GovCERT Austria

CERT.at

Bericht

Internet-Sicherheit

Österreich 2023

Inhaltsverzeichnis

Impressum

Medieninhaber und Verleger: nic.at GmbH, Computer Emergency Response Team Austria, Karlsplatz 1/2/9, 1010 Wien.
Diese Publikation wurde in Kooperation mit dem Bundeskanzleramt erstellt.

Konzeption und Redaktion: CERT.at

Herstellungsort: Wien, Jänner 2024.

Vorwort: Wolfgang Rosenkranz (CERT.at)

Sehr geehrte Leser:innen,

das Jahr 2023 war ein besonderes Jahr für die Digitalisierung und für das Thema Cybersicherheit. Nicht, weil es im Vergleich zu anderen Jahren besonders viele oder besonders komplexe Cyberangriffe zu bewältigen gegeben hätte. Sondern, weil das Thema ”Artificial Intelligence” einen bisher nie dagewesenen Höhenflug erlebt hat. Mit der Veröffentlichung von ChatGPT Ende 2022 wurde eine Welle an Berichten, Diskussionen und Analysen gestartet, die auch 2024 und vermutlich noch danach Auswirkungen haben wird. Dabei ist noch nicht wirklich absehbar, wohin der Weg tatsächlich geht.

Recht rasch war jedoch klar, dass die für Cybersicherheit zuständigen Personen Antworten liefern müssen, wenn gefragt wird, ob KI ein Werkzeug, eine Bedrohung oder nur ein temporärer Trend ist. Damit wurden auch das GovCERT und CERT.at gefragt und unsere eindeutige und typisch österreichische Antwort war ”schau ma mal” - denn auch wenn die Möglichkeiten von ChatGPT und Co beeindruckend sind, so bedeutet das noch nicht, dass daraus auch tatsächlich eine Bedrohung entsteht, die nicht mit den immer schon empfohlenen Maßnahmen bewältigt werden kann. Das Jahr 2024 wird hier hoffentlich mehr Einsicht bringen.

Eindeutiger war 2023 da schon in Bezug auf die Anforderungen, die aus NIS 2, DORA und anderen Regularien für die Verantwortlichen entstehen. Bis Jahresende gab es zwar noch keinen öffentlichen Entwurf der österreichischen Umsetzung der NIS 2 Richtlinie, also des Cybersicherheitsgesetzes. Aber schon alleine aus der NIS 2 Richtlinie konnte abgeleitet werden, dass die Auswirkungen weitreichend und tiefgreifend sein werden. Beispiele von kleinen Unternehmen, die bisher nie etwas mit Cybersicherheit zu tun hatten und nun unter NIS 2 fallen, wurden bei jeder Gelegenheit diskutiert. Es ist damit jetzt schon klar, dass NIS 2 wesentliche Auswirkungen auf die Cybersicherheit in Österreich haben wird - welche es genau sind, werden wir aber erst im Laufe des kommenden Jahres verstehen.

Ein wichtiges Thema in NIS 2 und DORA ist die Lieferantensicherheit. Und das ist auch gerechtfertigt, war 2023 doch geprägt durch mehrere Sicherheitsvorfälle, die bei Dienstleister:innen oder Anbieter:innen von Third-Party-Software vorgefallen sind und die auf österreichische Unternehmen und Behörden wesentliche Auswirkungen hatten. Eine Sicherheitslücke in der Software MoveIT-Transfer beschäftigte CERT.at und GovCERT für mehrere Wochen, da unter anderem die Finanzmarktaufsicht (FMA) betroffen war. Von Seite der FMA wurde rasch die Öffentlichkeit informiert, was als positives Beispiel für offene Kommunikation dienen sollte. Aber auch andere Organisationen in Österreich waren betroffen und die Analyst:innen von CERT.at haben mit viel Einsatz dabei geholfen, die gesamten Auswirkungen der Schwachstelle und der durch deren Ausnutzung ermöglichten Angriffe zu verstehen und zu bewältigen.

Ein weiteres Thema im Bereich der Lieferantensicherheit war der Diebstahl eines für Cloud Systeme notwendigen kryptographischen Schlüssels bei Microsoft, dessen Auswirkungen auch vor Österreich nicht halt machten. Dabei hat sich wieder einmal gezeigt, wie wichtig es wäre, dass große Unternehmen wie Microsoft Security-Ansprechpartner:innen in Österreich oder zumindest in der EU hätten. Denn viel Zeit wurde darauf verwendet, von Microsoft zu erfahren, welche Unternehmen und Organisationen in Österreich betroffen waren. Der Vorfall hat auch erneut gezeigt, dass immer ein Notfallplan für solche Szenarien vorhanden sein muss, weil sie nicht

ausgeschlossen werden können und dürfen.

Positiv war an 2023, dass Cybersicherheit in vielen Veranstaltungen Kernthema war. Die IKT Sicherheitskonferenz des Bundesheeres wurde von mehreren tausend Personen besucht. Die Immobilienbranche hat sich mit einer Cybersecurity-Veranstaltung in die Diskussion eingebracht, die Aufsichtskonferenz der FMA hatte DORA im Fokus, und ein KSÖ Cybersecurity Planspiel ermöglichte das Üben der Zusammenarbeit über Organisationsgrenzen hinweg.

Die Veranstaltungen des Austrian Trust Circle sind nach den durch die Pandemie bedingten Einschränkungen wieder in den vollständigen Regulärbetrieb übergegangen und rechtzeitig vor Jahresende wurde auch der von CERT.at und der Universität Wien organisierte IT-Security Stammtisch hybrid, so dass auch hier wieder persönliche Treffen möglich waren.

Das Thema Cybersecurity wird daher 2024 ein vorrangiges Thema bleiben und mit der Vorbereitung durch die Arbeiten in 2023 steht einem erfolgreichen Jahr nichts im Wege. Ich wünsche daher allen Leser:innen dieses Jahresberichtes viel Vergnügen bei der Lektüre und dass Österreich auch im kommenden Jahr cybersicher bleibt!

Wolfgang Rosenkranz

Teamleiter CERT.at

Kapitel 1

CERT.at und GovCERT Austria

CERT.at als nationales Computer-Notfallteam nach NIS-Gesetz und GovCERT Austria leisten einen wichtigen Beitrag für die IT-Sicherheit in Österreich und seiner Behörden. Eine enge Zusammenarbeit hilft dabei, Probleme flächendeckender angehen zu können.

1.1 CERT.at – Österreichs nationales CERT

CERT.at ist das österreichische nationale Computer-Notfallteam, das im Jahr 2008 gemeinsam mit dem GovCERT Austria vom Bundeskanzleramt (BKA) in Kooperation mit nic.at, der österreichischen Domain-Registrierungsstelle, als Projekt bei nic.at eingerichtet wurde. Als solches ist CERT.at die Anlaufstelle für IT-Sicherheit im nationalen Umfeld und ist für all jene Fälle zuständig, die nicht durch ein spezifischeres CERT (etwa ein Sektor-CERT) abgedeckt werden. Seit 2019 ist CERT.at außerdem das nationale Computer-Notfallteam nach NIS Gesetz. Dadurch ist die Zusammenarbeit mit Betreibern wesentlicher Dienste, der kritischen Infrastruktur und relevanten staatlichen Einrichtungen noch enger geworden.

CERT.at vernetzt andere CERTs (Computer Emergency Response Teams) und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen der kritischen Infrastruktur und IKT, (Informations- und Kommunikationstechnologie) und gibt Warnungen, Hinweise auf konkrete Probleme und Tipps für Unternehmen und Privatpersonen heraus. Bei Angriffen auf IKT auf nationaler Ebene koordiniert CERT.at die Reaktion auf den Vorfall und informiert die jeweiligen Netzbetreiber:innen und die zuständigen, lokalen Security Teams. Das Team von CERT.at wird in erster Linie bei akuten Sicherheitsbedrohungen und -ereignissen aktiv.

Damit ist CERT.at in seinem Tätigkeitsfeld mit einer gesamt-österreichischen “Internet-Feuerwehr” gleichzusetzen, die laufendes Monitoring betreibt, Informationen weitergibt, sich effektiv national und international vernetzt und auf Bedrohungen reagiert. Parallel zu CERT.at wurde 2008, im Rahmen einer Public-Private-Partnership mit dem Bundeskanzleramt, GovCERT Austria für den öffentlichen Sektor ins Leben gerufen. Seit 2017 besteht, in einer ähnlichen Kooperation des österreichischen Energiesektors mit CERT.at, auch das Austrian Energy CERT.

Darüber hinaus ist CERT.at auch für vorbeugende Maßnahmen, wie Früherkennung, Vorberei-

tung für Notfälle, Öffentlichkeitsarbeit und Beratung zuständig. CERT.at versteht sich als zentraler Ansprechpartner für sicherheitsrelevante IKT-Ereignisse in Österreich und dient als vertrauenswürdige und anerkannte Informationsdrehscheibe. Das Team von CERT.at besteht derzeit aus 13 Personen und wird von Robert Schischka als Geschäftsführer und Wolfgang Rosenkranz als Teamleiter geleitet. Eine wichtige Abgrenzung: CERT.at ist keine Ermittlungsbehörde und befasst sich daher nicht mit dem Thema der Strafverfolgung im Internet. Es hat kein Durchgriffsrecht auf die Netzwerkinfrastruktur Österreichs und kann bei Sicherheitsvorfällen nur koordinierend und beratend aktiv werden.

1.1.1 CERT-Beirat – Strategische Leitplanken

In seiner strategischen Ausrichtung wird CERT.at durch einen eigenen Beirat unterstützt, dessen Mitglieder einen Querschnitt der österreichischen Internetgemeinde repräsentieren.

Sie fungieren als Botschafter:innen für CERT.at und stellen sicher, dass CERT.at mit Hinblick auf, sowie im Sinne des ganzen Landes agiert. Als beratendes Organ liefert er wichtige Beiträge sowie Themenvorschläge für zukünftige Tätigkeiten, um die IT-Sicherheit und die Resilienz vernetzter Systeme in ganz Österreich zu stärken.

Die Mitglieder des CERT-Beirats waren 2023:

- DI Philipp Blauensteiner (BVT)
- Mag. Wolfgang Ebner (BMDW)
- Michael Eichinger (BMI)
- Univ. Prof. Dr. Nikolaus Forgo (Universität Wien)
- Andreas Koman (Internetstiftung)
- Ing. Thomas Mandl (CDCE)
- Ing. Clemens Möslinger, BA MSc (BKA)
- Christopher Ozvald (BMG)
- Christian Panigl (UniVie/ACOnet/VIX)
- Univ. Prof. Dr. Reinhard Posch (TU Graz)
- Ing. Robert Scharinger, MBCS (Gesundheitsministerium)
- Lambert Scharwitzl (BMLV)
- Andreas Schildberger (BOKU)
- Robert Schischka (nic.at)
- Ing. Dr. iur Christof Tschohl (Research Institute & Co. KG)
- Christian Zec (BKA)

- Markus Kloibhofer (BMF)
- Franz Hoheiser-Pförtner (Wien)

1.1.2 Vernetzung

CERT.at ist keine isoliert arbeitende Einrichtung, sondern vielmehr eine koordinierende und informierende Stelle, die bei Angriffen auf IKT Geräte sofort mit den jeweiligen Netzbetreiber:innen und zuständigen Security Teams in Kontakt tritt. Ein Expert:innen-Team, das im Falle des Falles Hilfe zur Verfügung stellt und in enger Abstimmung mit anderen Beteiligten den österreichischen Teil des Internets von Problemen befreit – auf Basis eines freiwilligen Angebots.

Die Zusammenarbeit mit anderen Organisationen ist daher ein wichtiger Bestandteil der täglichen Arbeit von CERT.at: Diese reicht von der EU-Agentur für Cybersicherheit ENISA, internationalen Konzernen, über CERTs/CSIRTs in anderen Staaten, anderen Sicherheitsteams in Österreich, Universitäten, Fachhochschulen, Forschungseinrichtungen bis hin zu engagierten Privatpersonen.

1.1.3 Gesetzlicher Auftrag von CERT.at

Die Europäische Union hat die Notwendigkeit einer gemeinsamen Gefahrenabwehr längst erkannt. Mitte 2016 trat die NIS-Richtlinie in Kraft, die “Directive on Security of **N**etwork and **I**nformation **S**ystems” (NISG). Sie stellt einen einheitlichen Rechtsrahmen dar, innerhalb dessen jedes Land Kapazitäten für die Cyber-Sicherheit aufbauen muss. Zudem formuliert sie Mindestsicherheitsanforderungen und Meldepflichten für kritische Infrastrukturen und für das Angebot bestimmter digitaler Dienste wie Cloud-Services oder Online-Marktplätze.

Österreich hatte bereits 2013 eine IT-Sicherheits-Strategie vorgestellt, die viele Punkte der Richtlinie vorwegnahm. Eines ist jedoch neu: Die Richtlinie verlangt von jedem Land, dass es ein offizielles Computer-Notfallteam einrichtet. Auf dieser rechtlichen Grundlage (§15 Abs. 3 NISG) hat das BKA – als zuständige NIS-Behörde – im März 2019 CERT.at mit dieser Rolle betraut, ohne aber dessen Unabhängigkeit und Vertraulichkeit anzutasten.

1.2 GovCERT Austria – Expertise im Behördenbereich

GovCERT Austria ist das Government Computer Emergency Response Team für die öffentliche Verwaltung in Österreich. Damit dient es auf nationaler Ebene als primäre Anlaufstelle für die einzelnen Stellen der öffentlichen Verwaltung im Falle eines Cyberangriffes. Für diese erfüllt es die Funktion des Computer-Notfallteams nach NISG, die CERT.at in den anderen Bereichen abdeckt.

Auf internationaler Ebene agiert GovCERT Austria als österreichischer Ansprechpartner für Regierungen und internationale Organisationen bei Fragen der IKT-Sicherheit. Es tauscht Informationen und Warnungen mit diesen aus und leitet sie bei Bedarf an inländische Interessent:innen weiter. GovCERT Austria erfüllt dabei seine Arbeit und Aufgaben in Personalunion mit CERT.at.

