zu können.

Wollen wir den sich kontinuierlich ausgefeilter organisierenden Cyberakteuren wirkungsvolle Mittel entgegensetzen, müssen alle Unternehmen den Cyberrisiken in ihren Lieferketten angemessen entgegenwirken.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid AG

3 Fokus: Supply Chain-Angriffe

3.1 Was ist ein Supply Chain-Angriff?

Zahlreiche Unternehmen arbeiten mit einer Vielzahl von Partnern (Lieferanten, Drittanbieter) zusammen. Diese liefern verschiedene Produkte wie Rohstoffe, Dienstleistungen oder Technologien zu, aus denen danach ein Endprodukt erzeugt wird oder die in Angebote oder Dienstleistungen weiterverarbeitet werden. Viele Unternehmen sind dadurch von externen Leistungen abhängig, um ihren Betrieb aufrecht zu erhalten. Diese Liefer- oder Versorgungskette, auch Supply Chain genannt, beinhaltet im grösseren Kontext die ganze Wertschöpfungskette. Jedes Glied in dieser Kette ist in den Gesamtprozess integriert und kann potenziell als Eintrittsvektor für Angreifer dienen (Angriff *über* die Lieferkette). Auch kann die Kette durch punktuelle Störungen unterbrochen werden (Angriff *auf* die Lieferkette). Um Cyberangriffe zu verhindern, muss deshalb die ganze Supply Chain und somit alle involvierten Lieferanten und Dienstleister angemessen geschützt sein, zuverlässig funktionieren, und wenn möglich die Kontinuität durch Redundanzen sichergestellt sein.

Ein Angriff über eine Lieferkette ist eine Kombination aus zwei Angriffen. Der erste Angriff richtet sich gegen einen einzelnen Lieferanten. Der Zugang zu dessen Systemen und seine privilegierte Beziehung zu seinen Kunden wird genutzt, um das eigentliche Ziel anzugreifen. Dies erfolgt in einfachen Fällen durch schlecht geschützte Fernzugriffe, Netzwerkübergänge oder etablierte Datenübertragungsverbindungen. Im Rahmen von aufwendigen Operationen haben Angreifer auch schon in die Software-Entwicklung bei Unternehmen eingegriffen und dort einen Code platziert, der dann via reguläre Updates zu den Kunden ausgeliefert wurde.[1] Vorstellbar sind auch Angriffe auf Soft- oder Hardware während des Herstellungsprozesses. Entsprechend wird das Produkt dann mit einer Schwachstelle, einer Hintertür oder mit vorinstallierter Schadsoftware ausgeliefert. Angriffe über die Lieferkette können ein ganz bestimmtes hochwertiges Ziel haben[2], einen beschränkten Adressatenkreis anvisieren[3] oder breit Wirkung entfalten, damit nachher einzelne Ziele spezifisch ausgewählt werden können.[4] Zudem können über die Lieferkette auch Angriffe gegen eine möglichst grosse Anzahl potenzieller Opfer ausgeführt werden, zum Beispiel mit der Verbreitung von Ransomware nach der Kompromittierung eines IT-Dienstleisters.[5]

Angriffe auf die Lieferkette mit der Absicht, den Betrieb von spezifischen Endkunden zu stören, sind häufig nicht klar zuzuweisen.

---

1 Siehe hierzu den Halbjahresbericht 2020/2 (ncsc.admin.ch), Kap. 4.2.7 zu Solarwinds.

2 Siehe Halbjahresbericht 2010/2 (ncsc.admin.ch), Kap. 4.1 zu «Stuxnet», mit dem gezielt die iranische Uranananreicherung sabotiert wurde.

3 Siehe Halbjahresbericht 2017/1 (ncsc.admin.ch), Kap. 3 zu «NotPetya», der via ukrainische Steuererklärungssoftware verbreitet wurde.

4 Siehe Halbjahresbericht 2020/2 (ncsc.admin.ch), Kap. 4.7.2 zum Solarwinds-Hack und Halbjahresbericht 2017/1 (ncsc.admin.ch), Kap. 5.1.1 zur Operation «CloudHopper».

5 Siehe Kap. 3.3 hiernach und unten Kap. 4.2.2.

DDoS-Angriffe auf den DNS-Anbieter Dyn im Jahr 2016 führten dazu, dass verschiedene Plattformen (u. a. Twitter, Spotify, Soundcloud), die dessen Dienste nutzten, für eine Vielzahl von Kunden nicht erreichbar waren.[6] Unternehmen in der Lieferkette haben typischerweise Verträge mit ihren Kunden bezüglich Leistungen oder Lieferungen. In jüngster Zeit gab es diverse Ransomware-Angriffe auf Dienstleister und Lieferanten. Diese stehen unter enormem Druck, ihre Leistungen wieder anbieten oder Produkte produzieren zu können, da sie den Verpflichtungen gegenüber ihren Kunden nachkommen müssen. Die Erpresser erhoffen sich dadurch, dass das Opfer eher bereit ist, Lösegeld zu bezahlen.

3.2 Ransomware-Attacke auf Supply Chain der VSA-Software von Kaseya

Kaseya Limited ist ein Software-Dienstleister, der sich auf Tools für die Fernüberwachung und -verwaltung von Systemen spezialisiert hat. Er bietet seinen Kunden VSA-Software (Virtual System/Server Administrator) zum Herunterladen an, die auch über seine eigenen Cloud-Server funktioniert. Managed Service Providers (MSPs) können die VSA-Software vor Ort nutzen oder die VSA-Cloud-Server von Kaseya lizenzieren. MSPs bieten ihrerseits anderen Kunden verschiedene IT-Dienstleistungen an. Bei Aktualisierungen der Software kann Kaseya Remote-Updates an alle VSA-Server senden.

Mitte 2021 nutzten Angreifer eine Zero-Day-Schwachstelle in Kaseyas eigenen Systemen aus (CVE-2021-30116)[7], um aus der Ferne schädliche Befehle auf den VSA-Appliances der Kunden von Kaseya auszuführen. So wurde am 2. Juli 2021 ein Update an die VSA der Kaseya-Kunden verteilt, das den Code der Angreifer ausführte. Dieser bösartige Code setzte wiederum Ransomware bei den Kunden ein, die von dieser VSA verwaltet wurden.[8]

In der Folge haben amerikanische Behörden einen Leitfaden für MSPs und deren Kunden herausgegeben, die von der Ransomware-Attacke auf die VSA-Supply Chain von Kaseya betroffen sind.[9]

3.3 Vorfälle in der Schweiz

Mehrere KMUs waren Anfang September 2021 von der Ransomware «BlackMatter» betroffen, nachdem es Angreifern gelungen war, einen österreichischen IT-Provider zu kompromittieren und dessen Kunden anzugreifen.[10] Durch DDoS-Angriffe auf eine Hosting-Firma, welche u. a. die Website des Kantons St. Gallen[11] beherbergt, wurden mehrere Webauftritte temporär gestört (vgl. unten Kap. 4.3.1).

---

6 Siehe Halbjahresbericht 2016/2 (ncsc.admin.ch), Kap. 3.2, 4.4.1 und 4.6.

7 CVE - CVE-2021-30116 (mitre.org)

8 REvil ransomware hits 1,000+ companies in MSP supply-chain attack (bleepingcomputer.com); siehe auch Kap. 4.2.2.

9 CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack (cisa.gov)

10 Hackerangriff auf 34 Firmen (orf.at)

11 Website des Kantons wieder online (sg.ch)

3.4 Vorstösse und Massnahmen

Auf politischer Ebene wurde Ende 2021 im Bericht[12] des Bundesrates in Erfüllung der Postulate Dobler 19.3135[13] und 19.3136[14] die Thematik Supply Chain Risk Management (SCRM) thematisiert und eine Auslegung der anwendbaren nationalen Regeln und internationalen Standards gemacht. Zudem wurden die rechtlichen Grundlagen für die Anwendung von Standards bei kritischen Infrastrukturen durchleuchtet.

Der Bericht geht auch auf Forderungen aus dem Diskussionspapier «Supply Chain Security»[15] einer Arbeitsgruppe der Kommission Cybersecurity von ICTswitzerland ein, die u. a. Prüfzentren in der Schweiz für Hard- und Softwarekomponenten vorsehen. Der Bund ist bereit, private Initiativen in diesem Bereich mit Fachwissen zu unterstützen.[16]

Schlussfolgerung / Empfehlungen:

Eine regelmässige Überprüfung der Lieferanten- und Dienstleisterbeziehungen gegenüber dem sich entwickelnden Risikoprofil stellt bei fortschreitender Digitalisierung sämtlicher Geschäftsbereiche eine dringliche Herausforderung für Unternehmensführungen dar.

Für kleinere Organisationen ohne eigene Spezialisten bleibt fast nur die Möglichkeit, die Risiken mit externer Unterstützung aus Verbänden oder spezialisierten Beratern vertraglich abzusichern, inklusive dem Recht, die Dienstleister auch unabhängig überprüfen zu lassen. Dieser Mehraufwand bringt zwangsläufig höhere Kosten mit sich und lohnt sich nur da, wo auch ein erhöhtes Risiko für die Organisation besteht.

Das NCSC des Vereinigtes Königreichs (NCSC-UK) bietet auf seiner Website eine Wegleitung[17] und einen Fragenkatalog[18] an, der den Priorisierungsprozess und die Auswahl unterstützen kann.

Die amerikanische Cybersicherheitsbehörde CISA bietet ebenfalls viele Informationen[19] zu Risiken im Zusammenhang mit der Versorgungskette.

Auf der Website des NCSC finden Sie zudem Empfehlungen für die Zusammenarbeit mit IT-Providern (ncsc.admin.ch).

12 Produktesicherheit und Supply Chain Risk Management in den Bereichen Cybersicherheit und Cyberdefence (parlament.ch)
13 Haben wir die Cybersicherheit bei Beschaffungen der Armee im Griff? (parlament.ch)
14 Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff? (parlament.ch)
15 White_Paper_Supply_Chain_Security_2019_09_25_DE.pdf (digitalswitzerland.com)
16 Siehe dazu Halbjahresbericht 2020/2 (ncsc.admin.ch), Kap. 4.5.2.
17 Supply chain security guidance (ncsc.gov.uk)
18 Supplier assurance questions (ncsc.gov.uk)
19 Supply Chain (cisa.gov)

3.5 Schwachstellen in Software-Komponenten

Die meisten Software-Produkte werden nicht von Grund auf und komplett neu geschrieben. Bei der Software-Entwicklung werden häufig bereits bestehende Bibliotheken oder Open Source Code integriert. Dies führt dazu, dass mit diesen Bestandteilen unabsichtlich auch enthaltene Schwachstellen integriert und verbreitet werden. Wenn eine solche Schwachstelle bekannt wird, muss sie in allen Produkten, in denen die Komponente mit der Schwachstelle vorkommt, behoben werden. Dies wurde spätestens 2014 offensichtlich, als die «Heartbleed»-Lücke weltweit für Aufsehen sorgte.[20]

Im Dezember 2021 wurde eine Schwachstelle in der weit verbreiteten Java-Programmbibliothek «Log4j»[21] bekannt, welche global als kritisch eingestuft wurde. «Log4j» ist ein Programmiergerüst (Framework), das dem Protokollieren von Anwendungsmeldungen dient und einen substanziellen Bestandteil in der heutigen Software-Entwicklung darstellt. Folglich wird es in vielen kommerziellen und Open Source Software-Produkten eingesetzt.[22] Die Sicherheitslücke ermöglicht es, aus der Ferne beliebigen Code auszuführen (Remote Code Execution, RCE), was kurz nach Bekanntwerden bereits breitflächig international durch Cyberkriminelle ausgenutzt wurde. Vgl. hierzu Kap. 4.5.3.

4 Ereignisse / Lage

4.1 Eingegangene Meldungen zu Cybervorfällen – Überblick

Mit der stattlichen Anzahl von 21'714 Meldungen hat das NCSC im Jahr 2021 rund doppelt so viele Meldungen erhalten als im Vorjahr (10'833). Ein Grund für diese starke Zunahme dürfte unter anderem sein, dass das NCSC-Meldeformular Ende 2020 erneuert und vereinfacht wurde, sowie seither auch prominenter auf der Startseite platziert ist. Bei einzelnen Phänomenen gab es aber auch eine deutliche Steigerung, die ebenfalls zu dieser Zunahme beigetragen haben.

Bei vielen der gemeldeten Vorfälle handelt es sich um erkannte Angriffsversuche und nicht um erfolgreiche Angriffe. Zudem ist von einer nicht unerheblichen Dunkelziffer insbesondere bei nicht erfolgreichen Versuchen auszugehen, da in der Schweiz keine generelle Meldepflicht besteht.