Das GovCERT leistet, neben der oben beschriebenen Rolle als Internetfeuerwehr und intensiver Netzwerker im öffentlichen Bereich, zentrale Aufgaben in der Koordination zwischen den einzelnen Stellen der öffentlichen Verwaltung in Angelegenheiten der Cybersicherheit.

Im Zentrum stehen für GovCERT dabei die Sammlung und Bewertung von Vorfällen aus dem operativen IKT-Betrieb der Bundes-, Landes-, Städte- und Gemeindeverwaltungen sowie der verfassungsmäßigen Einrichtungen des Bundes, das Setzen von Präventivmaßnahmen sowie die Bündelung sicherheitstechnischer und operativer Expertise für den Bereich der öffentlichen Verwaltung.

Das GovCERT überwacht dabei Sicherheitsvorfälle auf nationaler Ebene und gibt Warnungen und Alarmmeldungen sowie Bekanntmachungen über Risiken und Vorfälle heraus. Es reagiert auf Sicherheitsvorfälle, unterstützt bei Bedarf auch vor Ort und erweitert sein Wissen und Netzwerk durch die Koordination und Teilnahme an nationalen und internationalen Cyber-Übungen.

1.2.1 Public-Private-Partnership mit vielen Vorteilen

Da das GovCERT als Public-Private Partnership (PPP) des Bundeskanzleramtes mit nic.at eingerichtet wurde und auf das gleiche technische Team wie CERT.at zurückgreift, erhält der Staat Zugriff auf qualifizierte, technische Cybersicherheitsexpertise aus dem Privatsektor sowie auf das Kontaktnetzwerk von CERT.at, welches nationales und internationales Know-how und relevante Sicherheitsinformationen (z.B. klassifizierte Dokumente, White Papers usw.) bereithält.

Hinzu kommt die Mitarbeit an und das Teilen von gesamtstaatlichen Cyberlagebildern im Rahmen von OpKoord[1] und IKDOK[2] und die Teilnahme an Expert:innenworkshops, Trainings und sonstigen einschlägigen Fach- und Netzwerkveranstaltungen.

1.3 Kernaufgaben von CERT.at und GovCERT Austria

Die Notwendigkeit der von CERT.at und GovCERT Austria wahrgenommenen Aufgaben wird durch die gestiegenen IT-Sicherheitsbedrohungen der letzten Jahre deutlich: Systeme werden immer komplexer, immer mehr Geräte sind online erreichbar und Angreifer:innen agieren immer professioneller.

CERT.at und GovCERT Austria erfüllen, zusammen und in ihrem jeweiligen Zuständigkeitsbereich, eine Reihe unverzichtbarer Aufgaben, um den Anstieg dieser Bedrohungen effektiv zu bewältigen:

Information in allen Bereichen: CERT.at und GovCERT Austria verfolgen laufend die Nachrichtenlage zur globalen IT-Sicherheit. Daraus entstehen Warnungen (via Web, Mail, RSS, Presse, Twitter) für potentiell Betroffene, wenn akuter Handlungsbedarf aufgrund neuer Erkenntnisse

[1] Operative Koordinierungsstrukturen im Cybersicherheitsfall.
[2] Der **I**nneren **K**reis **d**er **o**perativen **K**oordinierungsstrukturen nimmt zentrale Aufgaben der OpKoord wahr.

besteht. Die CERTs erstellen auch Tageszusammenfassungen der wichtigsten Meldungen betreffend IT-Security und sind Ansprechpartner für Medien, Unternehmen und Öffentlichkeit bei Fragen zu aktuellen IT-Security Themen.

Netzwerkhygiene: CERT.at sammelt Informationen zu konkreten Sicherheitsproblemen im österreichischen Teil des Internets, wie etwa infizierte Computer, manipulierte Webseiten oder falsch konfigurierte Server. Dazu stützen sich CERT.at und GovCERT Austria neben eigener Sensorik auf Quellen[3] innerhalb der internationalen Gemeinschaft der IT-Sicherheitsbranche. Ziel ist es, das Niveau der Netzwerksicherheit in Österreich durch die Übermittlung von Informationen über Sicherheitsprobleme an Betroffene laufend zu heben.

Reaktion bei Vorfällen: CERT.at und GovCERT Austria unterstützen im Rahmen ihrer Möglichkeiten und Vorgaben bei Sicherheitsvorfällen. Während sich dieser Support in den meisten Fällen auf die Bereitstellung von Informationen wie etwa technischer Hinweise oder Verweise auf kommerzielle Anbieter für Internet Service Provider (ISPs) bzw. Domaineigentümer beschränkt, agieren CERT.at und GovCERT Austria bei größeren Vorfällen als Koordinationsstelle und Schnittstelle zwischen den Betroffenen und anderen relevanten AkteurInnen auf nationaler und internationaler Ebene. Dabei werden auch Handlungsanleitungen bereitgestellt und Informationen geteilt, wie Bedrohungen am besten beseitigt werden können.

Vernetzung: Neben der reinen technischen Rolle der CERTs als Informationsdrehscheibe und Hilfe bei Vorfällen fungieren sie auch als Kristallisationspunkt für die Vernetzung der in diesem Bereich arbeitenden Fachleute. Das reicht von selbst organisierten Foren wie dem Austrian Trust Circle oder dem IT Security Stammtisch, der aktiven Teilnahme an anderen Veranstaltungen der IT Security Community bis hin zur Mitarbeit bei Forschungsprojekten. Ebenso liefert das CERT Entscheider:innen technische Expertise, um die Entwicklung von Gesetzen und Richtlinien im Sinne der Cybersicherheit positiv zu unterstützen.

1.4 Zertifizierungen 2023

1.4.1 ISO 27001 Zertifizierung

Unternehmen müssen sich umfassend gegen Angriffe auf ihre Daten und Netzwerke absichern. Auch CERT.at muss nicht nur für die Sicherheit im Internet in Österreich sorgen; auch die Sicherheit der eigenen IT-Systeme und der eigenen Infrastruktur ist ein entscheidender Faktor.

Eine Zertifizierung nach ISO 27001/2013 ist der Nachweis, dass IT-Sicherheit in einem Unternehmen umfassend behandelt wird und umfasst, neben der Prüfung der Sicherheit der technischen Systeme und der Sicherheit der physischen Infrastruktur, auch organisatorische Aspekte. Die ISO 27001 Zertifizierung ist ein Gütesiegel nach außen und zum anderen auch ein laufender Ansporn für die Sicherstellung der eigenen Sicherheit nach innen. Jährliche Audits bei CERT.at stellen sicher, dass dieser Standard auch gehalten wird.

[3] Eine ausführliche Beschreibung der verwendeten Quellen findet sich in 2.6 Tooling.

nic.at wurde bereits im Jahr 2014 ISO 27001 zertifiziert. Gemeinsam beschloss man im Zuge des ersten großen Re-Audits von nic.at (nach drei Jahren) auch die Zertifizierung von CERT.at und GovCERT Austria anzustreben. Eine gemeinsame Zertifizierung von nic.at und CERT.at im Jahr 2014 wäre wegen der unterschiedlichen Anforderungen und getrennten Systemen zu aufwendig gewesen. Der notwendige Prozess und alle Maßnahmen zur ISO-Zertifizierung von CERT.at und GovCERT Austria wurden im Jahr 2017 erfolgreich abgeschlossen, und 2023 im Rahmen einer Re-Zertifizierung bestätigt.

1.4.2 TI Zertifizierung

Das **Trusted Introducer (TI) Service** ist eine Einrichtung des europäischen Verbands der CSIRTs (TF-CSIRT), die die Vertrauenswürdigkeit und den Reifegrad von Teams im europäischen CERT-Netzwerk mithilfe der Stufen “listed”, “accredited” und “certified” dokumentiert. Wer in der TI-Datenbank aufscheint, belegt damit das Vertrauen seiner Peer-Group, was ein wichtiges Kapital in der IT-Sicherheitsbranche darstellt.

Im Jahr 2017 hat CERT.at den Schritt von der TI-Akkreditierung hin zur Zertifizierung gemacht. Dieser Prozess, der durch das TF-CSIRT-Netzwerk und damit die Branche selbst durchgeführt wird, überprüft die Organisation, die internen Sicherheitsmaßnahmen und Arbeitsprozesse des betroffenen CERTs anhand des international anerkannten SIM3 Reifegradmodells. CERT.at konnte diesen Prozess erfolgreich abschließen und ist (mit Stand 2023) eines von 11 nationalen CERTs in Europa, das mit dem TI-Prädikat “Certified” ausgezeichnet wurde. Das ist die höchste Stufe des Trusted Introducer Zertifizierungsrasters. Das GovCERT wird als “accredited” geführt.

Kapitel 2

Das IT-Sicherheitsjahr 2023

CERT.at fungiert als Informationsdrehscheibe für alle Cybersicherheits-Themen in Österreich, ist also zuständig für sämtliche Sicherheitsprobleme von IKT-Geräten unter österreichischen IP-Adressen oder der Domäne .at. Dabei hat das nationale CERT keinerlei Exekutivgewalt und steht Betroffenen mit Informationen und Koordinationsleistungen zur Seite. Die ersten Ansprechpartner:innen sind hierbei die Expert:innen der Unternehmen und Internet Service Provider selbst, die sich in ihren Unternehmen um die Behebung von Sicherheitsproblemen kümmern.

Als öffentlich sichtbarer Ansprechpartner für das Thema Cybersicherheit. stellt CERT.at Warnungen und Informationen für die Öffentlichkeit bereit. Jede:r kann sich bei Interesse über die Webseite für Mailinglisten mit Warnungen und Informationen registrieren.

GovCERT.at ist spezialisiert auf alle Sicherheitsprobleme von IKT-Geräten, welche die öffentliche Infrastruktur betreffen.

2.1 NIS Meldungen

Das NIS Gesetz von Ende 2018 sieht vor, dass freiwillige und Pflichtmeldungen an die jeweils zuständigen Computer-Notfallteams übermittelt werden. CERT.at wurde am 20. März 2019 per Bescheid die Rolle des ”nationalen Computer-Notfallteams” zugewiesen, seit diesem Tag ist auch das Meldeportal unter https://nis.cert.at/ online.

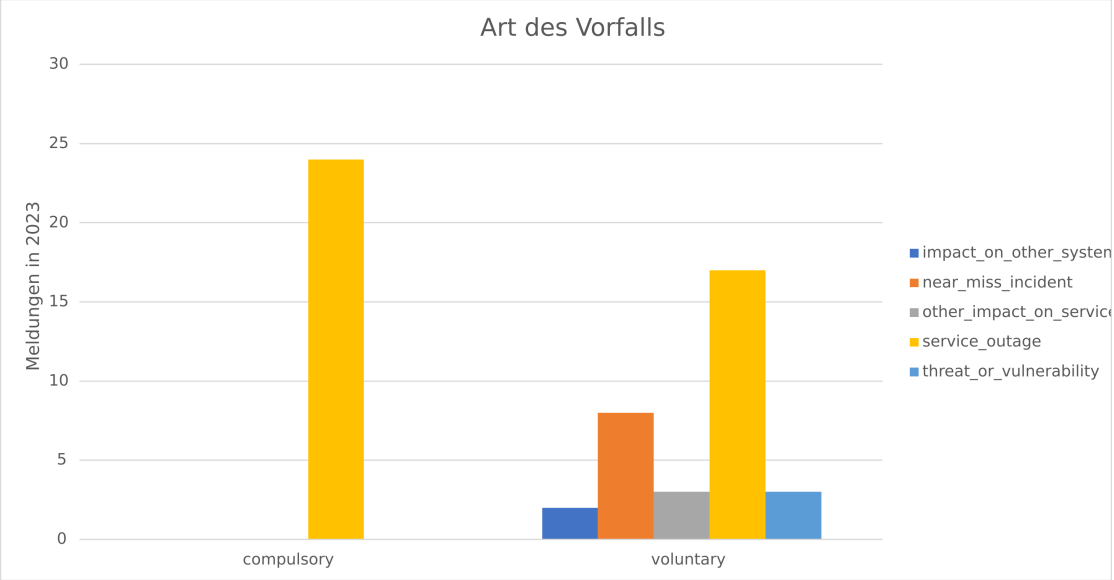


Abbildung 2.1: NIS Meldungen 2019 - 2023: Meldungsart

Pflichtmeldungen laut §19 (Betreiber wesentlicher Dienste) und §21 (Anbieter digitaler Dienste) NISG sind dann vorgeschrieben, wenn es zu einem Sicherheitsvorfall gekommen ist. Einen solchen definiert das Gesetz als ”eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat”.

Die Schranke für eine freiwillige Meldungen (§23 NISG) ist deutlich niedriger: einerseits reichen schon ”Risiken” und ”Vorfälle” bei Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste, um eine solche Meldung abzugeben, andererseits dürfen auch Einrichtungen die keiner Meldepflicht unterliegen, Vorfälle und Risiken bei sich melden. Im Gegensatz zu Pflichtmeldungen können freiwillige Meldungen anonym erfolgen und CERT.at kann diese Meldung aggregiert an das Innenministerium weiterleiten.

Die Zahl der Meldungen liegt unter den Erwartungen, insbesondere bei den freiwilligen Meldungen bestand die Hoffnung, dass diese die Grundlage für das nationale Lagebild zur Cybersicherheit in Österreich bilden werden. Aufgrund der geringen Anzahl an Meldungen liefert diese Informationsquelle keine ausreichende Datenbasis, um statistisch fundierte Aussagen treffen zu können.

Wichtig ist auch der Hinweis, dass ein Ausfall – egal aus welchem Grund – eines IT Systems, von dem ein Dienst abhängt, zu einer Meldepflicht führen kann. Daher sagt die Zahl der Pflichtmeldungen wenig über ”Cyberangriffe auf die kritische Infrastruktur” aus, weil fast alle dieser Meldungen auf normale ”IT Gebrechen” wie Hardwareausfälle, Softwareprobleme oder menschliche Fehler zurückzuführen waren.