---

20 Siehe Halbjahresbericht 2014/1 (ncsc.admin.ch), Kap. 4.1.

21 Log4j – Apache Log4j Security Vulnerabilities (apache.org)

22 New zero-day exploit for Log4j Java library is an enterprise nightmare (bleepingcomputer.com)

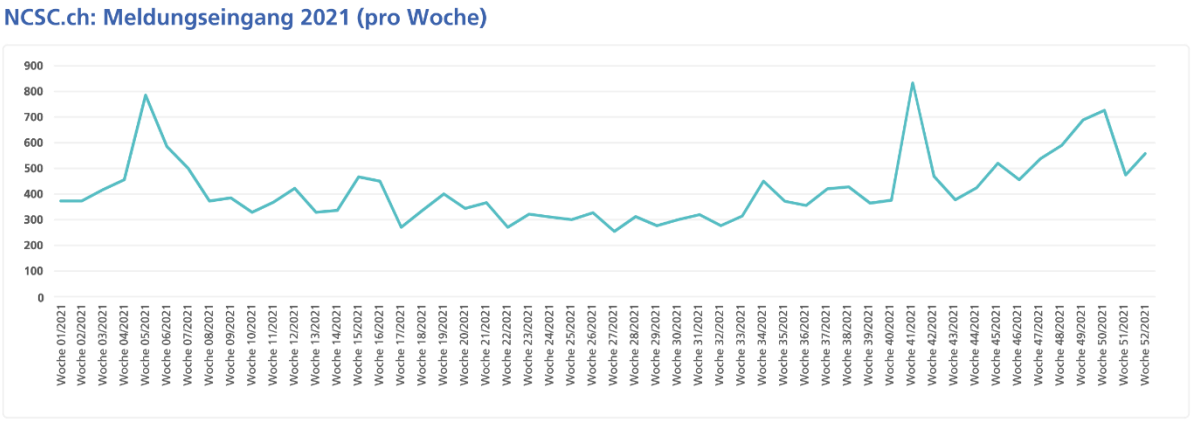


Abb. 1: Anzahl Meldungen pro Woche beim NCSC vom Januar bis Dezember 2021, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

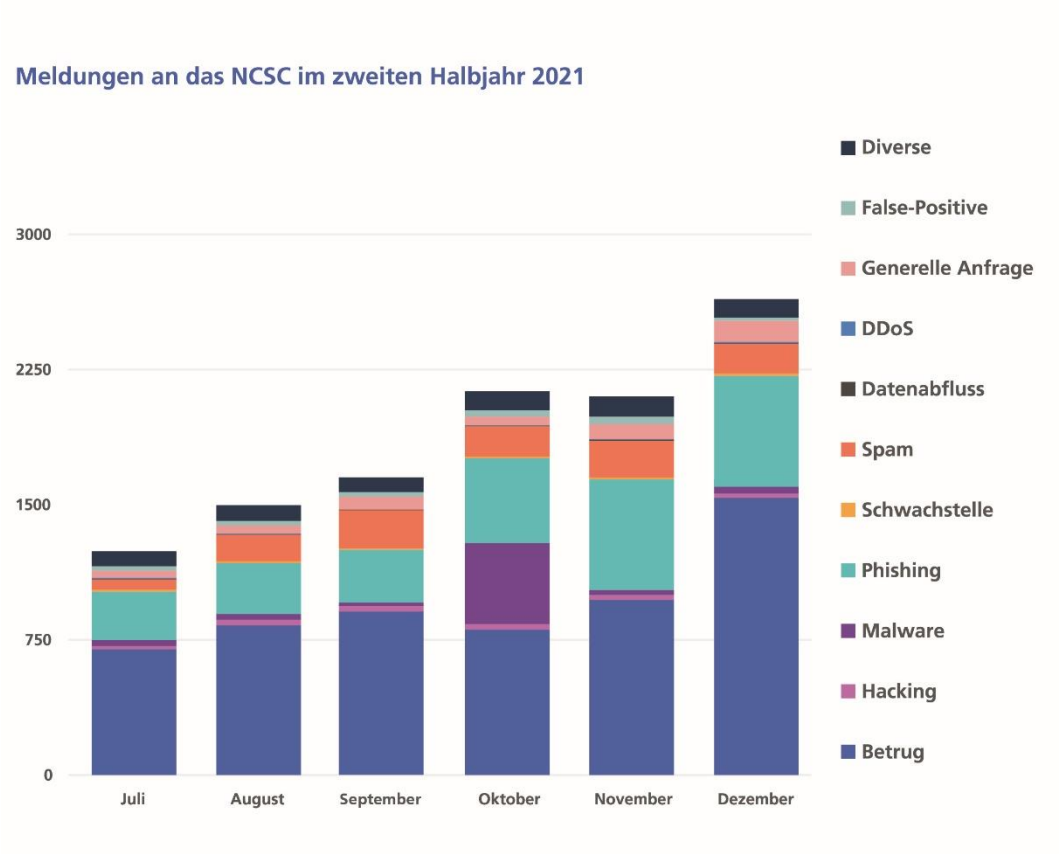


Abb. 2: Meldungen an das NCSC im zweiten Halbjahr 2021 nach Kategorien, siehe auch Aktuelle Zahlen (ncsc.admin.ch).

4.1.1 Am häufigsten gemeldet: Betrug

Wie auch im vorangehenden Jahr wurden dem NCSC im Jahr 2021 am häufigsten Betrugsversuche gemeldet. Insgesamt waren dies über 11'300 Hinweise. Während Fake Sextortion[23]

[23] Fake Sextortion (ncsc.admin.ch)

in der ersten Jahreshälfte dominant war und zahlreiche Wellen beobachtet wurden, nahmen die Meldungen zu diesem Phänomen in der zweiten Jahreshälfte tendenziell ab. Dafür nahmen ab Oktober Meldungen zu Drohmails stark zu, welche vortäuschten, von Strafverfolgungsbehörden zu stammen und die Bezahlung einer Busse oder Kaution forderten.[24] Dieses bereits seit längerem aus Frankreich bekannte und mit Fake Sextortion verwandte Phänomen machte in den Monaten November und Dezember 2021 den grössten Anteil der Meldungen aus und führte zu einem starken Anstieg der Gesamtmeldungen. Weitere Kategorien mit hohem Meldeeingang im Jahr 2021 waren Hinweise zu Vorschussbetrug (2'704), Investment-Betrug (397), CEO-Betrug (394) und Kleinanzeigen-Betrug (820). Gemäss den Meldungen zum Kleinanzeigen-Betrug hat sich in diesem Bereich vor allem die Variante durchgesetzt, bei der der Verkäufer trotz eines Verkaufes für einen angeblichen Transport noch Gebühren vorschiessen soll.[25]

In der Rubrik Investment-Betrug wurden neben den klassischen Varianten[26] auch sogenannte Give Away-Aktionen gemeldet. Wenn ein Betrag auf eine bestimmte Cryptowallet-Adresse einbezahlt werde, so werde anschliessend der doppelte Betrag zurückbezahlt. Auf der angegebenen Website wird der Besucher unter Druck gesetzt, indem ein Zähler eingeblendet wird, welcher anzeigt, wieviel Geld und Zeit noch für die Werbeaktion zur Verfügung stehe.

4.1.2 Meldungen zu Phishing

Meldungen zu Phishing E-Mails bleiben auch im Jahr 2021 hoch. Dominant sind hierbei vor allem die E-Mails mit den falschen Paketankündigungen im Namen der diversen Paketdienstleister oder der Eidgenössischen Zollverwaltung, die irgendwelche Gebühren verlangen. Diese E-Mails gibt es in zahlreichen Varianten. In einigen Fällen soll eine Paysafe-Karte gekauft und der Code an die Betrüger gesendet werden, in anderen Fällen führt der Link auf eine Abofalle. Am häufigsten führen diese E-Mails aber auf eine Phishing-Webseite, auf welcher Kreditkartendaten angegeben werden sollen.

Ein Dauerbrenner in der Kategorie Phishing sind die angeblich doppelt bezahlten Rechnungen von Internetprovidern. Dabei nehmen es die Angreifer mit den jeweils angegebenen Daten allerdings nicht immer sehr genau. Die Frist für die Reaktion, welche die Empfängerin oder den Empfänger eigentlich unter Druck setzen sollte, lag in einigen Fällen fast ein halbes Jahr zurück.

Auch Phishing-Versuche gegen Webmail und Office365 wurden beobachtet. Gerade solche Zugangsdaten werden häufig verwendet, um einen Rechnungsmanipulationsbetrug (BEC) durchzuführen. Bei dieser Betrugsform wird jeweils auf eine bestehende E-Mail-Kommunikation Bezug genommen, die eine Zahlungsanweisung oder eine Rechnung enthält. Die Betrüger ändern dabei die IBAN-Nummer, auf die der Betrag einbezahlt werden soll. Da die Angreifer in diesen Fällen Zugriff auf das E-Mail-Konto des Senders oder eines Empfängers erlangen,

---

[24] Die Woche 37 im Rückblick (ncsc.admin.ch)

[25] Siehe auch unten Kap. 5.2.

[26] Siehe Investmentbetrug (ncsc.admin.ch) und Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 4.8.

haben sie auch Zugriff auf die entsprechende interne Firmenkommunikation oder Kommunikation mit Kunden. Darunter können sich vertrauliche Informationen befinden. Dies eröffnet den Angreifern weitere Betrugsmöglichkeiten und ein Opfer kann mit diesen Daten zusätzlich erpresst werden.

4.1.3 Meldungen zu Schadsoftware / Malware

In der Rubrik Schadsoftware betrafen fast die Hälfte der Meldungen die Schadsoftware «FluBot».[27] Verantwortlich dafür war eine Welle in den Wochen 41 und 42, bei der die Empfänger mit einem SMS dazu verleitet werden sollten, eine bösartige Android-App, welche die Schadsoftware «FluBot» enthielt, auf ihrem Mobiltelefon zu installieren. Diese Welle führte in der Woche 41 zum höchsten Meldeeingang des Jahres.

Meldungen zu Ransomware sind ebenfalls überproportional angestiegen. Im Vergleich zum letzten Jahr mit 67 Meldungen hat das NCSC im Jahr 2021 161 Meldungen zu Ransomware erhalten. Im Frühjahr wurden dem NCSC beispielsweise zahlreiche Angriffe mit der Ransomware «Qlocker» gegen Netzwerkspeicher (NAS) gemeldet, welche vor allem bei Privatpersonen im Einsatz sind. Insgesamt gingen im vergangenen Jahr 44 gemeldete Fälle auf das Konto von «Qlocker».[28]

Auch Angriffsversuche mit der Schadsoftware «Retefe» sind immer noch aktuell und werden regelmässig gemeldet. Entsprechende E-Mails sind oftmals begleitet von einem Telefonanruf von einer Firma Swiss Express Service (oder ähnlich), welche die Versandpapiere visieren lassen will. Im Verlauf des Telefongesprächs wird mitgeteilt, dass die Papiere per E-Mail zugestellt würden. Der Link im E-Mail respektive im angehängten PDF-Dokument führt dann zu Schadsoftware – meist einem E-Banking-Trojaner.

4.1.4 Meldungen zu Schwachstellen

In der Kategorie Schwachstelle wurden neben der «Log4j»-Schwachstelle[29] im vergangenen Jahr vor allem Meldungen im Zusammenhang mit Exchange-Servern verzeichnet.[30] Diese Schwachstellen werden beispielsweise ausgenutzt, um Schadsoftware zu verteilen. Dabei werden gestohlene E-Mails mit Links auf Schadsoftware angereichert und dann erneut an die Empfängerin oder den Empfänger versendet. Aufgrund der vertrauten Kommunikation soll auf diese Weise das potenzielle Opfer zum Öffnen eines Dokumentes verleitet werden. Die Office-Dokumente enthalten ein bösartiges Makro, inklusive Anleitung, wie man die Einstellungen so anpassen kann, dass das Makro auf dem Rechner ausgeführt wird. Der beste Schutz vor solchen Angriffen ist also, keine Makros auszuführen, auch wenn man explizit und mit Nachdruck dazu aufgefordert wird.

---

27 Vgl. Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 4.2.1 sowie unten Kap. 4.2.1.
28 Vgl. Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 4.1.3.
29 Siehe unten Kap. 4.5.3.
30 Siehe Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 3.1.1.

4.2 Schadsoftware / Malware

4.2.1 Generelle Lage

In der zweiten Jahreshälfte 2021 war das Medieninteresse an Ransomware besonders ausgeprägt, obwohl Ransomware nur einen kleinen Teil aller Angriffe mit Malware ausmachen. Grund dafür war, dass in der Schweiz und im Ausland zahlreiche dieser Angriffe schwerwiegende Folgen für die Opfer hatten (siehe Kap. 4.2.2). Um Ransomware erfolgreich einzusetzen, braucht der Angreifer zuerst einen Zugang zum Zielsystem. Dieser Zugang erfolgt hauptsächlich über andere Malware, die darauf spezialisiert ist, sich zu verbreiten und sich in Systemen einzunisten. Eine solche Schadsoftware ist «Qakbot», auf die in Kapitel 4.2.3 näher eingegangen wird. Die weit verbreitete Malware «Emotet» hatte Anfang 2021 einen Rückschlag erlitten, als es mit einer internationalen Polizeiaktion gelang, die «Emotet»-Infrastruktur zu zerschlagen.[31] «Emotet» meldete sich Ende 2021 jedoch wieder zurück.[32] Möglich gemacht hatte dies die schon früher im Zusammenhang mit «Emotet» aufgetretene Malware «Trickbot». Während in der Vergangenheit «Emotet» «TrickBot» installierte, nutzte «Emotet» nun «Trickbot» für den Wiederaufbau seiner Infrastruktur. Solche Interaktionen sind nicht zuletzt auf die Entwicklung des «Malware-as-a-Service»-Modells zurückzuführen.[33] Dabei vermieten Malware-Entwickler respektive Botnetz-Betreiber ihre Infrastruktur an andere Kriminelle. So kann sich jeder Akteur auf bestimmte Teilleistungen spezialisieren und diese auf dem Untergrundmarkt anbieten.

---

31 World's most dangerous malware EMOTET disrupted through global action (europa.eu); Halbjahresbericht 2020/2 (ncsc.admin.ch), Kap. 4.3.2.