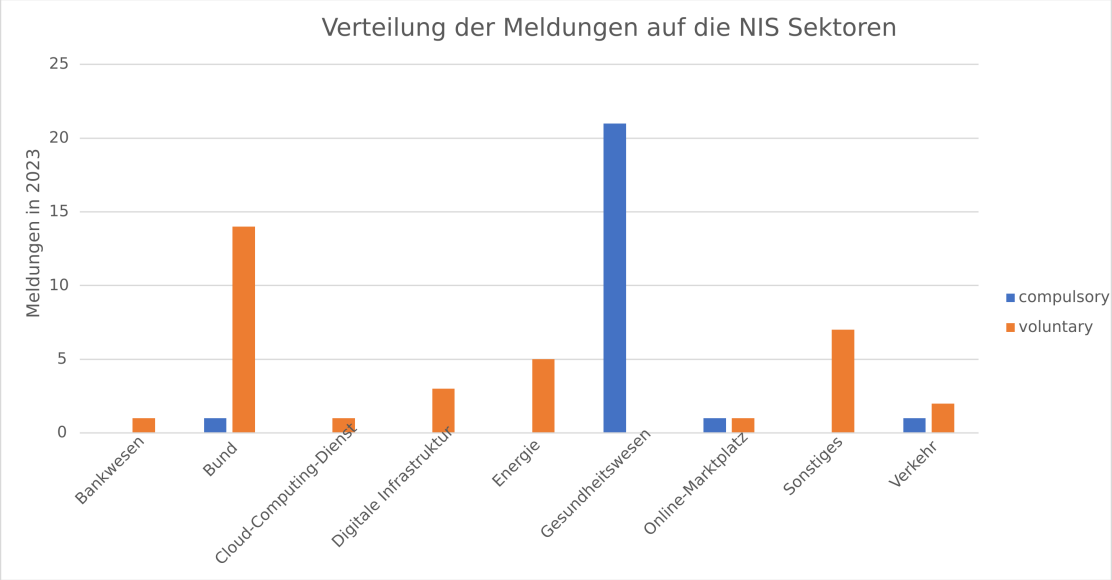


Abbildung 2.2: NIS Meldungen 2019 - 2023: Sektorenverteilung

2.2 Incident Reports, Incidents und Investigations

Eingehende und ausgehende Informationen werden bei CERT.at und GovCERT Austria über ein Ticketsystem (aktuell Request Tracker for Incident Response a.k.a. RTIR) abgehandelt. Dabei wird bei Vorfällen zwischen Incident Reports, Incidents und Investigations unterschieden:

Incident Reports sind Meldungen über Sicherheitsprobleme oder -vorfälle, die bei CERT.at eingehen. Diese werden anschließend als relevant, informativ oder als Fehlalarm kategorisiert. Als "informativ" sieht CERT.at Meldungen an, bei denen eine Weiterverarbeitung aufgrund verschiedener Faktoren nicht sinnvoll ist; beispielsweise Hinweise auf Opfer von bereits geschehenen DDoS Angriffen. Hier ist es nicht hilfreich, die Betroffenen über vergangene Attacken zu informieren, die sie aller Wahrscheinlichkeit nach ohnehin bemerkt haben.

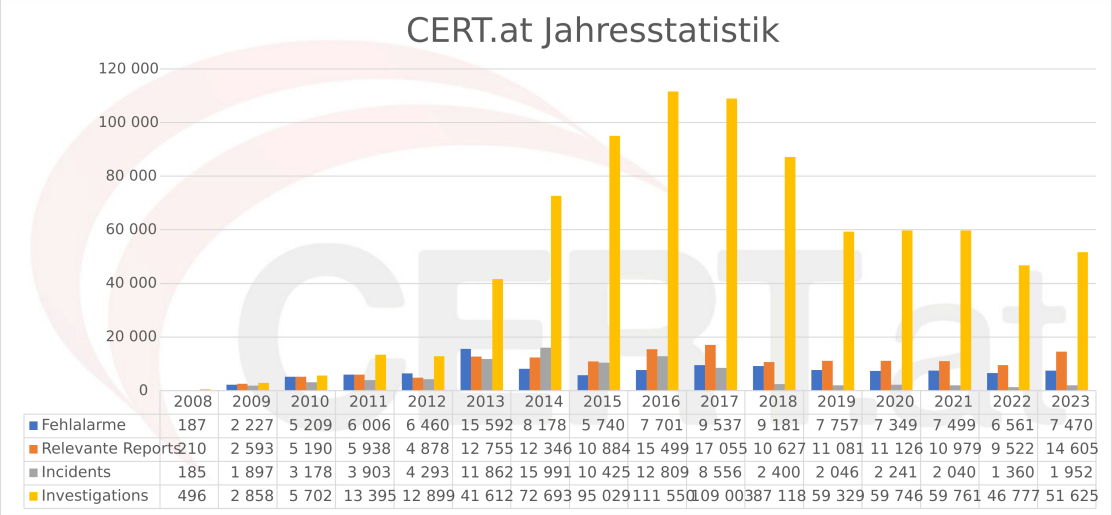
Incident Reports können sowohl von automatisierten Datenfeeds (siehe 2.5 Datenbasis) als auch von Privatpersonen stammen. Sie werden grundsätzlich vertraulich behandelt und können auch per PGP-verschlüsselte E-Mail übermittelt werden.[1]

Incidents werden aus Incident Reports generiert, die CERT.at als relevant eingestuft hat und denen daher nachgegangen wird.

Investigations schließlich meinen die Kontaktaufnahme von CERT.at mit Betroffenen. Auch diese kann automatisiert, wie im Falle von ISPs (Internet Service Providern), oder persönlich, wie bei einer Responsible Disclosure, erfolgen.

2016 wurde damit begonnen, die Abwicklung der Vorfallsbehandlung wo immer möglich zu automatisieren. Dieser Vorgang wurde Ende 2017 abgeschlossen, was es CERT.at ermöglicht, sich

[1] Unsere PGP-Keys finden Sie unter https://cert.at/static/pgpkeys.asc.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Fehlalarme	187	2 227	5 209	6 006	6 460	15 592	8 178	5 740	7 701	9 537	9 181	7 757	7 349	7 499	6 561	7 470
Relevante Reports	210	2 593	5 190	5 938	4 878	12 755	12 346	10 884	15 499	17 055	10 627	11 081	11 126	10 979	9 522	14 605
Incidents	185	1 897	3 178	3 903	4 293	11 862	15 991	10 425	12 809	8 556	2 400	2 046	2 241	2 040	1 360	1 952
Investigations	496	2 858	5 702	13 395	12 899	41 612	72 693	95 029	111 550	109 003	87 118	59 329	59 746	59 761	46 777	51 625

Abbildung 2.3: Incident Reports, Incidents und Investigations im Überblick

stärker auf Meldungen von Privatpersonen oder auch Firmen zu konzentrieren, anstatt täglich automatisierte Feeds manuell zu überprüfen. Eine weitere Folge dieses Umstands ist, dass Reports aus mehreren Datenquellen zuerst zusammengefasst, in ein einheitliches Format gebracht und danach gesammelt an Betroffene gesendet werden.

Diese Automatisierung geschieht mithilfe des Open Source Tools IntelMQ, das aktuell unter der Leitung von CERT.at von mehreren europäischen CERTs/CSIRTs entwickelt wird. Für nähere Informationen zur Software, siehe 2.6.1 IntelMQ.

Bei den Incident Reports und den Investigations überwiegt die Kategorie “vulnerable” bei weitem, während die Aufteilung bei den Incidents insgesamt wesentlich gleichmäßiger ist. Darin spiegelt sich die Tatsache wider, dass zu einem Incident mehrere Incident Reports und mehrere Investigations gehören können. Wenn wir also in einem Monat ähnlich viele Incidents unter den Kategorien “vulnerable” und “malicious code” haben, sagt dies erst einmal nichts über die Anzahl der zugehörigen Incident Reports und Investigations aus. Dadurch erklärt sich auch der Umstand, dass die Top 5 nicht identisch sind.

Ein Beispiel (mit erfundenen Zahlen): Wir erhalten an einem Tag aus acht verschiedenen Quellen Incident Reports zu offenen DNS Resolvern (Taxonomie “vulnerable”) und aus einer Quelle Incident Reports zu IP-Adressen, hinter denen von einem bestimmten Trojaner befallene Geräten (Taxonomie “malicious code”) erkannt wurden.

Diese werden dann jeweils unter einem Incident für alle offenen DNS Resolver und einem Incident für alle mit diesem Trojaner infizierten Geräte zusammengefasst. Insgesamt wurden uns 100 offene DNS Resolver gemeldet, die sich auf 20 Netzbetreiber verteilen, was zu 20 Investigations unter diesem Incident der Kategorie “vulnerable” führt, aber nur drei mit dem Trojaner infizierte Geräte, was zu lediglich drei Investigations unter dem Incident der Kategorie “malicious code” führt. So kommen eine ähnliche Anzahl von Incidents, aber sehr unterschiedlich viele Incident Reports und Investigations zustande.

Diese Zahlen repräsentieren entsprechend der Definitionen oben also die Anzahl der ein- und ausgehenden E-Mails von CERT.at. Auf die dahinterliegenden Daten, die die IT-Sicherheitslage

in Österreich beschreiben wird in 2.5 Datenbasis näher eingegangen.

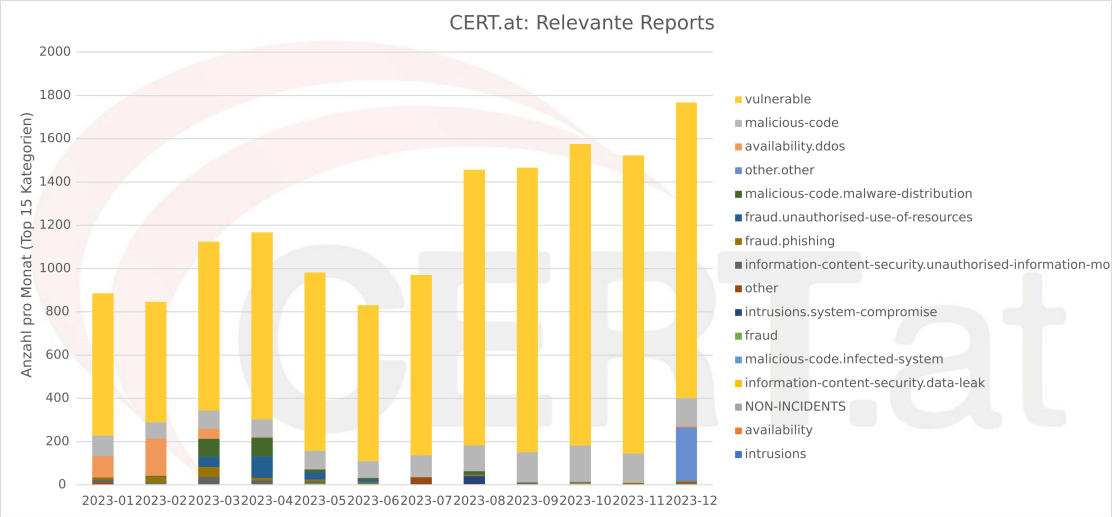


Abbildung 2.4: Incident Reports

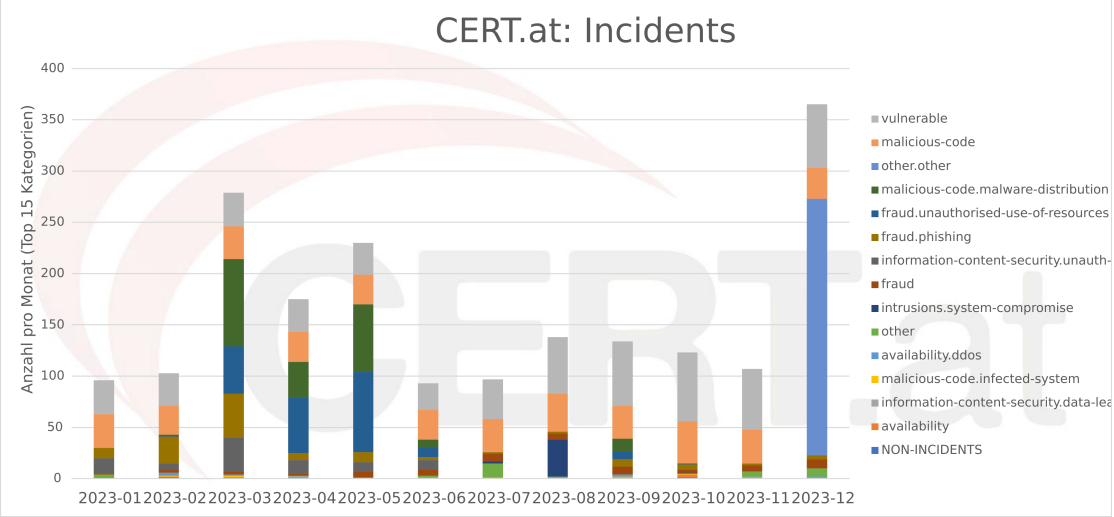


Abbildung 2.5: Incidents

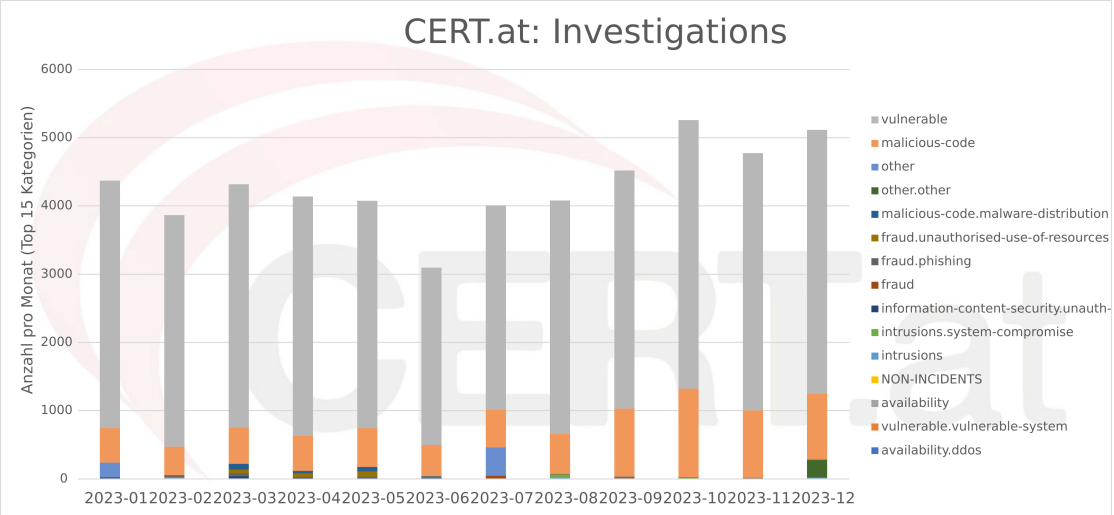


Abbildung 2.6: Investigations

2.3 Taxonomie

Um einen schnellen Informationsfluss innerhalb der IT-Sicherheits-Community gewährleisten zu können, braucht es eine gemeinsame Sprache. CERTs/CSIRTs, Strafverfolgungsbehörden, Sicherheitsfirmen und SicherheitsforscherInnen müssen sich auf gemeinsame Richtlinien zum Austausch von Informationen einigen, um im Notfall schnell eingreifen zu können. Auch eine automatisierte Verarbeitung von Reports ist nur möglich, wenn sich alle einer einheitlichen Sprache bedienen.

Die Taxonomie, auf die sich CERT.at stützt, ist die Reference Security Incident Taxonomy, die auf der älteren eCSIRT II Taxonomy (PDF) basiert. Die Kategorien dieser Taxonomie sind nicht exklusiv, d.h. mehrere Kategorien können auf einen Vorfall zutreffen. In Bezug auf Probleme mit Webservern verwendet CERT.at eine noch genauere Aufspaltung der einzelnen Kategorien.

Die Reference Security Incident Classification Taxonomy wird von einer eigenen Arbeitsgruppe der TF-CSIRT kontinuierlich weiterentwickelt, vgl. Reference Security Incident Taxonomy. Die aktuelle Version wird in einem lebenden Dokument auf GitHub veröffentlicht.

2.3.1 Reference Security Incident Taxonomy – ein kurzer Überblick

Abusive Content: Darunter fallen z.B. Spam, Hate-Speech, gewaltverherrlichende oder auch Child Sexual Abuse Material (CSAM).

Malicious Code: Gemeint sind dabei einerseits Computer, die Schadsoftware oder deren Konfiguration hosten bzw. als Command and Control Server fungieren und andererseits von Schadsoftware befallene Systeme.

Information Gathering: In dieser Kategorie findet sich neben rein technischen Vorgängen, wie dem Scannen nach Geräten, die für eine bestimmte Lücke anfällig sind, auch Social Engineering. Dabei wird versucht, über menschliche "Schwachstellen" an Informationen zu gelangen.

Intrusion Attempts: Bei einem Versuch, in ein System einzudringen, können unterschiedliche Methoden angewandt werden, wie z.B. das Ausprobieren von Passwörter oder das Ausnützen (un)bekannter Schwachstellen.

Intrusions: Ist ein Intrusion Attempt erfolgreich, liegt eine Intrusion vor. Auch hier ist zu beachten, dass neben den IT-basierten Einbrüchen, wie einer Account-Übernahme in manchen Fällen ganz "traditionelles", physisches Eindringen in Gebäude aus einer IT-Sicherheitsperspektive relevant sein kann.

Availability: Die Verfügbarkeit kann nicht nur durch Angriffe wie DoS (Denial of Service), DDoS (Distributed DoS) oder Sabotage beeinträchtigt werden, sondern auch durch andere Faktoren wie eine fehlerhafte Konfiguration oder Umwelteinflüsse.

Information Content Security: Hierunter fallen nicht authorisierte Zugriffe und Änderungen an Daten sowie Datenverlust. Wiederum gibt es unterschiedlichste Wege, wie so etwas zustande kommt, unter anderem durch gestohlene Zugangsdaten, fehlende Zugriffsbeschränkungen, kaputte Hardware, etc.

Fraud: Betrugsversuche treten online wie offline in verschiedensten Formen auf, von Phishing-Mails zu betrügerischen Pyramidenspielen und Urheberrechtsverletzungen.

Vulnerable: Dies bezeichnet einfach Systeme, die für diverse Angriffe verwundbar sind. Hier ist bei Aussendungen eine nähere Klassifizierung unerlässlich, siehe 2.4.1 Taxonomie "vulnerable".

Other: Eine Sammelkategorie für Vorfälle, die sonst nirgends einzuordnen sind. Das ist insofern nützlich, als ein starker Anstieg von Fällen mit dieser Klassifikation ein guter Indikator dafür ist, dass die Taxonomie insgesamt einer Überarbeitung bedarf.

Test: Für Testfälle.

2.4 2023 im Detail

Der größte Teil der Daten, die CERT.at ausschickt, kommt aus diversen automatischen Feeds.[2] Bevor sie über das Ticket-System ausgeschickt werden, werden sie, bereits taxonomisiert, in eine Datenbank geschrieben. Die folgenden Graphen basieren jeweils auf diesen Rohdaten. Dabei wurden jeweils die betroffenen IP Adressen pro Tag zugrundegelegt und anschließend die Wochenmaxima als Datenpunkte in den Graphen verwenden.

Im Verhältnis zu den Aussendungen ist zweierlei zu beachten:

1. CERT.at schickt Informationen zum gleichen Problem nur alle 30 Tage aus. Das heißt also, auch wenn wir jeden Tag die Information erhalten, dass auf IP Adresse X Port Y offen ist, obwohl er das wahrscheinlich nicht sein sollte, schicken wir das nicht täglich weiter, um die Betreiber/ISPs nicht mit Benachrichtigungen zu überfluten. Diese Deduplikation wurde in den Rohdaten noch nicht vorgenommen.
2. Gibt es in einem Netzwerk mehrere Fälle desselben Problems (z.B. Geräte, die für die gleiche Schwachstelle anfällig sind), leiten wir diese Informationen aggregiert an die Verantwortlichen weiter, d.h. hinter einer einzelnen Investigation können zahlreiche Datenbankeinträge a.k.a. “Events” stecken.

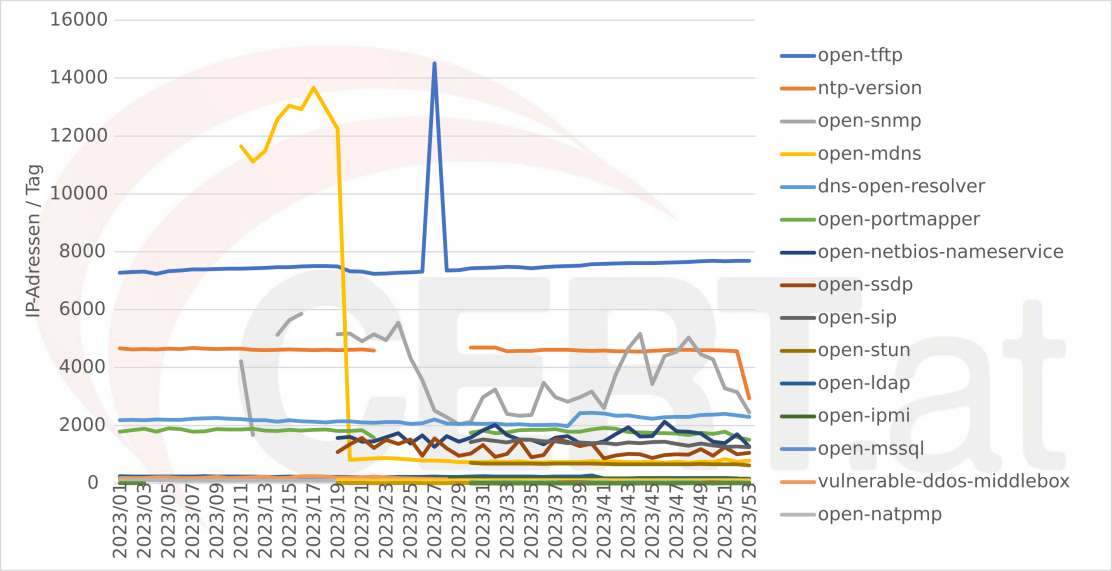


Abbildung 2.7: Events nach Taxonomie (logarithmische Skala)

Bei den Gesamtzahlen ist zu beachten, dass manche Events doppelt gezählt werden, nämlich dann, wenn sie in zwei unterschiedliche Taxonomien fallen. Das ist beispielsweise bei Services der Fall, die einerseits als DDoS-Amplifier missbraucht werden können, andererseits aber auch potentiell sensible Informationen preisgeben.

[2] Für eine genauere Beschreibung siehe 2.5 Datenbasis.

2.4.1 Taxonomie “vulnerable”

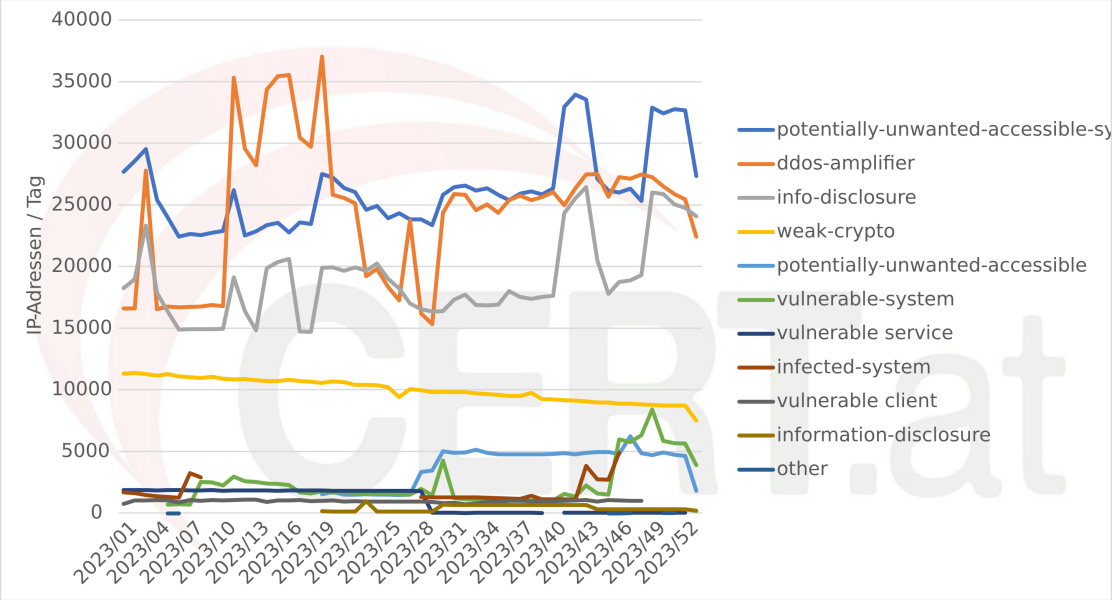


Abbildung 2.8: Alle Events der Taxonomie “vulnerable”

CWMP, RDP, Telnet, Portmapper und Netbios-Nameservice sind die Protokolle, die am häufigsten offen aus dem Internet erreichbar sind, obwohl es gute Gründe dafür gibt, sie besser abzusichern. So etwa sind Fernwartungszugänge direkt per RDP oft ein Faktor bei Ransomwarevorfällen. (Abb. 2.9)

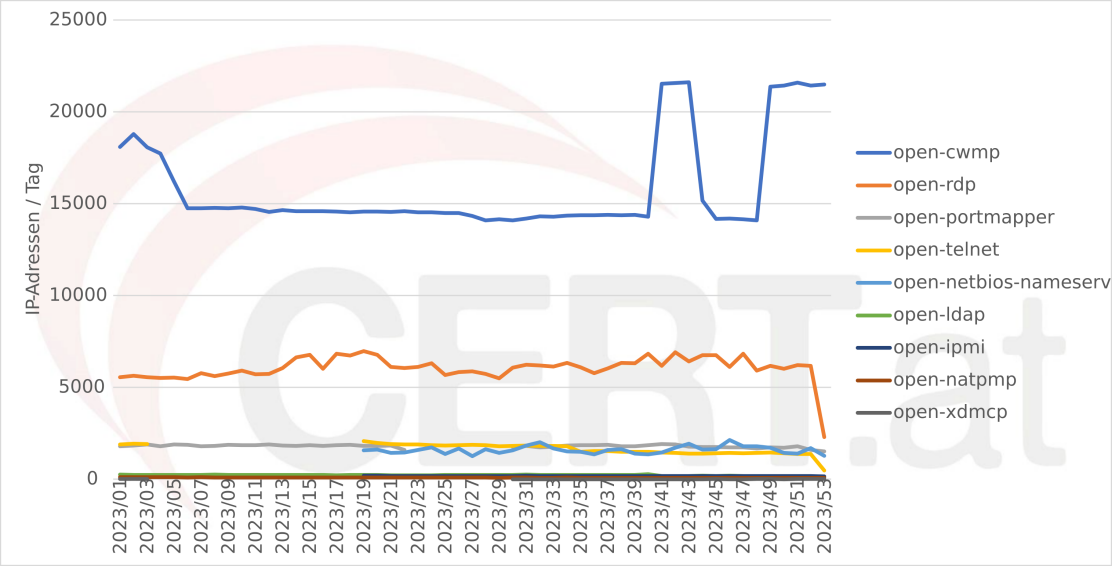


Abbildung 2.9: Ports, die nicht öffentlich erreichbar sein sollten

Bei einiges Protokollen/Services besteht die Gefahr eines Datenlecks. Man kann über sie potentiell Daten abrufen, die der Betreiber dieses Dienstes nicht bewusst veröffentlichen wollen.