32 Emotet malware is back and rebuilding its botnet via TrickBot (bleepingcomputer.com)

33 Malware-as-a-service is the growing threat every security team must confront today (securitymagazine.com); Malware-as-a-service (MaaS) (kaspersky.com); Malware Has Evolved: Defining Malware-as-a-Service (zerofox.com)

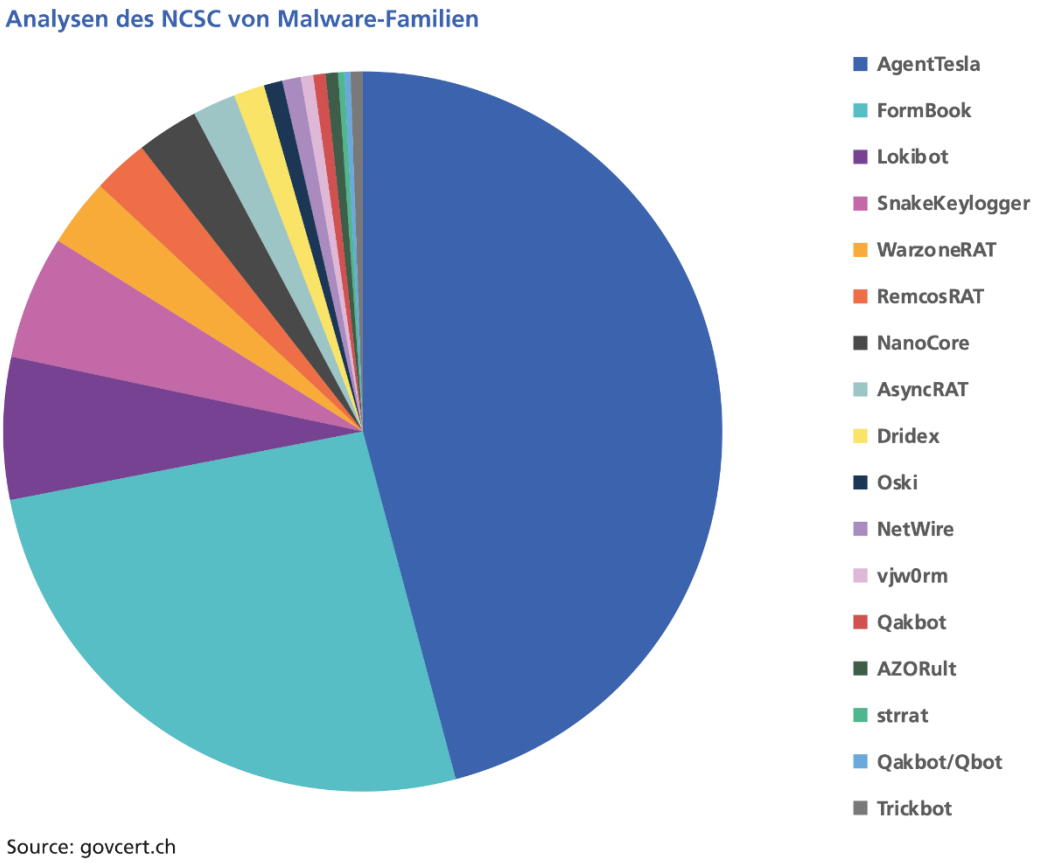


Abb. 3: Analysen des NCSC von Malware-Familien in der Schweiz im zweiten Halbjahr 2021.

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

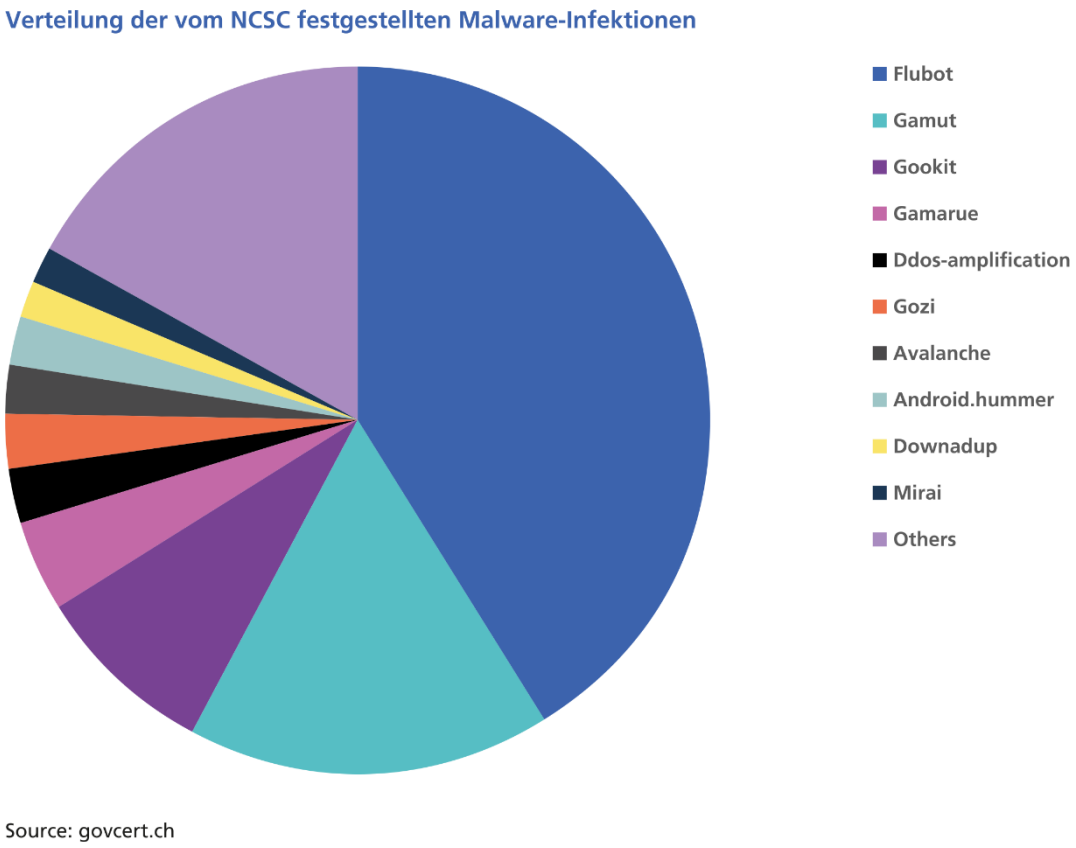


Abb. 4: Verteilung der vom NCSC festgestellten Malware-Infektionen in der Schweiz im zweiten Halbjahr 2021.

Platz 1 der am stärksten verbreiteten Malware-Familien belegte wie in der ersten Jahreshälfte auch im zweiten Halbjahr 2021 «Flubot». Um diese Malware für Android-Geräte zu verbreiten, versenden die Kriminellen SMS mit einem Link zu einer angeblichen Sprachnachricht. Der Link führt zu einer vermeintlichen App, die installiert werden müsse, um die Sprachnachricht abzurufen. Statt einer Sprachnachricht holt sich das Opfer damit jedoch «Flubot» auf sein Gerät. In der Folge können die Angreifer Daten auf dem Gerät stehlen und unter anderem auf Anwendungen, die durch einen zweiten Faktor geschützt sind, zugreifen sobald der zweite Faktor per SMS versandt wird. Es können aber auch die E-Banking-Aktivitäten des Opfers ausspioniert werden.[34]

Schlussfolgerung / Empfehlungen:

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

[34] FluBot (Malware Family) (fraunhofer.de); Die Woche 41 im Rückblick (ncsc.admin.ch)

- Falls Sie dennoch eine solche App installiert haben, sollten Sie das Gerät von einer Fachperson überprüfen lassen und bis dahin damit weder Bankgeschäfte noch Online-Einkäufe tätigen und keine Passwörter eingeben.
- Das Zurücksetzen des befallenen Geräts auf die Werkeinstellungen ist nahezu die einzige Möglichkeit, diese Schadsoftware vom Gerät zu entfernen.

Auf Platz 2 ist der Spambot «Gamut» anzutreffen. Mit «Gamut» infizierte Geräte werden in ein Botnetz eingebunden und verwendet, um Spam Mails zu verschicken, meist zu Themen wie intime Begegnungen, Pharmaprodukte oder Jobmöglichkeiten.[35]

Dahinter folgt auf Platz 3 der Infostealer «Gootkit». Diese Malware ist darauf spezialisiert, Bankdaten des Opfers zu stehlen. Um ihre Opfer zu erreichen, benutzt sie neben Spam-Kampagnen kompromittierte Internetseiten, die die Besucher zum Herunterladen der Schadsoftware verleiten.[36]

4.2.2 Ransomware

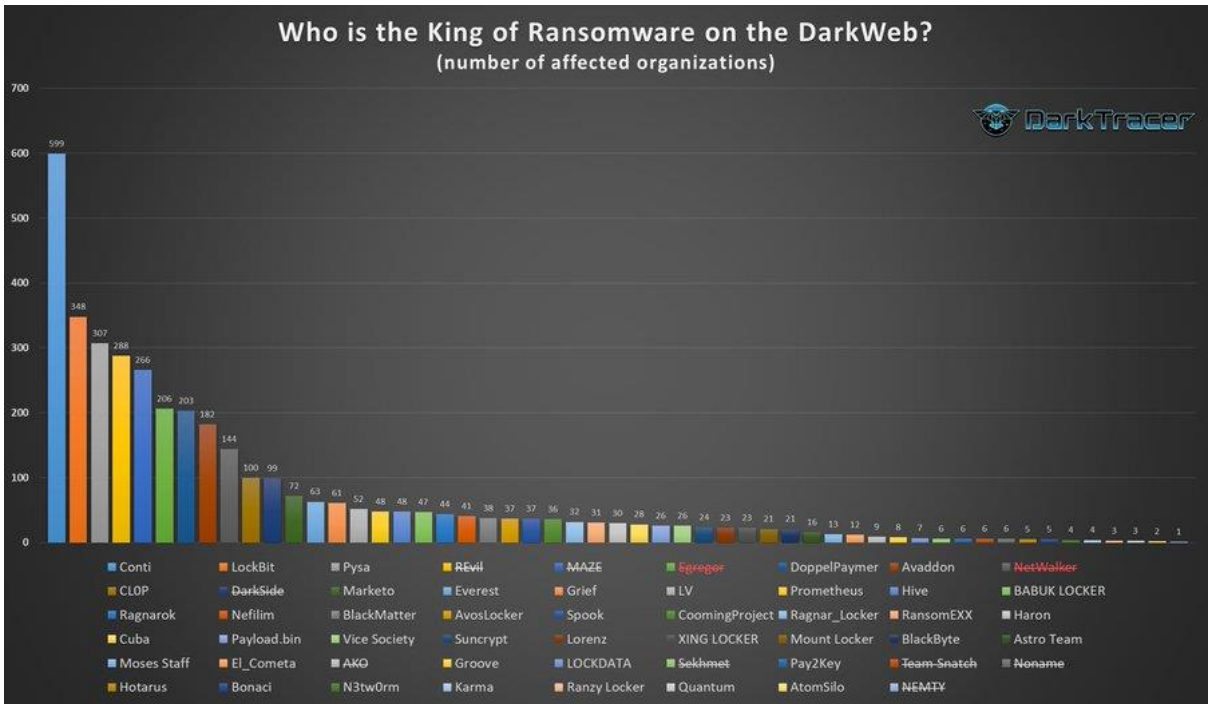


Abb. 5: Weltweite Opfer von Ransomware nach Angreifern gemäss Data Leak Sites. Die durchgestrichenen Gruppierungen waren zum Zeitpunkt der Erstellung der Grafik nicht mehr aktiv. (Quelle: darktracer.com).

35 ENISA Threat Landscape 2020 - Spam (enisa.europa.eu)

36 GootKit (Malware Family) (fraunhofer.de); «Gootloader» expands its payload delivery options (sophos.com); Gootkit: the cautious Trojan (securelist.com)

Ransomware-Infektionen bleiben auch in der zweiten Hälfte des Jahres 2021 die Vorfälle mit den schwerwiegendsten potenziellen Auswirkungen für schweizerische Unternehmen.

Während des Berichtszeitraums registrierte das NCSC Meldungen zu über zwanzig verschiedenen in der Schweiz aktiven Ransomware-Varianten. Besonders aktiv waren die bereits bekannten «REvil» (alias «Sodinokibi»), «LockBit 2.0», «Conti» und «ech0raix». Bei den Neueinsteigern profilierten sich insbesondere «Blackmatter» und «Grief», der Nachfolger von «Doppelpaymer».