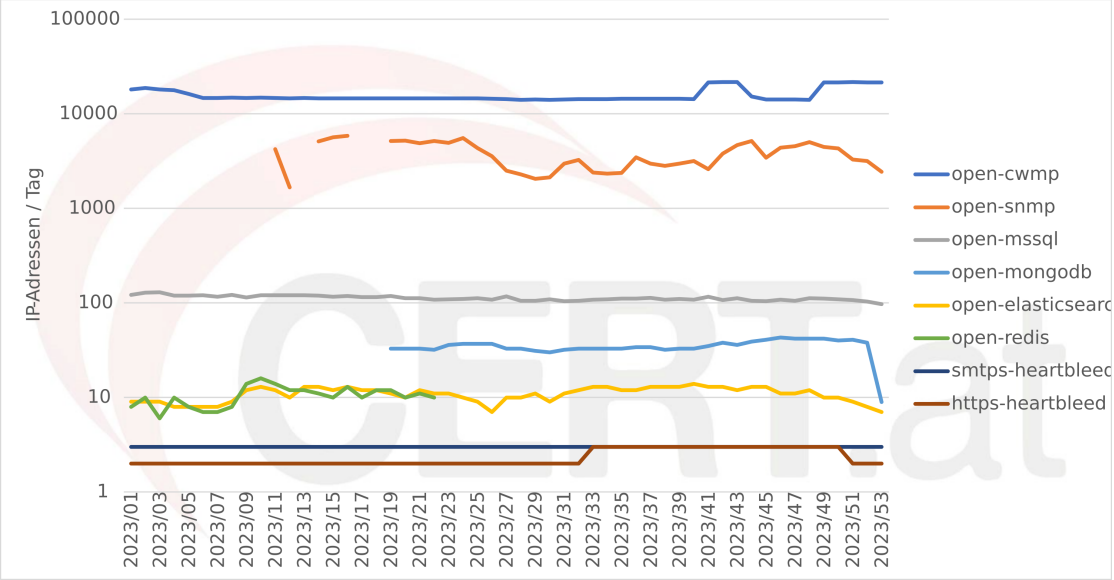


Abbildung 2.10: Services, über die sensible Informationen gewonnen werden können

Verwundbar kann aber auch heißen, dass der Computer anfällig dafür ist, sich für Angriffe auf Dritte einspannen zu lassen. Mit Hilfe solcher Reflektoren/Verstärker können Tätergruppen starke DDoS-Angriffe starten, die etwa für die Erpressungsversuche (siehe 2.8 Hilfe bei Vorfällen) benutzt werden. (Abb. 2.11)

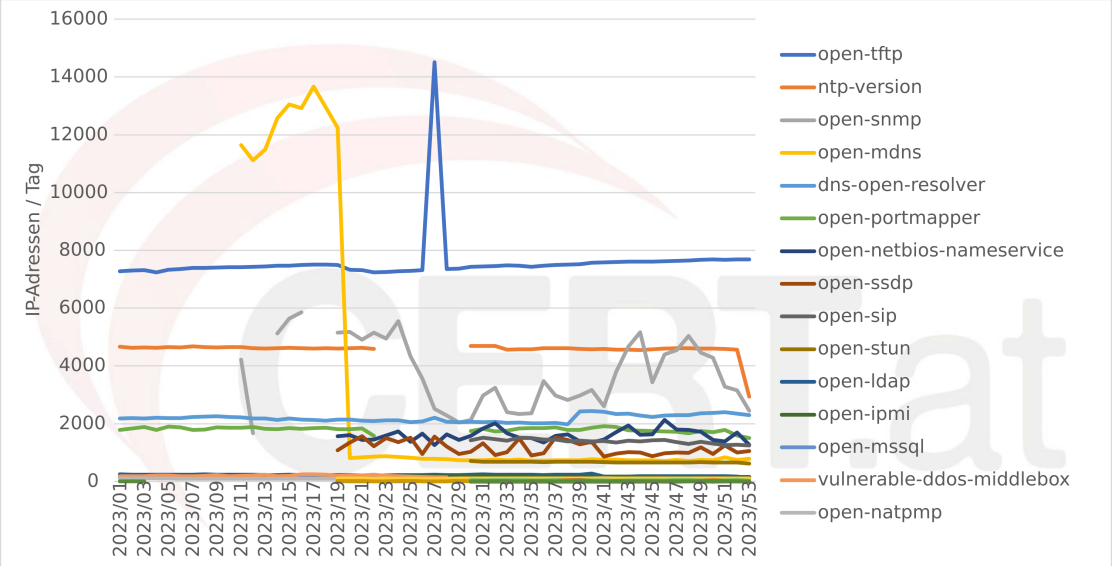


Abbildung 2.11: Geräte, die für UDP DDoS Amplifikation missbraucht werden können

Wie auch in den Jahren zuvor, fiel 2023 der größte Teil der von uns behandelten Meldungen in die Kategorie “vulnerable”, weshalb wir sie etwas näher vorstellen.

Warum hier immer die meisten Events auftreten, haben wir zwar nicht tiefgehend untersucht, gehen aber davon aus, dass hier eine Reihe von Faktoren zusammenspielen:

Default Konfigurationen: Vielfach ist es die voreingestellte Konfiguration von Software und Hardware, die diese aus dem öffentlichen Internet erreichbar macht. Gerade im Fall von IoT-Geräten und Home-Routern wissen die betroffenen NutzerInnen das oft gar nicht bzw. verfügen nicht über das technische Know-How, um Änderungen vorzunehmen (so das überhaupt möglich ist).

(Vergessene) "Spielwiesen": Technisch versierte NutzerInnen richten oft Testinstanzen ein, um neue Dinge auszuprobieren. Nicht selten wird dann aber darauf vergessen, diese wieder abzuschalten.

Risikoeinschätzung: Im Gegensatz zu Geräten, die mit Malware befallen sind, stufen viele die mit "potentiell verwundbaren" Computern verbundenen Gefahren als eher gering ein, v.a. wenn es sich z.B. um DDoS Amplifikatoren handelt – hier wird zwar das betroffene Gerät für einen Angriff missbraucht, der Schaden entsteht aber nicht bei den Betreiber:innen des Geräts, sondern beim Opfer des Angriffs.

Shodan "Verified Vulnerabilities"

Im Jahr 2020 veröffentlichte die Suchmaschine Shodan ein neues Feature zur Schwachstellenanalyse. Diese "Verified Vulnerabilities" zeigen ihrem Namen entsprechend Schwachstellen an, die Shodan gefunden und verifiziert hat.[3] Diese Funktionalität ist nur für eine begrenzte Anzahl von IP Adressen anwendbar; im Falle von CERT.at sind das all jene, die in Österreich geolokalisiert sind. Diese Informationen werden automatisiert an ausgesuchte Netzverantwortliche geschickt, um diese bei der Erhaltung der "Netzhygiene" zu unterstützen.

2.4.2 Veraltete Kryptographie

Verschlüsselung bei Web- und E-Mail-Servern ist heutzutage erfreulicherweise weit verbreitet. Allerdings werden immer wieder Schwachstellen in kryptographischen Verfahren gefunden, die eine Aktualisierung der betroffenen Server notwendig machen. Das geschieht leider nicht immer sofort und zieht sich meist über viele Jahre oder sogar Jahrzehnte, bis es keine verwundbaren Server mehr gibt.

[3] Die genaue Methodik dazu, ist je nach Schwachstelle unterschiedlich und auch nicht in allen Fällen gleich verlässlich, wie sich aus diesem Twitter-Thread ableiten lässt.

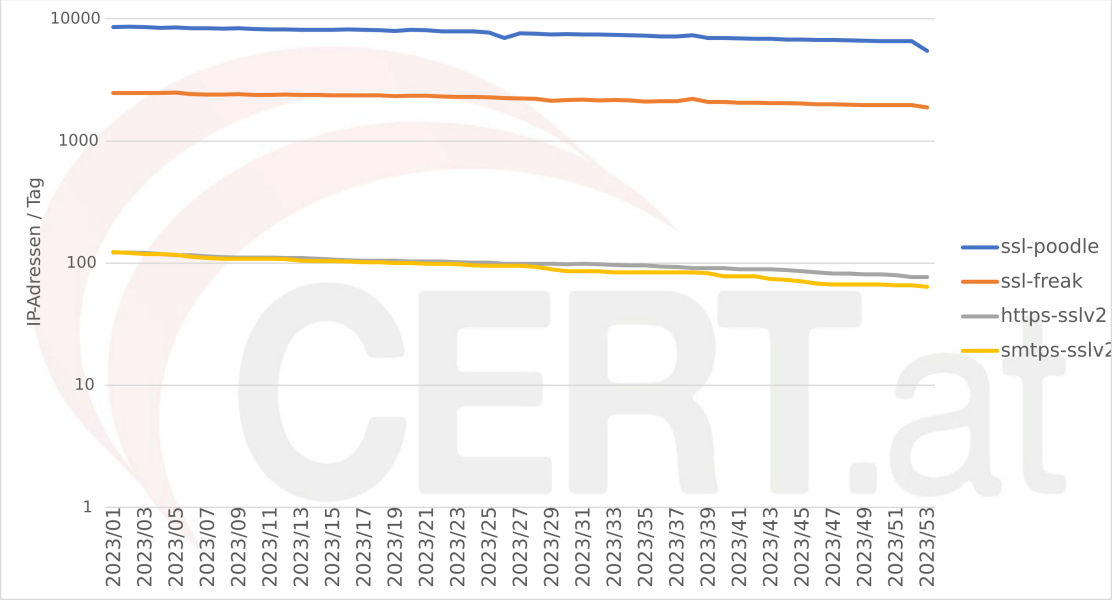


Abbildung 2.12: Unsichere Kryptographie

2.4.3 Malware

Im Jahr 2023 hat sich im Bereich Malware, wie jedes Jahr, einiges getan. Trotz der ständigen Fortschritte in der Cybersicherheit haben Cyberkriminelle weiterhin neue Wege gefunden, Malware zu entwickeln und zu verbreiten, um Schaden zu verursachen und persönliche und geschäftliche Informationen zu stehlen.

Vor allem Ransomware-Angriffe auf Unternehmen, Regierungen und kritische Infrastrukturen weltweit haben erhebliche Schäden verursacht, darunter finanzielle Verluste in Millionenhöhe und erhebliche Störungen des Betriebs.

Jedoch konnten nationale und internationale Strafverfolgungsbehörden einige wichtige Erfolge im Kampf gegen verschiedene kriminelle Bedrohungsakteure erzielen. Unter anderem konnten die Ermittler:innen erfolgreich die Infrastruktur der Ransomware ”Hive” zerschlagen und die Systeme hinter der Schadsoftware ”Qakbot” aus dem Verkehr ziehen.

2.5 Datenbasis

Informationen über Probleme in der IT-Sicherheit sind die Grundvoraussetzung für die Arbeit von CERT.at und GovCERT Austria. Sie sind nicht nur notwenig, um einen Überblick zur Lage in Österreich und den staatlichen Institutionen zu haben, sondern dienen dem noch wichtigeren Zweck, Betroffene schnell über Probleme zu informieren, damit diese behoben werden können.

Die Daten werden einerseits von CERT.at bzw. GovCERT Austria direkt erhoben und stammen andererseits von diversen externen Quellen.

2.5.1 Eigene Erhebungen

Scanning Tools

Für die Suche nach ausgewählten verwundbaren Software-Installationen verwendet CERT.at `masscan` oder andere, zum Teil selbst geschriebene Scanning Tools bzw. Suchmaschinen wie shodan.io. Die selbst geschriebenen Webscanner melden sich als:

```
CERT.at-Statistics-Survey/1.0 (+http://www.cert.at/about/consec/content.html)
```

Die Liste der aktuellen Scans findet sich eben auf der darin verlinkten Webseite. Der Suchbereich beschränkt sich hierbei üblicherweise auf IP-Ranges mit Bezug zu Österreich oder auf .at-Domains.

Der Ablauf eines Scans stellt sich gewöhnlich folgendermaßen dar:

1. Aktuelle IP-Ranges/.at-Domains holen
2. Versuch eines initialen TCP Handshakes mit jedem so identifizierten Server auf dem/den Port(s) für den jeweiligen Scan.
3. Abspeichern, welche Handshakes erfolgreich waren, da dies auf eine mögliche Schwachstelle bzw. Infektion hinweist.
4. Verifikation der Schwachstelle,[4] sofern es unbedenkliche Möglichkeiten dazu gibt. "Unbedenklich" meint beispielsweise, wenn ein einfacher `HEAD`-Request auf eine URL und der HTTP Response-Code ausreichen, um die Anfälligkeit zu bestätigen/widerlegen.

2023 führte CERT.at folgende Scans regelmäßig durch:

SSLv2 ist ein 1995 veröffentlichtes Protokoll zur Verschlüsselung von z.B. Web- und E-Mail-Verkehr. Es weist gravierende Schwachstellen auf Protokoll-Ebene auf und sollte daher nicht mehr eingesetzt werden. CERT.at versucht dabei mit allen .at-Domains eine SSLv2 Verbindung für HTTPS und SMTP mit STARTTLS aufzubauen. Ist eine Anfrage erfolgreich, verschickt CERT.at eine Warnung an die Betroffenen.

Heartbleed war ein Fehler in der OpenSSL Bibliothek (CVE-2014-0160), der 2014 veröffentlicht und behoben wurde. Mit diesem Fehler können entfernte AngreiferInnen sensible Daten aus dem Hauptspeicher des Servers (z.B. Passwörter oder Session-Cookies) extrahieren. Leider sind bis heute nicht auf allen Systemen die notwendigen Updates eingespielt worden, es gibt also immer noch verwundbare Server.

CVE-2021-41773 ist eine schwere Sicherheitslücke im Apache Webserver, welche ausschließlich Version 2.4.49 betrifft. Dabei handelt es sich grundsätzlich um eine Path-Traversal

[4] Im Falle von Infektionen ist das oft nicht relevant, da allein die Tatsache, dass der betroffene Port offen ist, Hinweis genug ist.

Schwachstelle, d.h. Angreifer:innen können dadurch auf Dateien außerhalb des Web-Root Verzeichnisses des Webservers zugreifen. Allerdings wurden innerhalb kurzer Zeit Exploits veröffentlicht, mit deren Hilfe die Lücke zu einer Remote Code Execution (RCE) ausgebaut werden kann, d.h. bei Angriffen können beliebige Befehle mit den Rechten des Dienstes ausgeführt werden.

CVE-2021-34473 besser bekannt als "ProxyShell", ist eine Sicherheitslücke, die es Angreifer:innen ermöglich, ohne jegliche Authentifizierung beliebige Befehle als 'NT Authority\-System' über das Netzwerk auszuführen. Innerhalb weniger Tage wurde über Internet-weite Scans nach verwundbaren Servern berichtet. CERT.at sucht via Shodan nach potentiell verwundbaren Installationen in Österreich und verifiziert die Ergebnisse mit Hilfe der Logik eines nmap NSE-Scripts eines Researchers. Zusätzlich haben wir alle Geräte, die uns im Zuge der Scans zu CVE-2021-26855 als Exchange Server gemeldet wurden, miteinbezogen.

CVE-2021-26855 wurde Anfang März von Microsoft außerhalb des üblichen Updatezyklus mittels eines Patches behoben. Diese, zu dem Zeitpunkt der Veröffentlichung der Aktualisierung bereits aktiv ausgenutzte, Schwachstelle in Microsoft Exchange Server 2013, 2016 und 2019 ist besser bekannt als "ProxyLogon", ermöglicht die Kompromittierung aus dem Internet erreichbarer Systeme.

QNAP NAS Geräte mit Photo Station Im November 2019 veröffentlichte die Firma QNAP Patches für mehrere kritische Schwachstellen in ihren NAS-Geräten. Im Mai 2020 wurde Exploit-Code dazu veröffentlicht. CERT.at hat daher mithilfe der Suchmaschine shodan.io nach potentiell verwundbaren Geräten in Österreich gesucht und die Betroffenen informiert. Selbstverständlich wurde die Lücke dabei nicht ausgenutzt.

CVE-2020-0688 ist eine Schwachstelle in einigen Versionen des Exchange E-Mail-Servers, die es Angreifer:innen ermöglicht, beliebige Befehle mit Administrationsrechten über das Netzwerk auszuführen. Sie benötigen dafür nur Zugangsdaten mit beschränkten Rechten, da es bei der Schwachstelle auch zu einer Privilege-Escalation kommt.

TLS < 1.2 Im März 2020 werden die führenden Browser (Chrome, Firefox, Safari, Microsoft Edge) die Untersützung für TLS-Versionen niedriger als 1.2 standardmäßig deaktivieren, d.h. ab diesem Zeitpunkt werden NutzerInnen Webseiten, die nicht mindestens TLSv1.2 unterstützen nicht mehr besuchen können. CERT.at testet daher alle öffentlich per HTTPS erreichbaren .at Domänen und in Österreich geolokalisierten IPv4-Adressen und infomiert deren BetreiberInnen, falls ihre Server ab März 2020 über gängige Browser nicht mehr erreichbar sein werden.

Dazu kamen einige einmalige bzw. unregelmäßige Scans. Diese sind auf der oben verlinkten Webseite genauer beschrieben.

2.5.2 Externe Quellen

Neben diesen eigenen Scans, erhalten CERT.at und GovCERT Austria Informationen aus einer Vielzahl externer Quellen.

Researcher:innen und NPOs

Es gibt einige Non-Profit Organisationen, die Daten für die IT-Security-Community erheben und dieser gratis zur Verfügung stellen.

Die für CERT.at und GovCERT Austria wichtigste davon ist die Shadowserver Foundation, die überwiegend im Bereich der Analyse von Botnetzen und Malware arbeitet. Dazu wurde ein riesiges Netzwerk aus Honeypots[5] aufgebaut. Die Erkenntnisse daraus liefern wertvolle Analysedaten, um beispielsweise Botnetzen auf die Spur zu kommen und sie auszuschalten. Weiters scannt Shadowserver täglich das Internet nach diversen Kriterien ab: daraus ergeben sich viele der Informationen, die zur unseren Warnungen über verwundbare bzw. missbrauchbare Systeme (siehe Kapitel 2.4.1) führen.

Zusätzlich arbeiten CERT.at und GovCERT Austria immer wieder mit unabhängigen Forscher:innen zusammen. Diese informieren uns beispielsweise vorab, wenn sie eine neue Lücke entdeckt haben, lassen uns Listen von verwundbaren Geräten zukommen, oder wickeln Responsible Disclosures[6] über uns ab.

Andere CERTs/CSIRTs

Die IT-Sicherheitscommunity tauscht sich in unterschiedlichen Netzwerken und Plattformen aus, siehe dazu Kapitel 3: Kooperationen und Networking. Wir bekommen von Partnern aus diesen Netzwerken sowohl laufenden Feeds, die wir automatisch verarbeiten, als auch immer wieder Datensätze, die wir dann als “one-shot” (Siehe Kapitel 2.6.1: Einmalige Aussendungen a.k.a. “One-Shots”) verarbeiten.

Kommerzielle IT-Firmen

Machne Firmen wie Microsoft, die kommerzielle Sicherheitslösungen anbieten, arbeiten mit CERT.at und GovCERT Austria und anderen CERTs/CSIRTs zusammen, indem sie Daten kostenlos zur Verfügung stellen.

Suchmaschinen und Archive

Suchmaschinen wie Google oder Shodan inkludieren Hinweise über möglicherweise gehackte Websites oder Netzwerksicherheit in ihre Suchergebnisse. Webseiten, die Opfer von Defacements geworden sind, werden auf Zone-H archiviert. CERT.at und GovCERT Austria erhalten von Zone-H Informationen über dort auftauchende .at bzw. .gv.at Domänen.

[5] Das sind Systeme, die mit dem einzigen Zweck eingerichtet werden, dass sie von Malware angegriffen und ausgebeutet werden können. Beobachtete Aktivitäten werden für die BetreiberInnen aufgezeichnet und anschließend analysiert.

[6] Zum Begriffe siehe den Eintrag in der englischen Wikipedia.

Ermittlungsbehörden

Wenn Ermittlungsbehörden ein Schlag gegen die Internetkriminalität gelingt, sammeln sie oft Daten aus der Beschlagnahmung von Domains oder Servern von Botnetzen.

Dabei werden die ursprünglich von den Angreifern eingesetzten Steuerserver der Botnetze (sog. “Command and Control Server”) durch Sensoren (diese werden “Sinkholes” genannt) ersetzt, die für die Strafverfolgungsbehörden mitprotokollieren, von welchen IP-Adressen infizierte Geräte neue Befehle abholen wollen. Diese ”Botnet drones” befinden sich meistens verteilt über mehrere Länder und daher werden die so erfassten Daten – sofern es der rechtliche Rahmen erlaubt – an die zuständigen nationale CERTs/CSIRTs weitergeleitet, die diese dann wiederum im eigenen Land an die Betroffenen weitergeben können.

In vielen Fällen wird der “Command and Control Server” nicht über eine konstante Domain angesprochen, sondern über nur kurzfristig gültige Domains, die aus dem aktuellen Datum abgeleitet werden. Wenn eine Analyse der Malware diesen Algorithmus extrahiert, so besteht die Möglichkeit, die künftig verwendeten Domains im Voraus zu berechnen und sie rechtzeitig zu registrieren. Dort lassen sich dann Sinkholes betreiben.

Verwendet Malware einen Peer-to-Peer (P2P) Mechanismus für die Kommunikation, so können die Mitglieder des P2P-Netzes manchmal durch eine Teilnahme am P2P Protokoll bestimmt werden.

Hin und wieder gelingt es der Polizei, Sicherheitsforscher:innen oder CERTs/CSIRTs sogar, Zugang zu Servern der AngreiferInnen zu erlangen. Die dort vorgefundenen Daten geben oft Aufschluss über die Vorgehensweisen, eingesetzten Tools und Ziele der Kriminellen.

2.6 Tooling

CERT.at und GovCERT Austria setzen eine Vielzahl von Tools ein, die zum Teil selbst entwicklelt, zum Teil als Open Source Software verfügbar, und zum Teil zugekauft sind.

Zwei der wichtigsten Tools sind IntelMQ und MISP, die hier etwas näher vorgestellt werden sollen.

2.6.1 IntelMQ

Das Projekt

Gestartet wurde der Entwicklungsprozess von IntelMQ[7] bei einem Treffen mehrerer CERTs im Jahr 2014. Die damals verfügbaren Softwarelösungen zur Automatisierung und Verarbeitung von Daten im IT-Securitybereich waren zumeist teuer und/oder schwer zu bedienen. Einige Entwickler des portugiesischen CERT und von CERT.at beschlossen daher, selbst ein Tool zu entwi-

[7] Zusammengesetzt aus “Threat INTELligence” und “Message Queueing”.

ckeln, das diese Probleme adressiert, da eine manuelle Bearbeitung aufgrund der (stetig wachsenden) Datenmenge nicht machbar war.

Dementsprechend sollte IntelMQ möglichst einfach zu nutzen und zu administrieren sein sowie problemlos weiterentwickelt und angepasst werden können. Um das zu erreichen, waren und sind Kompatibilität mit und Schnittstellen zu anderen Tools sowie eine Veröffentlichung als Open Source Software unerlässlich. Der Quellcode von IntelMQ findet sich auf GitHub.

Diese Designprinzipien – Ease-of-Use und Kompatibilität – sind bis heute unverändert und maßgeblich für den Erfolg des Programms verantwortlich. Auch die Umsetzung des Ziels, große Datenmengen automatisiert zu verabeiten, erleichtert die Arbeit von CERTs/CSIRTs enorm. Bei CERT.at werden Dank IntelMQ täglich hunderte E-Mails verschickt, die BetreiberInnen von Internet-Diensten in Österreich auf Probleme in ihren Netzen hinweisen.

Viele CERTs/CSIRTs, die Alternativen genutzt hatten, sind im Laufe der Zeit auf IntelMQ umgestiegen. Mittlerweile verwenden auch viele SOCs (Security Operations Center) und andere Organisationen IntelMQ. Ausgegangen wird von einer weltweit zumindest dreistelligen Anzahl von Instanzen, genaue Daten gibt es dazu aber nicht.

IntelMQ 2023

Die im Vorjahr begonnenen Entwicklungsarbeiten nach der Veröffentlichung der Version 3.0.0 wurden fortgesetzt, und kulminierten in drei neuen Releases. Neben einer Vielzahl von Fehlerbehebungen beinhalteten diese auch lang erwartete Funktionserweiterungen. Beispielsweise ist es nun möglich, einzelne ”Bots” direkt in separaten Python-Scripts zu benutzen. Eine Übersicht zu den Releases findet sich auf GitHub.

Neben diesen Aktivitäten wurde erheblicher Aufwand in operative Verbesserungen gesteckt, und auch die technische Dokumentation wurde grunderneuert.

Einmalige Aussendungen a.k.a. “One-Shots”

IntelMQ ermöglicht es, über ein Web-Interface sog. “One-Shots” abzuwickeln. Dabei handelt es sich um Aussendungen, die anlassbezogen bei akuten Bedrohungen möglichst schnell alle Betroffenen erreichen müssen.

Ein Beispiel wäre die Veröffentlichung eines Exploit zu einer bekannten Sicherheitslücke, zu der es bereits einen Patch gibt: Sind Daten über dafür noch anfällige Geräte in Österreich, z.B. über die Suchmaschine shodan.io verfügbar, können diese in ein CSV-File umgewandelt werden, das dann bequem über das Web-Interface hochgeladen werden kann.

Anschließend muss noch ein Erklärungstext zum vorliegenden Problem inklusive Links zu Workarounds/Updates verfasst werden, um durch IntelMQ automatisch Mails an alle Betroffenen zu verschicken.

Dies ermöglicht CERT.at nicht nur, schnell auf aktuelle, aber einmalige Umstände zu reagieren, sondern eignet sich auch, um neue Feeds zu testen.

2023 wurde diese Funktion 31 Mal genutzt. Ausgesandt wurden unter anderem Informationen zu kompromittierten SSH-Servern in Österreich, verwundbaren und bereits kompromittierten Instanzen von Ivanti Connect Secure und zu veralteten Jenkins-Installationen.

2.6.2 MISP

MISP[8] ist eine Open Source Plattform, auf der Indicators of Compromise (IoCs), Threat Intelligence und andere für die IT-Sicherheit relevante Informationen geteilt, gespeichert und analysiert werden können.

CERT.at und GovCERT Austria betreiben gemeinsam eine MISP-Instanz zu der Teilnehmer:innen aus der Forschung, staatlichen Institutionen und der Wirtschaft Zugriff haben.[9]

Mit wem die Inhalte geteilt werden, wird beim Upload festgelegt – MISP bietet hier eine Vielzahl an Optionen, die von eigens angelegten Gruppen, zur eigenen Organisation oder sogar anderen MISP-Instanzen alles abdecken.

Das soeben erwähnte Teilen über Instanzen hinweg, ist eines *der* Features von MISP. Es bietet der CERT/CSIRT Community eine einfache Möglichkeit, Inhalte zu Vorfällen länderübergreifend verfügbar zu machen und je nach Bedarf auf sehr kleine Gruppen zu beschränken, oder anderen Beteiligten (Forschung, Behörden, Wirtschaft, etc.) zugänglich zu machen.

Das MISP-Projekt hat eine eigene Webseite, der Code wird in einem GitHub Repository zur Verfügung gestellt.

2.7 Bedrohungen 2023

Das Gros der Probleme der IT-Sicherheit sind gut bekannt, nur in seltenen Fällen werden von Grund auf neue Angriffsmethoden entwickelt. Dennoch bringen die meisten Jahre einzelne Weiterentwicklungen oder neue Verhaltensweise von Bedrohungsakteuren mit sich, die aus der breiten Masse hervorstechen.