Obwohl die Zahl der Meldungen über Ransomware-Angriffe beim NCSC im Vergleich zum letzten Halbjahr von 91 auf 70 leicht zurückgegangen ist, wurden auch im zweiten Halbjahr 2021 in der Schweiz zahlreiche Angriffe auf Privatpersonen und KMUs aus verschiedenen Wirtschaftssektoren verübt. Auch kritische Infrastrukturen waren betroffen, darunter mehrere Gemeinden[37] aber auch eine Bank[38] und eine Privatklinik.[39] Weitere schweizweit Aufsehen erregende Vorfälle betrafen unter anderem das nationale Filmarchiv[40], die Messe Schweiz[41], das bekannte Schweizer Vergleichsportal Comparis.ch[42] sowie Matisa, den Konstruktionsriesen für Maschinen zur Instandhaltung von Eisenbahnstrecken.[43] Auch Schweizer Filialen von Unternehmen mit Sitz im Ausland wurden durch Verschlüsselungsangriffe beeinträchtigt. Beispielsweise waren alle Landesgesellschaften von MediaMarktSaturn durch den «Hive»-Ransomware-Angriff auf die Muttergesellschaft Ceconomy betroffen.[44]

Wie bereits in früheren Ausgaben des Berichts beschrieben, wenden inzwischen verschiedene Ransomware-Akteure eine mehrstufige Erpressungstaktik an.[45] Haben die Kriminellen einmal Zugriff auf die Opfersysteme, beschaffen sie sich vor der Verschlüsselung Kopien von möglichst vielen Daten. Weigert sich das Opfer, das Lösegeld für die Entschlüsselung zu bezahlen, drohen die Angreifenden mit der Veröffentlichung dieser Daten. Auch in diesem Halbjahr wurden bei Ransomware-Angriffen gestohlene sensitive Informationen von Schweizer Unternehmen und Bürgern im Darkweb verkauft oder publiziert. Dies betrifft beispielsweise Steuerdaten, die mithilfe der Ransomware «Lockbit 2.0» von Treuhandgesellschaften entwendet wurden.[46] Oder Daten betreffend die Einwohnerinnen und Einwohner der Gemeinde Rolle, die von der Gruppe «Vice Society» im Rahmen eines Ransomware-Angriffs exfiltriert wurden.[47] Auch Pässe von Schweizer Reisenden, die vom deutschen Touristikunternehmen FTI mithilfe der Ransomware «Conti» erbeutet wurden, wurden von der Täterschaft online gestellt.[48]

---

37 Montreux a ét victime d'une cyber-attaque (watson.ch)
38 Hacker-Angriff hält Aquila in Bann (finews.ch)
39 20210823_MM_Pallas_Kliniken_Cyberattacke.pdf (pallas-kliniken.ch)
40 Cinémathèque suisse: Cyberattacke auf die Cinémathèque suisse (cinematheque.ch)
41 Cyber-Angriff: Informationen und Empfehlungen an unsere Kunden und Partner (mch-group.com)
42 Ransomware attackers demand $400,000 from Swiss website (swissinfo.ch)
43 Matisa: les hackers Grief ayant piraté Comparis volent le géant du rail (watson.ch)
44 Cyberangriff auf Media-Markt-Mutter Ceconomy (inside-it.ch)
45 Siehe Halbjahresbericht 2020/2 (ncsc.admin.ch), Kap. 4.3.1; Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 4.3.2.
46 48 heures pour payer la rançon de 200'000 francs en bitcoins (24heures.ch)
47 Cyberattaque contre Rolle: la commune appelle ses résidents à la vigilance (ictjourna.ch)
48 Hacker stehlen Daten eines Touristikriesen, darunter Reisepässe von Schweizern (inside-it.ch)

IT-Dienstleister sind attraktive Ziele, da Cyberkriminelle, die über ausreichende technische Fähigkeiten verfügen, ein Eindringen in ihr Netzwerk ausnutzen können, um sich zu den Systemen derer Kunden weiterzuhangeln. Die in Kapitel 3.2 und 3.3 angesprochenen Angriffe auf Kaseya durch «REvil» und einen österreichischen IT-Provider durch «BlackMatter» illustrieren dies eindrücklich.

Der Druck gegenüber Betreibern von Ransomware seitens der Behörden und die darauf folgenden Strafverfolgungsaktionen auf globaler Ebene wurden nach dem Angriff auf die Colonial Pipeline[49] verschärft. Europäische und amerikanische Strafverfolgungsbehörden konnten im Herbst in mehreren Aktionen einige Ransomware-Akteure verhaften.[50]

Schlussfolgerung / Empfehlungen:

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

Das NCSC empfiehlt Betroffenen, grundsätzlich kein Lösegeld zu bezahlen. Mit der Leistung einer Zahlung bestätigt man das Geschäftsmodell der Kriminellen, unterstützt diese finanziell und regt sie zur Weiterführung und Weiterentwicklung ihrer Tätigkeiten an. Im schlimmsten Fall verliert man die Daten und das Geld. Das NCSC rät, bei der zuständigen Polizeibehörde Anzeige zu erstatten.

Überlegungen bezüglich der Möglichkeit, Cybervorfälle zu versichern, wurden in der letzten Ausgabe des Halbjahresberichtes in Kap. 4.2.3 vorgenommen.

Darüber hinaus hat die US-amerikanische Cybersicherheitsbehörde CISA ein Dokument veröffentlicht, das sich an Unternehmen richtet, um Datenlecks durch Ransomware-Angriffe zu verhindern und darauf zu reagieren.[51] Ein weiterer relevanter Beitrag auf internationaler Ebene wurde vom neuseeländischen CERT geleistet, das ein Diagramm des Lebenszyklus von Ransomware erstellte, inklusive Kontrollen zum Stoppen des Eindringens.[52]

---

49 Siehe Halbjahresbericht 2021/1 (ncsc.admin.ch), Kap. 4.2.3.

50 Five affiliates to Sodinokibi/REvil unplugged (europol.europa.eu); Ransomware gang arrested in Ukraine with Europol's support (europol.europa.eu); Arrest in Romania of a ransomware affiliate scavenging for sensitive data (europol.europa.eu); Joint global ransomware operation sees arrests and criminal network dismantled (interpol.int); Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (justice.gov)

51 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches (cisa.gov)

52 How ransomware happens and how to stop it (cert.gov.nz)

4.2.3 Qakbot

«Qakbot» (auch bekannt als «Pinkslipbot», «Quakbot» oder «Qbot») war bei seiner Entdeckung 2007 ursprünglich ein Trojaner, der hauptsächlich dazu diente, Bankdaten und andere Finanzinformationen der Opfer zu stehlen. Seither wurde die Malware weiterentwickelt und mit verschiedensten Zusatzmodulen versehen. Sie kann sich in den Netzwerken des infizierten Systems verbreiten, Daten sammeln und extrahieren (insbesondere E-Mail-Inhalte, die in späteren Kampagnen verwendet werden) oder auf dem infizierten Rechner weitere Malware-Komponenten (sog. Payloads) installieren. Diese Funktionen machen «Qakbot» zu einer gefährlichen Schadsoftware, die vom NCSC schon mehrfach als Vektor für Ransomware-Angriffe in der Schweiz beobachtet wurde.[53]

Bei einer Analyse wurde die Angriffskette von «Qakbot» in einzelne Module zerlegt, die je nach Ziel der Kampagne unterschiedlich zusammengesetzt werden können. Damit sind unterschiedliche Angriffsketten möglich, was die Erkennung einer «Qakbot»-Kampagne in einem infizierten Netzwerk erschwert. Dennoch erfolgt die Infizierung mit «Qakbot» fast immer über ein E-Mail. Neben den altbekannten Methoden mit Anhang oder Link werden neuerdings Bilder verwendet, auf denen eine URL abgebildet ist, die das Opfer manuell im Browser eingeben soll. Schliesslich wird jedoch auch hier ein Office-Dokument mit Makros verwendet, um «Qakbot» auf dem Rechner zu installieren.[54]

Die versendeten E-Mails basieren häufig auf bereits getätigter Kommunikation («Thread hijacking»), wie das NCSC in der Berichtsperiode mehrfach beobachtet hat.[55] Da dem Opfer das E-Mail bekannt vorkommt, ist es eher geneigt, das Dokument zu öffnen und der Anleitung darin zu folgen. Typischerweise besagt diese Anleitung, dass der Inhalt nicht geöffnet werden kann, weil die Makros nicht aktiviert sind. Die Benutzerin oder der Benutzer werden dann durch die verschiedenen Schritte geführt, um die Makro-Funktion zu aktivieren.[56]

---

53 QAKBOT - Threat Encyclopedia (trendmicro.com); QakBot (Malware Family) (fraunhofer.de); QakBot, Software S0650 (mitre.org)

54 A closer look at Qakbot's latest building blocks (and how to knock them down) (microsoft.com)

55 Die Woche 44 im Rückblick (ncsc.admin.ch); Die Woche 50 im Rückblick (ncsc.admin.ch)

56 Die Woche 20 im Rückblick (ncsc.admin.ch)

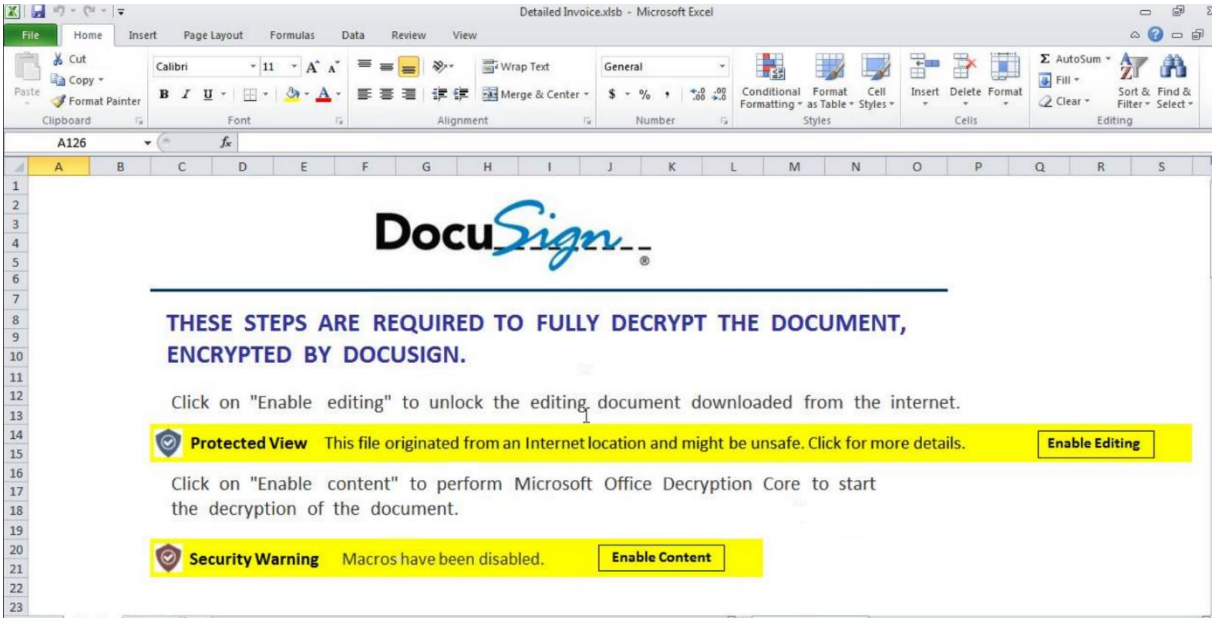


Abb. 6: Excel-Datei mit bösartigen Makros.

Seit Oktober 2021 wurde auch beobachtet, dass «Squirrelwaffle» (ein Malware-Loader, der sich ebenfalls über MS-Office-Dokumente mit bösartigen Makros verbreitet) zusätzlich «Qakbot» installiert. Ausserdem waren die «Qakbot»-Aktivitäten im zweiten Halbjahr durch die Verwendung kompromittierter Exchange-Server gekennzeichnet.[57]

Schlussfolgerung / Empfehlungen:

- Bösartige E-Mails können auch von angeblich bekannten Absendern kommen. Seien Sie vorsichtig, wenn plötzlich zusammenhangslos bereits getätigte Kommunikation verwendet wird.
- Schadsoftware wird vielfach über Office-Dokumente verteilt. In den meisten Fällen wird die Makro-Funktion ausgenutzt. Geben Sie nie die Erlaubnis, die Makro-Funktion zu aktivieren.
- Betreibern von Microsoft Exchange-Servern empfehlt das NCSC dringend, alle entsprechenden Patches einzuspielen und die Server auf dem neuesten Stand zu halten.
- Exchange-Server dürfen nicht direkt aus dem Internet erreichbar sein. Schalten Sie entweder eine WAF (Web Application Firewall) vor oder setzen Sie einen SMTP-Filtering-Proxy vor den Exchange-Server.
- Für die Verbreitung von «Qakbot» eingesetzte Websites sollen am Netzwerkperimeter gesperrt werden. Eine Liste dieser Websites wird von URLhaus (abuse.ch) kostenlos zur Verfügung gestellt.

[57] Vgl. oben Kap. 4.1.4.

4.3 Angriffe auf Websites und -dienste

4.3.1 DDoS

Die Beeinträchtigung der Verfügbarkeit von Websites durch DDoS-Angriffe («Distributed Denial of Service») bleiben ein anhaltendes Phänomen im In- und Ausland. Im zweiten Halbjahr 2021 wurden dem NCSC 17 Vorfälle dieser Art gemeldet.

Der Finanzsektor bleibt ein beliebtes Ziel von erpresserischen DDoS-Wellen. In der zweiten Hälfte 2021 wurden in der Schweiz jedoch auch IT-Dienstleister, Behörden und Bildungsinstitutionen anvisiert. Unter dem Namen «FancyLazarus» versuchten DDoS-Erpresser verschiedene Schweizer Unternehmen und kantonale Behörden zu erpressen. Die von den Angreifern nach Demonstrationsangriffen angedrohten schwerwiegenden Attacken blieben jedoch jeweils aus. Im Juli und Oktober wurde der Hosting-Provider der Stadt und des Kantons St. Gallen Opfer von DDoS-Angriffen, was vorübergehend zu Ausfällen der Websites führte.[58] Mehrere internationale VoIP (Voice-over-IP)-Dienstleister meldeten vorübergehende Leistungsausfälle aufgrund von DDoS-Angriffen, etwa Telnyx, Bandwidth und Twilio.[59] Im September kam es in Neuseeland zu Ausfällen von Online-Dienstleistungen von Banken.[60] Und der polnische Ableger von T-Mobile wehrte eine grössere DDoS-Welle im Dezember ab.[61]

Im Kontext der deutschen Bundestagswahl sind gemäss Pressemeldungen politisch motivierte DDoS-Angriffe beobachtet worden.[62]

DDoS-Angriffe werden auch mit anderen Angriffsmustern kombiniert: Die Ransomware-Familien «HelloKitty» und «Yanluowang» operieren beispielsweise mit DDoS, um ihre Erpressungsopfer zusätzlich unter Druck zu setzen.[63]

Schlussfolgerung / Empfehlungen:

DDoS-Erpressung ist ein Massengeschäft. Die Angreifenden versuchen relativ undifferenziert bei möglichst vielen Unternehmen ihr Glück. Hat dies keinen Erfolg, versuchen sie es anderswo. Gelingt es aber, mit einem (Demonstrations-)DDoS-Angriff die Systeme eines Unternehmens zu stören, so gerät dieses Unternehmen als potenzielles Opfer in den Fokus. In der Hoffnung, dass Lösegeld bezahlt wird, verstärken die Täter ihre Anstrengungen. Deshalb ist es ratsam, sich auf allfällige DDoS-Angriffe vorzubereiten.