Wie bereits in den vergangenen Jahren nahmen Angreifer:innen auch 2023 wieder vermehrt Systeme und Software in's Visier, welche aufgrund ihrer Aufgabe direkt aus dem Internet erreichbar sein müssen. Dabei nutzten Bedrohungsakteure Schwachstellen in verbreiteten Softwarelösungen von Unternehmen wie beispielsweise Atlassian, Ivanti, Cisco, MOVEit, Citrix, Fortinet, Aruba, Nextcloud oder Microsoft.

Auch geopolitische Ereignisse hatten abseits ihrer geografischen Lage weitreichende Auswirkungen, von denen auch Österreich nicht verschont geblieben ist. Sowohl der anhaltende Angriffskrieg Russlands gegen die Ukraine als auch der Überfall der Hamas auf Israel sorgten dafür, dass österreichische Unternehmen und Institutionen Opfer politisch motivierter Angriffe wurden.

[8] Das Kürzel stand ursprünglich für "Malware Information Sharing Platform". Da die Software aber heute wesentlich mehr kann als nur Informationen über Schadsoftware zu teilen, gibt es keine offizielle Langform mehr.

[9] Anfragen für einen Zugang bitte an team@cert.at.

2.7.1 Angriffe gegen Lieferketten

Im vergangenen Jahr konnten vermehrt Angriffe auf Anbieter:innen und Lieferant:innen von Software beobachtet werden, sogenannte Supply-Chain-Angriffe. Diese Form von Angriffen ist für finanziell motivierte Kriminelle, insbesondere aber auch für staatlich kontrollierte Bedrohungsakteure besonders attraktiv, da eine erfolgreiche Kompromittierung von Hersteller:innen oder Lieferant:innen bedeutet, dass sich der mögliche Schaden nicht nur auf das Unternehmen selbst bezieht, sondern auch dessen Kund:innen gefährdet sind.

Einer der bekanntesten Fälle im Jahr 2023 war die Kompromittierung der Systeme des Unternehmens 3CX, welches auf Voice-over-IP basierende Kommunikationslösungen für Firmen und Organisationen anbietet - der laut forensischen Untersuchungen selbst Opfer einer Supply-Chain-Angriffs gegen den Hersteller einer Finanzsoftware wurde.

Nach dem erfolgreichen Angriff gegen 3CX manipulierten die Angreifer:innen mehrere Installationspakete der von dem Unternehmen angebotenen Software und erweiterten sie um Schadcode, mit der weitere Daten von durch den Bedrohungsakteur kontrollierter Infrastruktur heruntergeladen werden konnte. Da die manipulierte Software mit der legitimen Signatur des Herstellers versehen war, erschwerte dies eine Erkennung der Manipulation.

Die tatsächliche Motivation der Angreifer:innen ist in diesem konkreten Fall nicht bekannt, die Möglichkeiten für die Kriminellen sind jedoch vielschichtig. Neben dem Ausspionieren verschiedenster Unternehmen wären auch grossflächige Ransomware-Angriffe im Bereich des Möglichen.

In der Vergangenheit wirksame Sicherheitsmechanismen, wie beispielsweise das Signieren von ausführbaren Dateien, werden durch diese Art von Angriffen ausgehebelt, da die Täter:innen Zugriff auf das für den Signaturvorgang notwendige Schlüsselmaterial haben.

Es ist davon auszugehen, dass die Anzahl an Angriffen auf Lieferketten in den nächsten Jahren weiter zunehmen wird. Daher ist und bleibt es wichtig, sich auf mögliche Angriffe vorzubereiten und entsprechende Schutzmassnahmen zu implementieren.

Durch eine proaktive Herangehensweise, regelmäßige Sicherheitsaudits entlang der Lieferkette und enge Zusammenarbeit mit Lieferanten können Organisationen Unternehmen ihre Resilienz gegenüber Supply-Chain-Angriffen stärken und potenzielle Risiken minimieren.

2.7.2 Relevante Schwachstellen

Wie in den vorangegangenen Jahren wurden auch 2023 eine Vielzahl von Sicherheitslücken in Software, Systemen und Produkten aller Art gefunden. Im Vergleich zu den Vorjahren war im diesjährigen Beobachtungszeitraum ein deutlicher Anstieg an gefundenen - und in weiterer Folge oftmals ausgenutzten - Schwachstellen in Edge-Geräten zu beobachten. Insbesondere Firewalls und Lösungen für sichere Fernzugriffe waren häufig betroffen. Zu folgenden Schwachstellen haben wir 2023 Warnungen und Blogposts veröffentlicht.

Webapplikationen

Produkte von Atlassian hatten mehrfach mit Schwachstellen zu kämpfen, deren Ausnutzung eine vollständige Übernahme betroffener Softwareversionen ermöglichte (CVE-2023-22522, CVE-2022-1471, CVE-2023-22518)

In der Software zur Übertragung von Dateien MOVEit Transfer wurden im Frühsommer 2023 im Abstand von wenigen Wochen unabhängig voneinander mehrere kritische Sicherheitslücken entdeckt (CVE-2023-35708, CVE-2023-35036, CVE-2023-34362, CVE-2023-34362). Diese wurden bereits kurz nach der ersten Veröffentlichung der Schwachstellen breitflächig und intensiv von verschiedensten Bedrohungsakteuren genutzt. Die Auswirkungen dieser Angriffe, darunter viele Vorfälle die Ransomware beinhalteten, plagten manche Unternehmen monatelang.

Auch Microsoft blieb nicht verschont, besonders hevorzuheben ist CVE-2023-23397. Diese schwerwiegende Sicherheitslücke betraf Microsoft Outlook. Durch speziell manipulierte E-Mails können Angreifer:innen Net-NTLMv2-Hashes von verwundbaren Systemen stehlen. Da die Ausnutzung der Schwachstelle bereits während der Verarbeitung der Nachricht auf dem Mailserver erfolgt war für den Missbrauch keine benutzerseitige Interaktion notwendig.

Durch den Schweregrad dieser Lücken, sowie entsprechend hohe Marktanteile innerhalb Österreichs, entstand für uns in diesen Fällen jeweils Handlungsbedarf. Die proaktive und zeitnahe Informationsverteilung von Bedrohnungsinformationen durch CERT.at gilt dabei als essenzieller Bestandteil öffentlich verfügbarer Warn-Systeme bezüglich IT-Security Themen innerhalb Österreichs.

Der Perimeter und die Infrastruktur

In dieser Kategorie erwähnen wir Probleme in Routern, Firewalls und Virtualisierungsplatformen. Anders als bei klassischen Applikationen und Services ist es oft schwierig, betroffene Geräte dieser Kategorie ”einfach abzudrehen” – das rasche Einspielen verfügbarer Patches ist oft der einzige gangbare Weg.

Cisco (unter anderem CVE-2023-20198, CVE-2023-20273, CVE-2023-20024, CVE-2023-20156, CVE-2023-20157, ..), Fortinet (CVE-CVE-2023-25610, CVE-2023-27997), Aruba (unter anderem CVE-2023-22779, CVE-2023-22780, CVE-2021-3712, CVE-2023-22747, ..) dienen hier als Beispiel: In den allermeisten Fällen wurde durch den Hersteller zum Zeitpunkt der Veröffentlichung der Schwachstellen bereits ein entsprechendes Update bereitgestellt.

In solchen Fällen ist unser primäres Ziel, schnell die relevanten Informationen an betroffene Unternehmen zu verteilen.

Die Kritikalität lässt sich nicht nur am Perimeter feststellen, sondern zeigt sich auch bei ”Basis-Services”, welche oft die Grundlage für den Betrieb einer Vielzahl weiterer Services darstellen. Auch hier hatten namhafte Hersteller mit kritischen Lücken zu kämpfen. Allen voran Citrix (CVE-2023-4966, CVE-2023-3466, CVE-2023-3467, 2023-3519) musste sich mit Remote Code Execution (RCE) und Authentication-ByPasses auseinandersetzen.

Management-Interfaces

Interfaces zur Administration von Services haben nichts im Internet verloren. Einfache Einschränkungen wie IP-Filter-Listen, oder besser eingeschränkter Zugriff nur via VPN, sind notwendig, um eine Kompromittierung zu verhindern. Beobachtungen verschiedener Sicherheitsforscher zeigen, dass zwischen Veröffentlichung eines Exploits, und der ersten Kompromittierungswelle häufig nur wenige Stunden liegen.

An dieser Stelle verweisen wir auf unseren Blog-Post "Sicherheitslücken in Management-Interfaces" .

2.7.3 Künstliche Intelligenz

Das US-amerikanische Unternehmen OpenAI hat im November 2022 erstmals ein auf einem Large Language Model (LLM) basierendes Service einer breiten Öffentlichkeit zugänglich gemacht. Dieser Schritt hat in weiterer Folge zu einer Vielzahl von Entwicklungen geführt, sowohl was technische Neuerungen als auch die Erschliessung neuer Anwendungsfelder betrifft.

Diese neue Technologie bringt, wie so oft, jedoch nicht nur Nutzen, sondern auch Risiken mit sich. Hauptsächlich machte sich dies im Jahr 2023 durch Skalierungseffekte bereits bekannter Bedrohungen bemerkbar, aber auch durch Angriffe auf LLMs die zum Ziel hatten, Daten zu stehlen oder zu manipulieren.

Skalierungseffekte

Durch den Einsatz von Sprachmodellen ist es Angreifer:innen möglich, Phishing-Mails zu generieren, die nicht nur weniger Grammatik- und Rechtschreibfehler enthalten, sondern auch Texte zu verfassen, die in Sprachstil und Wortwahl an ihre Ziele angepasst sind.

Die so ermöglichte Personalisierung der Nachrichten ist insbesondere für gezielte Angriffe, wie beispielsweise Spear-Phishing oder CEO-Fraud, hilfreich. Zukünftig ist damit zu rechnen, dass Angriffe durch generierte Bilder und Videos ebenfalls zunehmen, da sich die Technik auch in diesem Bereich rasant weiterentwickelt und so Angriffe ermöglicht, die noch vor kurzer Zeit aufgrund der leichten Erkennbarkeit der Fälschungen kaum denkbar gewesen wären.

Diese sogenannten "Deepfakes" sind nicht nur finanziell motivierte Bedrohungsakteure interessant, sondern möglicherweise auch für staatlich kontrollierte Angreifer:innen ein probates Mittel, um die eigenen Ziele zu erreichen.

Angriffe gegen KI-Systeme

Da immer mehr Organisationen auf Sprachmodelle setzen und diese auf die eine oder andere Art in verschiedensten Bereichen zum Einsatz kommen steigt nicht nur deren Bedeutung für den operativen Betrieb, sondern auch die Attraktivität als Angriffsziel für Kriminelle.

Je mehr Informationen ein Sprachmodell über ein Unternehmen hat, beziehungsweise je grösser der Zugriff, den es auf Systeme eines Netzwerkes hat, desto hilfreicher kann es für Mitarbeiter:innen bei der Erfüllung ihrer Aufgaben sein.

Gleichzeitig bedeutet dies aber auch, dass eine Vielzahl von unter Umständen sensiblen Unternehmensinformationen an einem Ort beziehungsweise in einem System gesammelt sind, welches aufgrund der technischen Gegebenheiten möglicherweise schwer abzusichern ist.

Diese Tatsache macht es notwendig, dass KI-Systeme jeder Art nicht nur in Bezug auf die darunterliegende Hard- und Software in das reguläre Risikomanagement mit einbezogen werden müssen. Auch die Menge an Informationen und Daten, auf die ein Sprachmodell zugreifen kann, sollte einer regelmässigen Risikoabwägung unterzogen werden.

2.8 Hilfe bei Vorfällen

Auch wenn die Hauptaufgabe von CERT.at und GovCERT Austria darin besteht, koordinierend zu unterstützen, gibt es Fälle, die dabei herausstechen und wesentlich mehr Zeit erfordern, als das normale Tagesgeschäft. In solchen Fällen unterstützen wir Betroffene sowohl mit unserem Fachwissen und unserer Erfahrung, als auch bei der Koordination mit den relevanten staatlichen Stellen.

2.8.1 DDoS gegen kritische Infrastruktur

Wie bereits im Vorjahr wurden staatliche und staatsnahe Organisationen sowie Unternehmen der kritischen Infrastruktur in Österreich im Dezember 2023 erneut Opfer von DDoS-Angriffen. Im Gegensatz zu den Angriffen Ende 2022 gab es diesmal keine Hinweise auf eine politische Motivation der Angreifer:innen, kein bekannter Bedrohungsakteur hat sich zu den Angriffen bekannt. Auch wurden die Angriffe nicht im Vorhinein angekündigt, was zur Folge hatte, dass die Ziele unerwartet getroffen wurden.

Glücklicherweise waren die betroffenen Organisationen gut vorbereitet, und hatten in vielen Fällen im letzten Jahr gesammelte Erfahrungen in die eigenen Prozesse und Verbesserungen der Sicherheitsmaßnahmen einfließen lassen. Wir wurden kurz nach Beginn der ersten Welle an Angriffen bereits informiert, und waren dadurch in der Lage, technische Informationen über die Art der Angriffe sowie Indikatoren zu den von den Angreifer:innen verwendeten Systemen rasch zu verteilen.

Die Kombination dieser Faktoren sorgte dafür, dass es den Kriminellen nicht gelang, ernsthaften Schaden anzurichten. Dies war vermutlich ein entscheidender Faktor dafür, dass die Angriffe bereits nach kurzer Zeit wieder eingestellt wurden.

2.8.2 Unterstützung bei Ransomware-Vorfällen

Zu Beginn des Jahres 2023 kam es weltweit zu massiven Angriffen gegen aus dem Internet erreichbare ESXi-Systeme. Dabei machten sich die Angreifer:innen neben verschiedenen kritischen Sicherheitslücken teilweise auch Backdoors zu Nutze, die bereits Monate zuvor in verwundbaren Systemen platziert wurden. Das ultimative Ziel der Kriminellen war es, durch Verschlüsselung von Daten Systemausfälle zu provozieren, um so Lösegeld von den Opfern erpressen zu können.