Das NCSC empfiehlt, für kritische Systeme einen kommerziellen DDoS-Schutz zu abonnieren («DDoS Mitigation Service»). Viele Internet-Service-Provider bieten solche Dienste an.

58 Homepages der St.Galler Behörden durch Hackerangriff lahmgelegt (tagblatt.ch)
59 DDoS attack takes yet another VoIP provider offline (techradar.com)
60 Government still gauging impact of Wednesday's denial-of-service attacks (stuff.co.nz)
61 Polish T-Mobile unit faces cyber attack, systems not compromised (reuters.com)
62 Bundestagswahl 2021: Hackerangriff auf Website des Bundeswahlleiters (businessinsider.de)
63 Kaspersky Q4 2021 DDoS attack report (securelist.com)

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

Das Inter-University Computation Center (IUCC) hat zudem im letzten Halbjahr einen ausführlichen Guide bezüglich Best-Practices für DDoS-Mitigationsstrategien publiziert:
Best Practices for DDoS Mitigation Strategies (geant.org)

4.3.2 Angriffe gegen VoIP-Systeme

Telefonie ist mittlerweile fast vollständig digitalisiert und die meiste Sprachkommunikation geht über das Internet (Voice over IP, VoIP). VoIP-Systeme in Unternehmen sind entsprechend ans Internet angeschlossen und bieten nicht nur Angriffsfläche für DDoS (vgl. Kap. 4.3.1 hiervor), sondern können auch missbraucht werden, wenn sie schlecht geschützt sind. Die VoIP-Systeme einer Schweizer Organisation, die nur mit einem Standardpasswort geschützt war, wurde von Kriminellen für kostenpflichtige Anrufe missbraucht. Durch Anrufe nach Tunesien verursachten die Täter eine Rechnung von mehreren hunderttausend Franken.

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

Angriffe direkt gegen industrielle Kontrollsysteme, um physische Prozesse zu stören oder zu beeinflussen, blieben auch im Berichtszeitraum die Ausnahme. Weit häufiger werden die betrieblichen Auswirkungen verursacht durch Verbindungen der Kontrollsystem-Netzwerke mit den administrativen IT-Systemen, über welche die Verwaltung des Unternehmens wie die kommerziellen Beziehungen zu Kunden und Lieferanten bearbeitet werden.

4.4.1 Treibstoffversorgung im Iran nach Cyberangriff eingeschränkt

Im vergangenen Oktober war der Betrieb an etlichen Tankstellen im Iran eingeschränkt. Das Zahlungssystem für subventionierte Treibstoffe war ausgefallen[64], gemäss iranischen Behörden auf Grund eines Cyberangriffs einer ausländischen Macht.[65] Die Zapfsäulen hätten zwar Benzin geliefert, jedoch funktionierte das Zahlungssystem für den subventionierten Bezug von Benzin nicht. Für die meisten einheimischen Kunden kam dies jedoch einem Ausfall gleich, da sie sich die Treibstoffe ohne die subventionsbedingte Vergünstigung nicht leisten können.

Der Ausfall erfolgte kurz vor dem zweiten Jahrestag der letzten grossen Protestwelle im Iran, welche ebenfalls durch die Erhöhung der Benzinpreise entfacht wurde. Gleichzeitig wurde Reisenden auf den Schnellstrassen auf den elektronischen Anzeigetafeln die Meldung «Khamenei, wo ist unser Benzin?» eingeblendet. Diese Meldungen erinnerten an einen ähnlich

64 Störung der Benzinversorgung - Schlangen vor Irans Zapfsäulen: «Khamenei, wo ist unser Benzin?» (srf.ch)
65 Iran says Israel, U.S. likely behind cyberattack on gas stations (reuters.com)

gelagerten Cyberangriff auf den iranischen Eisenbahnverkehr im Juli letzten Jahres, bei welchem auch eine «Wiper»-Komponente[66] eingesetzt wurde. Ein direkter Zusammenhang der beiden Vorfälle liess sich bislang jedoch nicht bestätigen.

4.4.2 Betreiber aus der Steuerung der Gebäudeautomation ausgesperrt

Welche Auswirkungen unberechtigte gezielte Manipulationen an industriellen Kontrollsystemen haben können, beschrieb der Computersicherheitsdienst Limes Security anhand eines Angriffs auf ein Gebäudeautomationssystem.[67] Ein Angreifer konnte sich Zugriff auf die KNX-Technologie basierten Komponenten verschaffen und durch Manipulation derer Konfiguration, dem regulären Betreiber die Kontrolle über die Geräte entziehen.

Der Angreifer benötigte spezifisches Fachwissen über die Funktionsweisen von KNX, um aus dem «smarten» Gebäude eine teilweise nur noch manuell vor Ort oder gar nicht mehr steuerbare Immobile zu machen. Die Absicht des Angreifers blieb bis zum Schluss unklar und einzig forensische Untersuchungen der Gerätespeicher durch beigezogene Spezialisten konnte einen aufwändigen Ersatz von teilweise fix in der Bausubstanz integrierten Geräten verhindern.

Schlussfolgerung / Empfehlungen:

Es lohnt sich, in die Absicherung des Zugriffs auf industrielle Kontrollsysteme zu investieren und den Betrieb sowie Manipulationen zu überwachen, damit bei Verdacht auf missbräuchliche Änderungen zeitnah reagiert werden kann.
Das NCSC empfiehlt auf seiner Website: Massnahmen zum Schutz von ICS (ncsc.admin.ch)

4.4.3 OT bedroht durch Aufklärung und Kollateralschäden

Angriffe, wie im vorangehenden Kapitel beschrieben, die den Betrieb industrieller Kontrollsysteme durch dedizierten Missbrauch derer Funktionaltäten stören, bleiben die Ausnahme bei Cybervorfällen, welche physische Prozesse negativ beeinträchtigen. Viel häufiger werden IT-Systeme, welche zur Bedienung der Steuerungssysteme eingesetzt werden, mit breit verteilter Schadsoftware infiziert[68], oder es wird versucht IoT-Geräte für DDoS- oder Kryptoschürfungs-Botnetze[69] einzuspannen.

Derartige Infektionen haben häufig noch keine Auswirkungen auf die gesteuerten Prozesse. In Fällen, bei welchen in der Folge Ransomware auf die Systeme ausgeliefert wird, ändert sich dies leider häufig. Sechs bekannte Ransomware-Familien («Cl0p», «MegaCortex», «Netfilim», «LockerGoga», «Maze» und «EKANS»), versuchen im Zuge des Angriffs gar explizit IT-Pro-

66 MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll (sentinelone.com)
67 KNXlock – an attack campaign against KNX-based building automation systems (limessecurity.com)
68 https://ics-cert.kaspersky.com/publications/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/
69 Honeypot experiment reveals what hackers want from IoT devices (bleepingcomputer.com)

zesse mit Bezug zu OT-Systemen zu terminieren. So beobachtete die auf ICS-Sicherheit spezialisierte Firma Dragos im vierten Quartal 2021 176 publizierte Datenlecks mit ICS-Bezug auf Darknet-Seiten von Ransomware-Gruppierungen[70]. Am häufigsten betroffen waren dabei die produzierende Industrie, gefolgt von der Transport- und Lebensmittelbranche.

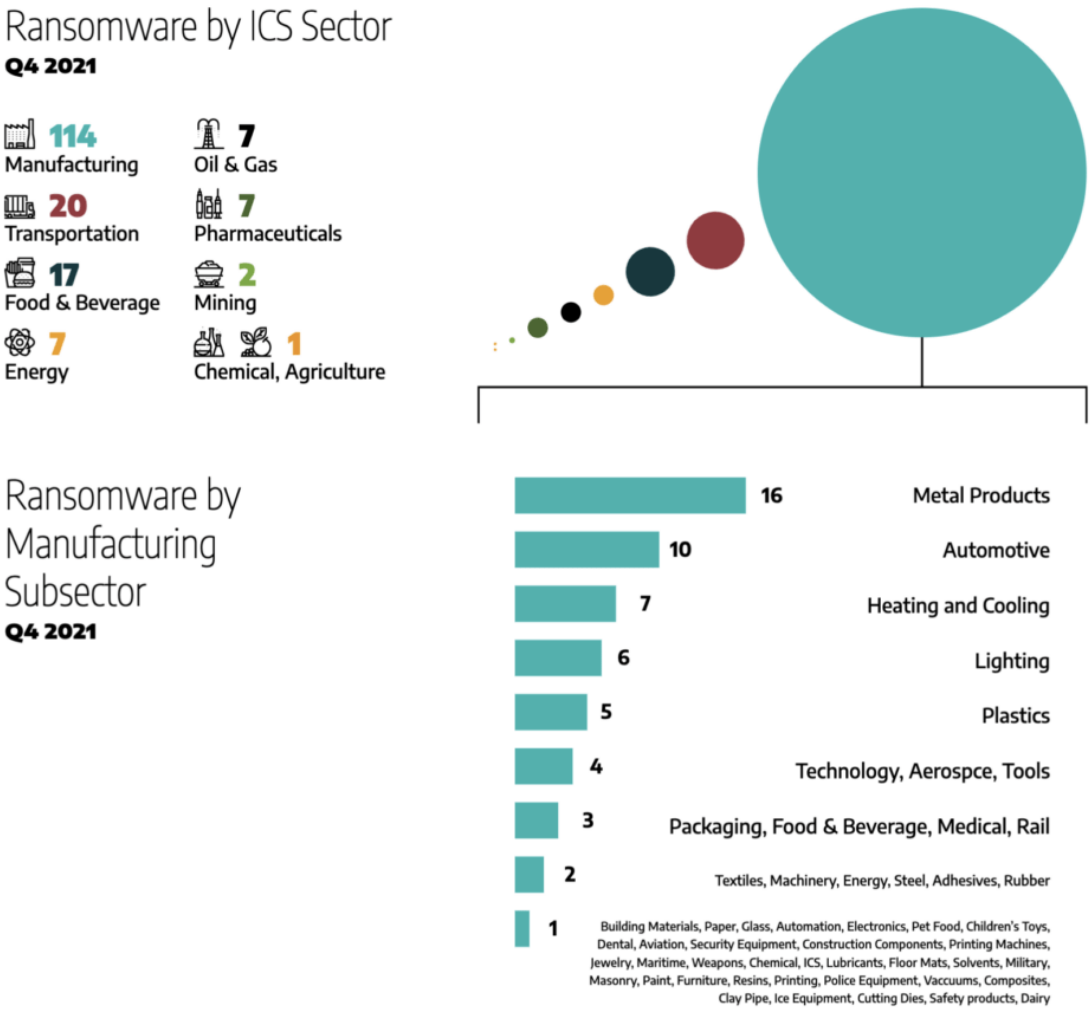


Abb. 7: Von Ransomware-Gruppen publiziere Daten mit ICS Bezug nach Sektor (Quelle: dragos.com)

Eine Umfrage[71] des ebenfalls im Bereich der OT-Absicherung spezialisierten Unternehmens Claroty bestätigte die Bedrohung der Systeme durch Ransomware. 47 % der befragten 1'100 Betreiber registrierten Auswirkungen auf OT-Systeme, welche durch Ransomware-Angriffe verursacht wurden.

70 Dragos ICS/OT Ransomware Analysis: Q4 2021 (dragos.com)
71 Ransomware Often Hits Industrial Systems, With Significant Impact: Survey (securityweek.com)

Werden abgefasste Dateien aus Ransomware-Angriffen publiziert, enthalten sie laut Mandiant in einem von sieben Fällen Dokumente mit Informationen über OT-Systeme (Netzwerkarchitektur, eingesetzte Hard- und Software, usw.), welche potentiell auch für künftige Angriffe benutzt werden könnten. Effektive Sabotage-Versuche auf industrielle Kontrollsysteme sind weiterhin am ehesten im Umfeld von bestehenden Konflikten zu erwarten. So verstärkte die Ukraine mit Hilfe von Spezialisten aus den USA und Grossbritannien ihr diesbezügliches Abwehrdispositiv[72] im Angesicht der Truppenaufmärsche an der Grenze zu Russland.

4.5 Schwachstellen

4.5.1 Atlassian Confluence - CVE-2021-26084 - Remote Code Execution

Am 25. August 2021 kündigte der Software-Anbieter Atlassian die Veröffentlichung eines Patches für eine kritische Schwachstelle in der Software Confluence an.[73] Confluence ist ein kollaboratives Tool zur Verwaltung von Arbeitsbereichen und Projekten, das von vielen Unternehmen weltweit verwendet wird und oft interne Daten enthält. Die Sicherheitslücke erlaubt einem Angreifer, aus der Ferne einen beliebigen Code auszuführen (Remote Code Execution, RCE). Der Angreifer kann den ganzen Server kompromittieren, auf dem Confluence betrieben wird. In mehreren Fällen wurde ein «Krypto-Miner» installiert[74] oder Unternehmen wurden durch Verschlüsselung ihrer Daten erpresst.[75]
Laut Atlassian war nur die On-Premises-Lösung ihres Produktes betroffen – die Cloud-Version war nicht gefährdet.

Schlussfolgerung / Empfehlungen:

Diese Schwachstelle lässt sich nachweislich leicht ausnutzen. In Anbetracht der bekannten Einzelheiten ist das Risiko als sehr hoch einzustufen.

Die Öffentlichkeit ist indirekt betroffen, wenn ein Unternehmen, zu dessen Kundschaft sie gehören, kompromittiert ist. Unternehmen, die On-Premises-Lösungen einsetzen, sollten besonders vorsichtig sein. Unternehmen, die ihre Confluence-Server selber warten, wird dringend empfohlen, die nötigen Patches einzuspielen.[76]

4.5.2 Azure - OMIGOD – Privilegienerweiterung, Remote Code Execution

Am 8. September 2021 kündigte Microsoft einen Patch für mehrere kritische Schwachstellen an, die ihr Azure-Angebot betrafen. Die Sammlung der Schwachstellen namens «OMIGOD» betrifft OMI, ein Tool zur Verwaltung von Linux- und UNIX-Systemen, die bei verschiedenen

72 U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault (nytimes.com)
73 Confluence Security Advisory - 2021-08-25 | Confluence Data Center and Server 7.16 (atlassian.com)
74 Cryptominer z0Miner Uses Newly Discovered Vulnerability CVE-2021-26084 to Its Advantage (trendmicro.com)
75 New Atom Silo ransomware targets vulnerable Confluence servers (bleepingcomputer.com)
76 [CONFSERVER-67940] Confluence Server Webwork OGNL injection - CVE-2021-26084 (atlassian.com)

Diensten des Azure-Angebots verwendet wird. Die Schwachstellen ermöglichen die Privilegien-Erweiterung eines Nutzers (CVE-2021-38645, CVE-2021-38648, CVE-202138649) sowie die Remote Code Execution durch einen nicht authentifizierten Angreifer (CVE-2021-38647). Die Lücken weisen einen Schweregrad zwischen 7.0 und 9.8 bei einem Maximum von 10 auf. Sechs Tage nach den Patches veröffentlichte die Firma, die die Schwachstellen entdeckt hatte, einen Artikel über deren Funktionsweise.[77] Microsoft hat am 14. September 2021 einen Patch veröffentlicht, der nur für bestimmte Cloud-Angebote automatisch bereitgestellt wurde. Kunden, die ihre eigene Azure-Infrastruktur betreiben, müssen den Patch selber einspielen. Microsoft hat eine Liste der betroffenen Dienste herausgegeben und das Vorgehen beschrieben.[78]

Schlussfolgerung / Empfehlungen:

Die Öffentlichkeit ist von dieser Art kritischer Schwachstelle indirekt betroffen, wenn persönliche Informationen der Unternehmen, deren Kunden sie sind, offengelegt werden können. Das Risiko für Unternehmen, die ihre eigene Azure-Infrastruktur betreiben, ist hoch. Ihnen wird empfohlen, die Angaben von Microsoft zu prüfen und zu befolgen.

4.5.3 Log4j – CVE-2021-44228 – Log4Shell

Am 9. Dezember 2021 wurde die kritische Schwachstelle in der Open-Source-Bibliothek Apache «Log4j» gemeldet (CVE-2021-44228). Die für die Ausnutzung erforderlichen Einzelheiten wurden ebenfalls veröffentlicht. «Log4j» ist eine beliebte Java-Bibliothek, die eine Protokollierungsinfrastruktur für Drittanwendungen bereitstellt. Die Sicherheitslücke wird als kritisch eingestuft (Schweregrad 10 von 10), da aus der Ferne ein beliebiger Code ausgeführt werden kann (Remote Code Execution, RCE).

Zahlreiche Produkte und Open Source Software beruhen auf der Verwendung von «Log4j» als Protokollierungsrahmen. Deshalb können viele Unternehmen durch die Nutzung externer Produkte in Teilen ihrer Infrastruktur betroffen sein, ohne dass sie sich dessen bewusst sind.

Im Zuge von CVE-2021-44228 wurden verschiedene Sicherheitslücken in Verbindung mit «Log4j» behoben. Das NCSC hat im GovCERT-Blog eine detaillierte Übersicht über die Ereignisse veröffentlicht.[79]

Schlussfolgerung / Empfehlungen:

Das NCSC hat dringend empfohlen, zur Verfügung stehende Sicherheits-Patches so rasch wie möglich einzuspielen und die Entwicklung der Situation für Unternehmen, die «Log4j» oder Lösungen mit «Log4j» in ihrer Infrastruktur verwenden, genau zu verfolgen.

---

77 OMIGOD: Critical Vulnerabilities in OMI Affecting Countless Azure Customers (wiz.io)
78 Additional Guidance Regarding OMI Vulnerabilities within Azure VM Management Extensions (microsoft.com)
79 Zero-Day Exploit Targeting Popular Java Library Log4j (govcert.admin.ch)

Da diese Schwachstelle auch Komponenten einer von Dritten entwickelten Infrastruktur betreffen kann, wird ausserdem dringend empfohlen, ein aktuelles Inventar dieser Dienste zu führen und betroffene Dienste laufend zu aktualisieren.

In Anbetracht dessen, dass diese Sicherheitslücke leicht ausgenutzt werden kann und nach den dazu veröffentlichten Informationen, ist das Risiko für Systeme, die den Patch nicht eingespielt haben, weiterhin extrem hoch.
Neben den indirekten Auswirkungen auf die Öffentlichkeit, wenn ein Unternehmen Opfer eines Angriffs geworden ist, hat diese Schwachstelle auch direkte Auswirkungen für Privatpersonen. Sowohl von Unternehmen und Privatpersonen verwendete NAS-Geräte (Network Attached Storage) wurden ebenfalls als anfällig für diese Art von Angriffen identifiziert. Der NAS-Hersteller QNAP hat Empfehlungen und Informationen zu den betroffenen Produkten veröffentlicht[80], und es wurde über mehrere erfolgreiche Ransomware-Angriffe berichtet.

4.5.4 Blacksmith - CVE-2021-42114

Am 15. November 2021 veröffentlichten Forscher der ETHZ, von Qualcomm und der Freien Universität Amsterdam eine Studie über eine Hardware-Schwachstelle namens «Blacksmith».[81] Die Schwachstelle betrifft Geräte mit einem RAM-Chip-Typ und zeigt eine neue Methode, wie auf DDR4-Chips implementierte Sicherheitssysteme effizient umgangen werden können.

Da das NCSC im September 2021 als Zulassungsbehörde für die Vergabe von CVE-Nummer anerkannt worden ist, hat dieses als Vermittlerin zwischen dem Forschungsteam und den Chip-Herstellern fungiert. Zudem hat es mit der Vergabe der CVE-Nummer für die Schwachstelle «Blacksmith» erstmals eine CVE-Nummer vergeben.

Schlussfolgerung / Empfehlungen:

Die Schwachstelle betrifft Chips der Hersteller Samsung, SK Hynix und Micron, die von verschiedenen Technologieunternehmen verwendet werden. Wegen deren weltweitem Einsatz wird die Schwachstelle als kritisch eingestuft. Das Risiko der Ausnutzung ist jedoch insofern sehr gering, weil der Aufwand dafür gross ist.

In diesem Fall gibt es keine Patches der Hersteller, die RAM-DDR4-Chips bleiben anfällig. Es wird empfohlen, für kritische Infrastrukturen einen Chip-Typ zu verwenden, der besser vor sogenannten «Rowhammer»-Angriffen geschützt ist (ECC oder DDR5).

80 Multiple Vulnerabilities in Apache Log4j Library - Security Advisory (qnap.com)
81 Blacksmith – Computer Security Group (ethz.ch)

4.6 Datenabflüsse

4.6.1 Fortinet VPN Credentials

Der Akteur «Orange» veröffentlichte eine halbe Million Zugangsdaten für Fortinet VPN-Konten auf seinem neuen Untergrundforum.[82] Angeblich wurden die Zugangsdaten im Sommer über eine Schwachstelle ausgelesen, für die mittlerweile ein Patch verfügbar ist.

Das NCSC hat die rund 400 Einträge mit Schweiz-Bezug eruiert und die betroffenen Organisationen entsprechend informiert.

Schlussfolgerung / Empfehlungen:

Verwundbare Fernzugriffslösungen werden regelmässig für die Lancierung von Ransomware verwendet. Wenn Kriminelle vollständige aktuell gültige Zugangsdaten für Fernzugriffe haben, sind auch gepatchte Systeme nicht vor ihnen sicher.

Schützen Sie Zugänge zu Daten, Konten, Systemen und Netzwerken wenn möglich mit Zwei-Faktor-Authentisierung und nicht nur mit einer Benutzername/Passwort-Kombination.

Zugangsdaten sollten regelmässig geändert werden. Das gilt insbesondere nach der Behebung einer Schwachstelle, welche das Risiko eines Abflusses von Zugangsdaten birgt.

4.6.2 EasyGov

Mit automatisierten Massenabfragen über die vom Staatssekretariat für Wirtschaft (SECO) betriebene Webplattform «www.easygov.swiss» ist es Hackern im August 2021 mutmasslich gelungen, an die Namen von bis zu 130’000 Unternehmen zu gelangen, die 2020 einen Covid-19-Kredit beantragt hatten. Wie hoch der Kredit jeweils war oder weitere Angaben über die betreffenden Unternehmen konnten die Hacker auf diesem Weg jedoch nicht in Erfahrung bringen. Das SECO wurde am 19. Oktober über die Angelegenheit informiert und ergriff Sofortmassnahmen: Die betroffene Web-Schnittstelle wurde innert weniger Minuten geschlossen, die Daten wurden vom Server entfernt und der eingesetzte Prozess auf «EasyGov» vollständig deaktiviert.[83] Das NCSC unterstützte und beriet das SECO in diesem Fall. Das SECO leitete eine Untersuchung ein.

[82] Hackers leak passwords for 500,000 Fortinet VPN accounts (bleepingcomputer.com)
[83] Cyberangriff auf EasyGov (seco.admin.ch)

Schlussfolgerung / Empfehlungen:

Die Digitalisierung bringt einige Vereinfachungen von administrativen Prozessen. Deshalb heisst das Portal des SECO auch «EasyGov». Während der Pandemie war zudem Dringlichkeit vorhanden, der Wirtschaft unkompliziert Hilfe zu leisten. Unternehmen konnten deshalb durch die Eingabe ihrer Unternehmensnummer (UID) ein Formular öffnen, um einen Kredit zu beantragen. Wenn bereits ein (erster) Kredit für eine UID beantragt war, öffnete sich kein Formular. Dies konnte ausgenutzt werden, um über Massenabfragen mit den im Handelsregister ersichtlichen UIDs herauszufinden, welche Unternehmen diese Möglichkeit genutzt hatten.

Das Aufschalten von Abfragemöglichkeiten oder Inhalten, die mit einer Datenbank verknüpft sind, birgt immer ein Missbrauchsrisiko. Deshalb muss man sich vorher überlegen, was eine unberechtigte neugierige Person durch diverse Eingaben für Resultate erzielen kann – auch eine «negativ»-Antwort lässt Schlüsse zu. Essenziell ist auf jeden Fall das Verhindern von Massenabfragen, damit unberechtigte Personen nicht in kürzester Zeit grosse Datenmengen beschaffen können.

4.7 Spionage

4.7.1 Pegasus

Im zweiten Halbjahr 2021 setzten sich Presse, Forschung, NGOs und Öffentlichkeit stark mit dem Einsatz der Spionage-Software «Pegasus» auseinander, nachdem Amnesty International im Juli 2021 einen Report über den weltweiten Einsatz von «Pegasus» gegen Menschenrechtsaktivistinnen und -aktivisten sowie Medienschaffende veröffentlicht hatte.[84] Die kanadische Forschungsplattform CitizenLab hatte bereits 2018 eine Information zu dessen Einsatz in 45 Ländern zwischen 2016 und 2018 publiziert.[85] «Pegasus» des israelischen Unternehmens NSO ist eine Überwachungssoftware für Mobilgeräte, die nach Angaben des Herstellers zur Terrorismusbekämpfung entwickelt worden ist und an staatliche Behörden verkauft wird. Im Rahmen strafrechtlicher Ermittlungen sowie bei Beschaffungsmassnahmen von Nachrichtendiensten werden solche Lösungen weltweit zur Aufklärung von Zielpersonen eingesetzt. Sicherheitsbehörden wählen ein solches Vorgehen hauptsächlich deshalb, weil von Verdachtspersonen eingesetzte Kommunikationskanäle und Applikationen zunehmend Ende-zu-Ende verschlüsselt sind und somit ein Abhören oder Mitlesen während der Übertragung nicht mehr möglich ist. Über die letzten Jahre hat sich eine Industrie entwickelt, welche Überwachungsprodukte für staatliche Behörden anbietet, die auf Endgeräte abzielen. Problematisch ist, dass diese Überwachungsmittel jeweils nach lokalem Rechtsrahmen der Käufer angewendet werden. Im September 2021 schloss Apple eine Schwachstelle im Chat-Dienst iMessage, die von «Pegasus» ausgenutzt worden war.[86]

84 Pegasus Projekt: Spionage-Software späht Medien, Zivilgesellschaft und Oppositionelle aus (amnesty.ch)
85 HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (citizenlab.ca)
86 Analyzing Pegasus Spyware's Zero-Click iPhone Exploit ForcedEntry (trendmicro.com)

4.7.2 Datendiebstahl über Slack-API

Die Hackergruppe «MuddyWater», die mutmasslich vom iranischen Staat unterstützt wird[87], setzt eine neu entdeckte Backdoor namens «Aclip» ein, welche die Schnittstelle (API) des webbasierten Instant-Messaging-Dienstes Slack für verdeckte Kommunikation missbraucht. «Aclip» wird über ein Windows-Batch-Skript namens «aclip.bat» ausgeführt, daher der Name. Die Backdoor verbleibt auf einem infizierten Gerät, indem sie einen Registrierungsschlüssel hinzufügt, und wird automatisch beim Systemstart gestartet. «Aclip» empfängt PowerShell-Befehle vom C2-Server über Slack-API-Funktionen und kann verwendet werden, um weitere Befehle auszuführen, Screenshots des aktiven Windows-Desktops zu senden und Dateien zu exfiltrieren. Der Akteur setzte diese Technik gemäss einem IBM-Bericht gegen Fluggesellschaften ein.[88]

4.7.3 Nobelium

Der Akteur hinter dem Lieferketten-Angriff auf SolarWinds wurde von Forschenden als «Nobelium» bezeichnet. «Nobelium» wurde von verschiedenen Stellen der Gruppierung «APT29» bzw. dem russischen Auslandnachrichtendienst SVR zugerechnet.[89] Im zweiten Halbjahr 2021 war «Nobelium» weiterhin aktiv und zielte gemäss Microsoft insbesondere auf IT-, Managed-Services- und Cloud-Dienstleister in den Vereinigten Staaten und Europa ab, um Zugriff auf deren Kunden zu erhalten. Microsoft beobachtete, dass der Akteur auf Konten mit privilegierten Rechten abzielte, um sich weiter in Cloud-Umgebungen auszubreiten und Kundenbeziehungen auszunutzen.[90] Die Kampagne unterstreicht die Relevanz von Vertrauens- und Kundenbeziehungen für Spionagerisiken, insbesondere im Bereich von IT-Dienstleistern.

4.7.4 Nickel / K3chang

Cyberspionage-Akteure nutzen weiterhin ungepatchte Fernzugriffslösungen stark aus: Microsoft berichtete über eine Kampagne des Akteurs «Nickel», der entsprechend vorging.[91] «Nickel» scheint aus China zu operieren und wurde der Gruppierung «K3chang» zugerechnet.[92] Die von Microsoft beschriebene Kampagne betraf diverse Ziele, unter anderem Regierungsorganisationen, diplomatische Vertretungen und Nicht-Regierungsorganisationen auf mehreren Kontinenten, unter anderem auch in der Schweiz.

---

87 MuddyWater (Threat Actor) (fraunhofer.de)
88 Nation State Threat Group Targets Airline with Aclip Backdoor (securityintelligence.com)
89 APT29, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, Group G0016 (mitre.org)
90 NOBELIUM targeting delegated administrative privileges to facilitate broader attacks (microsoft.com)
91 NICKEL targeting government organizations across Latin America and Europe (microsoft.com)
92 Ke3chang, APT15, Mirage, Vixen Panda, GREF, Playful Dragon, RoyalAPT, Group G0004 (mitre.org)

4.8 Social Engineering und Phishing

4.8.1 Übersicht Phishing

Im Berichtszeitraum wurden 90’046 URLs geprüft, nachdem sie über das vom NCSC betriebene Portal antiphishing.ch oder über das Meldeformular an die nationale Anlaufstellte gemeldet worden waren. Daraus resultierten 3’991 bestätigte Phishing-Webseiten, die das NCSC dann an die jeweiligen Hosting-Provider, verschiedene Browser-Hersteller und Anti-Phishing-Arbeitsgruppen weitermeldete. Im Vergleich zur ersten Jahreshälfte 2021 mit 4’682 detektierten Phishing-Webseiten ist das Niveau leicht gesunken.

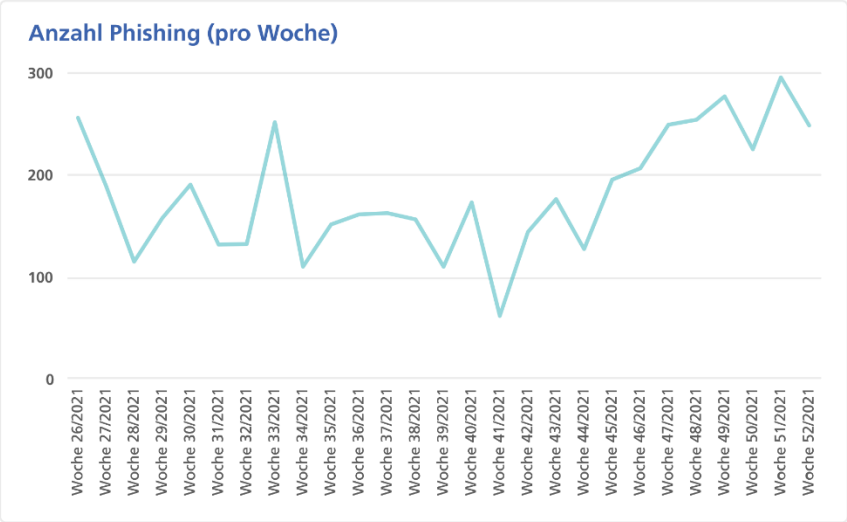


Abb. 8: Anzahl durch das NCSC überprüfte und bestätigte Phishing URLs pro Woche im zweiten Semester 2021. Aktuelle Daten finden Sie unter: https://www.govcert.admin.ch/statistics/phishing/

Das NCSC beobachtet eine Verlagerung der Phishing-Versuche: Statt grosse internationale Marken werden Identitäten von lokalen Unternehmen missbraucht, die zum Teil auch ausschliesslich auf dem Schweizer Markt tätig sind. Zu den Zielen gehören nach wie vor Zugangsdaten für Finanzdienstleister und Internetdienste. Um an Kreditkartendaten zu kommen, verwenden die Kriminellen die Logos von verschiedensten Unternehmen und diverse Vorwände.[93]

Phishing ist ursprünglich ein Massenphänomen. Mittlerweile greifen die Akteure aber teilweise sehr spezifische Ziele an. So wurde im Berichtshalbjahr ein Phishing-Versuch beobachtet, der sich gezielt gegen Unternehmen richtete, die Kunden der Migros Bank sind. Wer auf der Phishing-Webseite die Rubrik «Private» wählte, wurde auf die echte Migros-Bank-Website weitergeleitet. Die Phisher zielten auf Zugriffsdaten, welche für den Zugang mit Buchhaltungssoftware von Unternehmen verwendet werden können.

[93] Siehe oben Kap. 4.1.2 und unten Kap. 5.2.

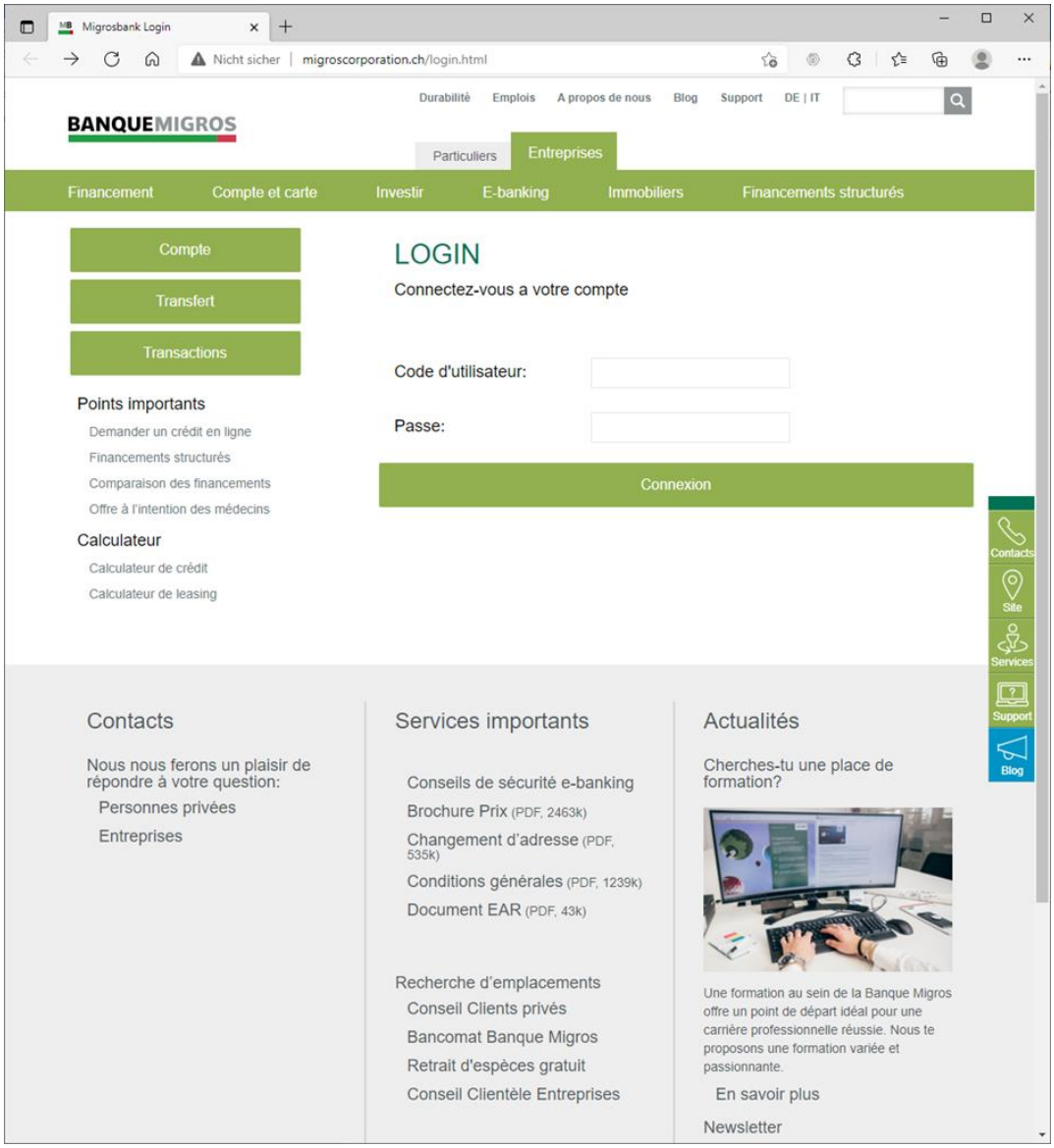


Abb. 9: Phishing-Webseite gegen Unternehmenskunden der Migrosbank.

Zudem wurde im zweiten Halbjahr erneut Real-Time-Phishing gegen Kunden von Schweizer Finanzinstituten festgestellt, obwohl das Volumen im Vergleich zu allen anderen Phishing-Angriffen äusserst gering war. Diese Technik, die die Zwei-Faktor-Authentifizierung aushebelt, aber eine aktivere Komponente seitens des Angreifers erfordert, da er sich zur gleichen Zeit wie das Opfer in das E-Banking-System einloggen muss, wurde bereits im Halbjahresbericht 2019-1 erläutert.[94]

[94] Halbjahresbericht 2019/1 (ncsc.admin.ch), Kap. 4.4.2.

Auch Soziale Netzwerke können für Phishing-Angriffe eingesetzt werden. So wurde Mitte November die Funktion von Facebook, Seiten anzuzeigen, auf denen man markiert wurde, für gezielte Phishing-Angriffe ausgenutzt.[95]

4.8.2 Smishing

SMS und andere Kurznachrichtendienste werden zunehmend für Phishing, sogenanntes «Smishing», missbraucht. Solche Nachrichten täuschen typischerweise vor, von vertrauenswürdigen Absendern zu stammen, z. B. von bekannten Detailhändlern oder Logistikunternehmen. Teilweise sind diese Nachrichten als Wettbewerb getarnt. Ein Link in der Nachricht führt normalerweise auf eine eigens von Kriminellen gestaltete Website, auf welcher man aufgefordert wird, persönliche Daten oder Kreditkartendetails einzugeben.

In Berichtzeitraum hat zum Beispiel Coop über Soziale Netzwerke eine Warnung bezüglich einer Phishing-Nachricht aufgeschaltet, welche via WhatsApp im Umlauf war und vorgab, dass der Empfänger der Gewinner eines von Coop organisierten Wettbewerbs sei.

Abb. 10: Warnung von Coop bezüglich betrügerischen Gewinnspielen in deren Namen.[96]

4.8.3 SIM Swapping

Der Swap (Deutsch: Austausch) von SIM-Karten ist eine Technik, mit der Netzwerkverkehr zu einem mobilen Teilnehmer umgeleitet werden kann, ohne dass man Zugang zu seinem Gerät hat.[97] Durch das sogenannte SIM Swapping (oder auch SIM hijacking) bringt ein Angreifer einen Mobilfunkbetreiber dazu, eine neue SIM-Karte auszustellen und sie mit einer bestehenden Telefonnummer und einem Konto zu verknüpfen. Auf diese Weise erhält die Täterschaft,

95 Die Woche 45 im Rückblick (ncsc.admin.ch)
96 coop_ch auf Twitter: "#Phishing-Nachricht auf WhatsApp." (twitter.com)
97 Network Effects, Tactic TA0038 - Mobile (mitre.org)

die sich diese neue SIM-Karte zustellen lässt, beispielsweise SMS-Nachrichten mit Codes für die Zwei-Faktor-Authentifizierung, um auf bestimmte Dienste zuzugreifen, oder sie kann das Passwort eines Kontos zurücksetzen, da diese Aktion häufig die Eingabe eines per SMS gesendeten Codes erfordert.[98]

Eine Möglichkeit, wie Kriminelle das Ausstellen einer neuen SIM-Karte auslösen können, ist Social Engineering bei Angestellten von Mobilfunkunternehmen. Hilfreiche Informationen dafür können aus Datenlecks bei einem solchen Unternehmen stammen. Die amerikanische Tochterfirma der Deutschen Telekom, T-Mobile US Inc., hatte in den letzten Jahren mehrere Datenlecks zu beklagen. Den letzten Vorfall vom Dezember 2021 machte T-Mobile publik, nachdem mehrere Meldungen von Nutzern eingegangen waren, die von SIM Swapping betroffen waren.[99]

Eine andere Taktik besteht darin, Angestellte von Telekommunikationsunternehmens dazu zu bringen, eine Fernzugriffssoftware zu installieren oder die Anmeldedaten eines in Betrieb befindlichen Fernzugriffsdienstes anzugeben. Auf diese Weise erhält die Täterschaft externen Zugriff auf den Computer und kann die Ausstellung einer neuen SIM-Karte und deren Versand an eine beliebige Adresse lancieren.[100]

4.8.4 E-Banking Fake Support via Google Ad-Link

Das Phänomen der gefälschten Support-Anrufe[101], bei denen vorgegeben wird, dass der Computer infiziert sei, ist schon seit längerem bekannt. Die Kriminellen geben sich in der Regel als Mitarbeiter eines IT-Unternehmens aus und versuchen, das System des Opfers zu infizieren oder geben vor, ihm eine Dienstleistung zu verkaufen, um an seine Kreditkartendaten zu gelangen. In der zwischen Ende August und Ende September vom NCSC[102] und kantonalen Polizeibehörden[103] beobachteten Variante, schalteten die Betrüger Google-Anzeigen, die bei der Suche nach E-Banking-Plattformen bestimmter Schweizer Banken an erster Stelle erscheinen. Beim Klicken auf den Link in der Anzeige landet man auf einer Phishing-Seite. Gibt man Login und Passwort ein, erscheint allerdings eine Fehlermeldung mit dem Hinweis, eine Schweizer Telefonnummer anzurufen. Den Anruf nimmt ein angeblicher Bankmitarbeiter entgegen. Das Opfer wird überredet, eine Fernzugriffssoftware herunterzuladen, damit der Mitarbeiter auf den Computer zugreifen und das «Problem» beheben könne. Der vermeintliche Mitarbeiter übernimmt die Steuerung des PC und löst eine vermeintliche Testzahlung aus und macht sich danach mit dem Geld aus dem Staub.

98 SIM Card Swap, Technique T1451 - Mobile (mitre.org)
99 T-Mobile says new data breach caused by SIM swap attacks (bleepingcomputer.com)
100 Hackers Are Breaking Directly Into AT&T, T-Mobile, Sprint to Take Over Customer Phone Numbers (vice.com)
101 Fake-Support (ncsc.admin.ch)
102 «Die Woche 32 im Rückblick (ncsc.admin.ch); Die Woche 34 im Rückblick (ncsc.admin.ch)
103 Raiffeisen Meldung "Aufgrund verdächtiger Aktivitäten wurde Ihr Konto gesperrt" ist Betrug (cybercrimepolice.ch)

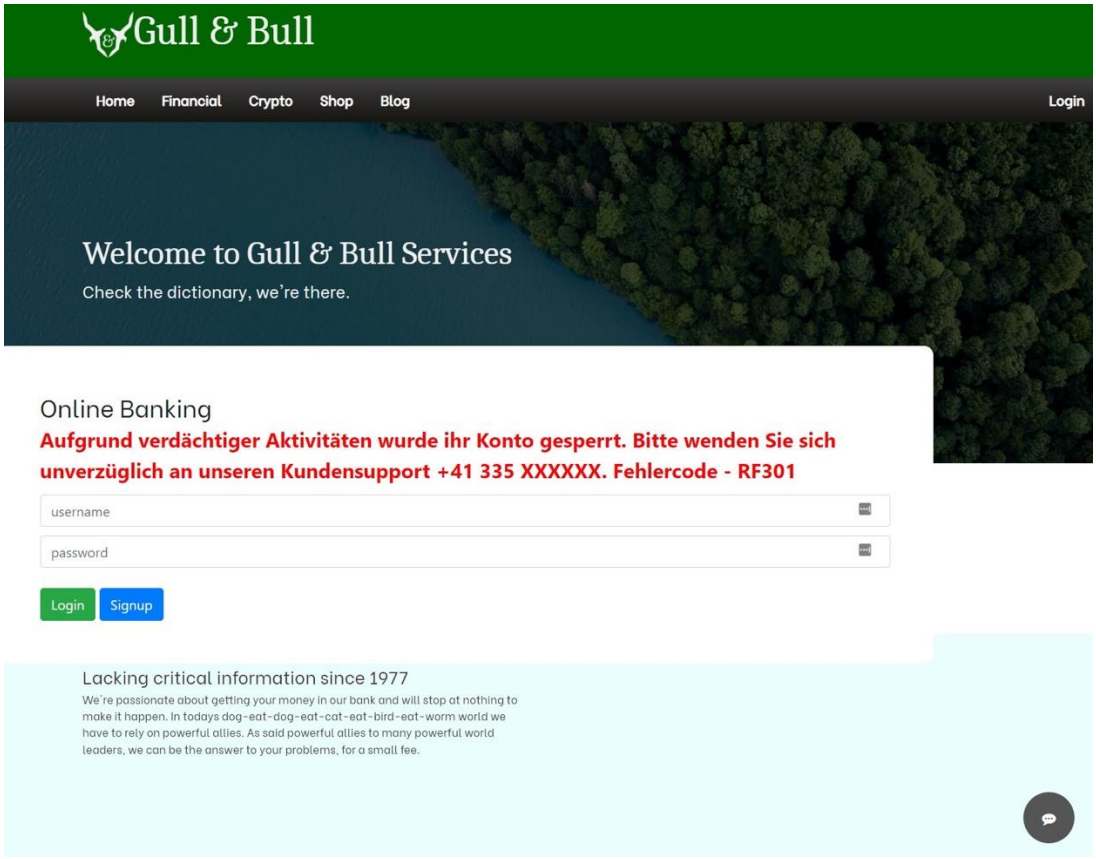


Abb. 11: Imitierte E-Banking-Login-Maske.

5 Kombinierte Phänomene bei Social Engineering

5.1 Trend: Massgeschneiderte Angriffe statt Massengeschäft

Vorschussbetrug, Fake Sextortion oder Fake Support. Dies ist nur ein kleiner Teil an Phänomenen, die das NCSC im letzten Jahr beobachtet hat. Eine Übersicht der mittlerweile über 45 Phänomene ist auf der Webseite «Cyberbedrohungen»[104] des NCSC aufgelistet. Immer öfter ist aber eine eindeutige Kategorisierung nicht möglich. Die Betrüger versuchen nämlich vermehrt, verschiedene Phänomene zu kombinieren. Hintergrund für diese Entwicklung ist, dass es für die Betrüger schwieriger wird, mit «normalen» Betrugs-E-Mails ihre Opfer zu täuschen und sie einen erhöhten Aufwand betreiben müssen, um an ihr Ziel zu gelangen.
Betrugsversuche waren in den letzten Jahren vor allem ein Massengeschäft. Dabei versenden Betrüger automatisiert hunderttausende E-Mails an beliebige Empfänger, in der Hoffnung, dass ein gewisser Prozentsatz darauf hereinfällt. Der Aufwand ist für die Betrüger zwar klein, allerdings ist auch die Erfolgsrate sehr klein. Trotzdem scheint sich dieses Geschäftsmodell in

[104] Cyberbedrohungen (ncsc.admin.ch)

den letzten Jahren gerechnet zu haben. Immer noch werden zahlreiche solche Massenversände beobachtet.

Internetnutzerinnen und Internetnutzer sind aber zunehmend sensibilisiert und die Erfolgsrate verschiebt sich kontinuierlich zu Ungunsten der Betrüger. Plumpe Angriffsversuche werden meistens erkannt. Die Betrüger müssen sich also andere Methoden einfallen lassen, um ein potentielles Opfer zu überzeugen, etwas zu tun, was es eigentlich unter normalen Umständen nicht tun würde. Es geht deshalb darum, über eine gewisse Zeit Vertrauen aufzubauen. Die Kontaktaufnahme geschieht dabei beispielsweise über Plattformen, die dem Empfänger vertraut sind und über die er bereits positive Erfahrungen gemacht hat. Dies senkt die Skepsis und erhöht die Wahrscheinlichkeit, dass ein Opfer auf einen an und für sich simplen Betrug dennoch hereinfällt.

Inserenten von Kleinanzeige-Plattformen werden so beispielsweise auf Phishing-Webseiten gelockt. Bei Angeboten auf Immobilienportalen meldet sich plötzlich ein angeblicher Soldat, der sein Vermögen in der Schweiz investieren wolle. Und auf klassischen Partnervermittlungsseiten versuchen die Betrüger ihre Opfer zu überzeugen, auf dubiosen Plattformen ihr Geld «anzulegen».

5.2 Auf Kleinanzeige folgt Phishing

Auf Kleinanzeigen-Plattformen tummeln sich zahlreiche Betrüger. So gehört Kleinanzeigen-Betrug zu den am häufigsten gemeldeten Delikten. Neben den klassischen Varianten, bei denen nichtexistierende Waren verkauft werden oder Waren nach der Bezahlung nicht geliefert werden, beobachtet das NCSC immer häufiger kombinierte Varianten, bei welchen Inserenten auf Kleinanzeigen-Plattformen die Kreditkartendaten gestohlen werden. Dazu betreiben die Betrüger einigen Aufwand und erstellen offiziell aussehende Webseiten von Paketdienstleistern. Dabei handelt es sich aber nicht um generische Webauftritte. Die Webseiten sind personalisiert und enthalten nicht nur den vermeintlichen Namen der Empfängerin oder des Empfängers, sondern auch eine Beschreibung und ein Bild des zu verkaufenden Artikels. Die Angreifer erstellen für jeden Verkäufer eine individuelle Webseite! Dieser Aufwand dient alleine dazu, die Skepsis beim Opfer abzubauen und dieses zu verleiten, schliesslich seine Kreditkartendaten anzugeben.

5.3 Statt Hauskauf winkt ein Erbe

Vorschussbetrug ist der Klassiker unter den Betrugsmails, die in grosser Zahl versendet werden. Angebliche Erbschaften und Lotteriegewinne sollen die Empfänger neugierig machen und sie verleiten, auf das Schreiben zu reagieren. Allerdings werden solche E-Mails mittlerweile von den meisten Empfängerinnen und Empfängern als betrügerisch erkannt und gelöscht. Betrüger testen deshalb neue Varianten, welche einen grösseren Erfolg versprechen. Bei einer solchen neuen Variante reagieren die Betrüger auf eine Immobilienanzeige. Dabei bekundet ein angeblicher Soldat, der in Afghanistan stationiert war und nun in der Schweiz eine neue Heimat sucht, Interesse an einer Immobilie. Nach zahlreichen vertrauensfördernden E-Mails, die im Zusammenhang mit dem zukünftigen Verkauf stehen, lenkt der angebliche Soldat die Diskussion auf ein Vermögen, das er angeblich besitze und welches er in der Schweiz investieren wolle. Dem Immobilienbesitzer wird dabei eine grosse Summe in Aussicht gestellt, wenn

er ihm bei der Investition helfe. Auch hier fallen früher oder später Gebühren an, welche das Opfer zu zahlen hat. Da die Geschichte frei erfunden ist, existieren weder der Soldat noch das Geld.

5.4 Investieren statt Ausleihen

Die digitale Form des Heiratsschwindels, sogenannter «Romance Scam» oder «Love Scam», wird bereits seit Jahren beobachtet. Bei dieser Betrugsart werden gefälschte Profile auf Social Media und Internet-Partnerbörsen erstellt, um anderen Personen eine Liebesbeziehung vorzuspielen und schliesslich finanzielle Zuwendungen des «Partners» zu erhalten. Auch hier wird es für die Betrüger zunehmend schwieriger, die Opfer zu einer Zahlung zu überreden, sei es für eine angeblich kranke Mutter oder irgendwelchen Schulden, die der angebliche Partner dringend zahlen soll und sonst auf der Strasse stehe. Diese Varianten sind weitherum bekannt und lassen beim potentiellen Opfer die Alarmglocken läuten. Auch hier suchen deshalb die Angreifer nach neuen Möglichkeiten. Häufig versuchen die Betrüger, das Opfer dazu zu überreden, auf einer Investment-Plattform zu investieren. Ein «Partner» oder «Bekannter» der Betrüger ist dabei entweder in dieser Branche tätig oder die Betrüger geben an, selbst bereits auf einer Plattform angeblich viel Geld verdient zu haben. Die Taktik ist klar. Der Betrüger lenkt von sich ab und gibt vor, wohlhabend zu sein. Anstatt dass er um Geld bettelt, lässt er das Opfer an seinem «Wissen» teilhaben und stellt so einen grossen Gewinn in Aussicht. Dass die Betreiber der vermeintlichen Investment-Plattform und der Lockvogel unter einer Decke stecken, ist für das Opfer praktisch nicht erkennbar.

Schlussfolgerung / Empfehlungen:

Zumindest teilweise verschieben Betrüger ihr Geschäftsfeld vom Massengeschäft zu individualisierten Angriffsversuchen. All diesen Varianten gemein ist, dass die Betrüger im Vorfeld über eine unterschwellige Kontaktaufnahme versuchen, Vertrauen beim Opfer aufzubauen. Es ist deshalb wichtig, dass man vorsichtig bleibt, auch wenn man das Gefühl hat, sein Gegenüber zu kennen. Das Internet ist und bleibt ein Ort, wo jeder und jede irgendeine Identität annehmen kann. Dies gilt auch für Profile auf bekannten Plattformen. Auch wenn über eine längere Zeit virtuell mit einer Person kommuniziert wird, heisst das noch lange nicht, dass das Gegenüber vertrauenswürdig ist.