Glücklicherweise hatte CERT.at in der Vergangenheit bereits verschiedenste Warnungen und Informationen zu aus dem Internet erreichbaren ESXi-Systemen an österreichische Netzbetreiber:innen versandt, was den Verantwortlichten ermöglicht hatte, einen Grossteil der Lücken zu schliessen, bevor diese missbraucht werden konnten.

Dies hatte zur Folge, dass in Österreich nur eine Handvoll an Systemen der Verschlüsselung zum Opfer fiel, im Gegensatz zu teilweise hunderten Systemen in anderen Ländern.

Auch in anderen Fällen, beispielsweise bei einer Welle von Lockbit-Angriffen, gelang es CERT.at, von den Kriminellen in's Visier genommene Organisationen rechtzeitig zu warnen, wodurch kompromittierte Systeme oftmals entdeckt werden konnten, bevor die Angreifer:innen in der Lage waren, den Verschlüsselungsprozess zu starten.

Kapitel 3

Kooperationen und Networking

Ohne Zusammenarbeit ist die Arbeit eines CERTs/CSIRTs nicht möglich; keine Institution kann alle Bereiche der IT-Sicherheit im Alleingang abdecken. Dementsprechend haben CERT.at und GovCERT Austria über die Jahre viel Zeit in den Vertrauensaufbau und Vernetzung gesteckt.

3.1 Vernetzung als Grundvoraussetzung für Vertrauensbildung

CERT.at arbeitet nicht im Verborgenen an der Sicherheit des österreichischen Internets. Nur durch intensive Vernetzung mit anderen in der IT-Security Branche kann sichergestellt werden, dass Gefahren erkannt und neue Lösungen und Erfahrungen geteilt werden. Ein gutes Netzwerk, nationale, europäische und internationale Sichtbarkeit und gegenseitiges Vertrauen, sind die Basis der Arbeit von CERT.at.

CERT.at und GovCERT Austria richten sich gemeinsam in ihrer Arbeit an jede Österreicherin und jeden Österreicher. Diese sind Kund:innen – das Produkt, das sie konsumieren, ist die Sicherheit im Netz. Da es aber nicht möglich ist, jede und jeden direkt anzusprechen, interagieren CERT.at und GovCERT Austria stellvertretend mit den wichtigsten Communities im Bereich IT-Sicherheit. Das sind jene österreichischen Unternehmen und Institutionen im Sicherheitsbereich, die sich mit diesem Thema auseinandersetzen oder davon betroffen sind.

CERT.at und GovCERT Austria betreiben ein aktives Community Management, sowohl offline durch Organisation und Teilnahmen an Konferenzen / Besuchen / Treffen als auch online durch Mailinglisten, soziale Medien und Instant Messaging. Während und wegen der Pandemie haben sich einige Aktivitäten auch zu hybriden Formaten entwickelt, 2023 hat in machen Bereichen zur Wiederaufnahme der physischen Treffen geführt.

Dadurch unterstützen sie die Vernetzung aller relevanten Personen, Firmen und Behörden in Österreich. Sie sind aber auch international sichtbare Partner für ausländische CERTs/CSIRTs. So besteht eine intensive Zusammenarbeit und reger Informations- und Erfahrungsaustausch mit ExpertInnen aus aller Welt. GovCERT Austria ist dabei der staatliche österreichische Ansprechpartner für vergleichbare Stellen im Ausland sowie für internationale Organisationen zu Fragen der IKT-Sicherheit.

3.2 Vernetzung auf nationaler Ebene

3.2.1 Austrian Trust Circle (ATC)

Der Austrian Trust Circle ist eine Initiative von CERT.at und dem österreichischen Bundeskanzleramt und besteht aus Security Information Exchanges in den einzelnen Bereichen der strategischen Informationsinfrastruktur (CIIP).

Im Rahmen des Austrian Trust Circles wird ein formeller Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich geboten. Wichtige österreichische Unternehmen finden hier Hilfe zur Selbsthilfe im Bereich IKT-Sicherheit. Im Rahmen des ATC bekommt CERT.at Zugang zu operativen Kontakten und Information über die Behandlung von Sicherheitsvorfällen in den jeweiligen Organisationen.

Der Austrian Trust Circle ist ein wichtiges Netzwerk der österreichischen IKT-Sicherheit. Er schafft eine Vertrauensbasis, um im Ernstfall gemeinsam agieren zu können und sorgt für Vernetzung und Informationsaustausch in und zwischen den Sektoren der strategischen IKT-Infrastruktur.

Der ATC wurde im Jahr 2011 gegründet. Als dann 7 Jahre später das NISG in Kraft trat, war es dadurch für viele Unternehmen, die nun Betreiber wesentlicher Dienste nach diesem Gesetz wurden, bereits gang und gäbe, sich mit anderen über Probleme im IT-Sicherheitsbereich auszutauschen, weshalb das Gefühl, sich für einen Vorfall ”schämen” zu müssen und ihn darum lieber nicht zu melden, gar nicht erst aufkommen konnte.

Nachdem letztes Jahr nach den vorangegangenen Einschränkungen durch die Pandemie bereits erste Schritte in die Richtung gesetzt worden konnten war es 2023 möglich, den ATC endgültig in den Regelbetrieb zurückzuführen.

3.2.2 CERT-Verbund

Im Mittelpunkt des Aufgabenbereichs des nationalen österreichischen CERT-Verbunds stehen die Verbesserung der Zusammenarbeit zwischen den österreichischen CERTs sowie die Förderung der CERT-Aktivitäten in Österreich. Ein flächendeckendes Netz an kooperierenden CERTs ist das wirksamste Mittel zur Absicherung der vernetzten Informations- und Kommunikationssysteme. Diese Sichtweise wird durch die in Österreich stetig wachsende Anzahl an CERTs beziehungsweise CSIRTs bestätigt.

Der CERT-Verbund wurde 2011 als Kooperation der damals existierenden österreichischen CERTs aus öffentlichem wie auch privatem Sektor gegründet. Die Intention dahinter war die Bündelung der verfügbaren Kräfte zur optimalen Nutzung des gemeinsamen Know-hows zur Gewährleistung bestmöglicher IKT-Sicherheit.

Die Teilnahme am CERT-Verbund ist freiwillig und kann jederzeit beendet werden. Alle Mitglieder verpflichten sich, folgende Ziele im Sinne eines gemeinschaftlich geführten und auf Kooperation basierenden CERT-Verbundes zu verfolgen:

1. Regelmäßiger Informations- und Erfahrungsaustausch

2. Identifikation und Bekanntmachung von Kernkompetenzen

3. Förderung nationaler CERTs in allen Sektoren

Im Lauf des Jahres 2023 fanden 6 Treffen physisch statt. Mit Stand Ende 2023 nehmen 17 Teams am österreichischen CERT-Verbund teil. Genauere Informationen finden Sie online.

3.2.3 IKDOK/OpKoord

Die "Struktur zur Koordination auf der operativen Ebene" (auch "Operative Koordinierungsstruktur" oder kurz "OpKoord" genannt) und der "Innere Kreis der operativen Koordinationsstruktur" (IKDOK) wurde erstmals in der im März 2013 herausgegebenen "Österreichische Strategie für Cyber Sicherheit" (ÖSCS 2013) beschrieben. Im Jahr 2016 nahmen beide Strukturen ihre Arbeit auf. Sowohl der IKDOK als die OpKoord bekamnen mit Inkrafttreten des NIS-Gesetzes Ende 2018 einen klaren rechtlichen Rahmen. Die Ende 2021 erschienene neue Version der "Österreichische Strategie für Cybersicherheit´´ (ÖSCS 2021) hat diese Strukturen nicht verändert.

Der IKDOK erstellt periodische und anlassbezogene operative Lagebilder zur staatlichen Cybersicherheit. Weiters ist er für die Erarbeitung von Maßnahmen im Anlassfall sowie für die Unterstützung und Koordinierung gesamtstaatlicher Notfallmaßnahmen im Rahmen des Cyber Krisenmanagements (CKM) zuständig.

Der IKDOK besteht (Siehe §3(4) NISG) aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres. Bis Dezember 2021 hatte das Cyber Security Center im BVT die Aufgabe, die Koordinationsstrukturen zu leiten. Mit der Etablierung der Direktion für Staatsschutz und Nachrichtendienst (DSN) wanderten diese Agenden gemeinsam mit den anderen der operativen NIS Behörde in die Abteilung IV/10 des Innenministerium. 2023 wurde diese Abteilung in IV/S/2 umbenannt.

Damit sind die folgenden Akteure im IKDOK aktiv: Die operative NIS Behörde im Innenministerium (BMI IV/S/2), die strategische NIS Behörde im Bundeskanzleramt (BKA I/8) plus dem GovCERT, die Direktion für Staatsschutz und Nachrichtendienst (BMI/DSN), das Cybercrime Competence Center (BMI/BK), das das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) sowie das Abwehramt, das Heeres-Nachrichtenamt und das IKT & Cybersicherheitszentrum (alle BMLV).

3.2.4 Austrian Energy CERT – AEC

Nach der NIS-Richtlinie der europäischen Union sind alle Betreiber kritischer Infrastruktur verpflichtet, Hacking-Angriffe oder Softwareprobleme an eine Meldestelle zu berichten. In einem (bisher) einzigartigen Modell hat sich die gesamte Energiewirtschaft Österreichs (Strom, Gas und Vertreter der Ölwirtschaft) in Form der Arbeitsgemeinschaft E-CERT auf ein "Private Public Partnership" verständigt, die das österreichische Austrian Energy Computer Emergency Response Team (AEC) aufgebaut hat.

Mehr Informationen über das AEC finden Sie auf deren Webseite unter https://www.energy-cert.at/.

3.3 Vernetzung auf internationaler Ebene

Neben der Zusammenarbeit innerhalb Österreichs, kooperieren CERT.at und GovCERT Austria auch auf internationaler Ebene mit zahlreichen Organisationen und Gruppen.

3.3.1 Bilaterale Vernetzung

CERT.at arbeitet mit vielen CERTs/CSIRTs aus Nachbar- und Partnerländern zusammen; besonders intensiver Austausch findet u.a. mit dem Deutschen CERT-Verbund statt. CERT.at wird regelmäßig zu Konferenzen des deutschen Verbundes eingeladen. Im Mittelpunkt stehen dabei gegenseitige Updates.

3.3.2 Task Force CSIRT

Die Task Force CSIRT (TF-CSIRT) dient vor allem als laufende, vertrauensbasierte Vernetzungsplattform. Die TF-CSIRT ist eine ursprünglich aus dem europäischen akademischen Netzwerk (GÉANT) entstandene Plattform. Mit der Etablierung des CSIRTs Network (s.u.) ist für uns die Bedeutung der TF-CSIRT gesunken.

Mit Trusted Introducer (TI) entstand aus dem Netzwerk weiters eine wichtige Datenbank, die über die Vertrauenswürdigkeit und Seriosität von Akteur:innen im europäischen IT-Sicherheitsbereich Auskunft gibt.

3.3.3 CSIRTs Network

Im Jahr 2017 wurde auf Initiative der Europäischen Union und auf Basis der NIS-Richtlinie ein neues Netzwerk auf EU-Ebene eingeführt, mit dem ein Zusammenschluss aller europäischer nationalen CERTs und Branchen-CERTs erfolgen soll.

Mitglieder im CSIRTs Network (CNW) sind alle nationalen CERTs (in diesem Kontext: CSIRTs, die laut Artikel 9 der ersten NIS-Direktive, bzw. Artikel 10 der NIS2-Direktive akkreditiert sind) der EU-Mitgliedsländer, wobei es sich größtenteils um staatliche Stellen handelt. Dazu kommt noch CERT-EU, das CERT der EU Organe, Einrichtungen und sonstige Stellen (EUIBAs). Das Netzwerk ist sehr divers, die Teamgröße reicht von klein (etwa die CSIRTs aus Zypern oder Malta) bis zu großen nationalen Cybersicherheitszentren wie NCSC-NL, ANSSI (Frankreich) oder dem CERT-Bund im deutschen BSI. Manche haben eher akademischen Hintergrund (CERT.LV, CERT.PL, CSIRT.CZ), andere hingegen sind sehr eng an den Nachrichtendienst (CFCS DK) angekoppelt. Für Österreich nimmt CERT.at, das GovCERT und das AEC am CSIRTs Network teil.

Das Netzwerk trifft sich meist drei mal im Jahr (2023 war das im März in Lissabon, im Juni in Stockholm und im September in Leon), online wird per Mailinglisten und vor allem über ein Instant Messaging System kooperiert. Letzteres hat sich seit seiner Einführung als wichtigstes Medium herausgestellt, da die niederschwellige Erreichbarkeit quer über die ganze Europäische Union die Zusammenarbeit zwischen Teams aller Mitgliedsstaaten deutlich verstärkt hat.

Die Phase des Vertrauensaufbaus hat das Netzwerk hinter sich gebracht, jetzt geht es um eine vertiefte Zusammenarbeit, sowohl im Tagesgeschäft, als auch während größerer Vorfälle. Letzteres wird im Netzwerk regelmäßig geübt. So wurden im November 2023 mit der CyberSOPEx in einer kompakten Übung die Eskalations- und Kooperationsprozesse im CSIRTs Network geprobt. Dadurch soll gewährleistet werden, dass bei Vorfällen, egal ob grenzübergreifend oder nicht, gegenseitige Unterstützung schnell und effizient erfolgen kann.

Um diese übergeordneten Ziele zu erreichen wird beispielsweise auf gleiche technische Lösungen[1] gesetzt, es gibt auch Versuche, eine gemeinsame Taxonomie (siehe 2.3: Taxonomie) zu etablieren.

3.3.4 European GovCERT Group

Die European GovCERT Group (EGC) ist ein historisch gewachsenes Netzwerk bestehend aus den GovCERTs von 12 europäischen Staaten plus CERT-EU. Letzteres ist für die EU Institutionen zuständig. Die Gruppe bildet eine informelle Vereinigung, deren Mitglieder in Fragen hinsichtlich der Reaktion auf Vorfälle effektiv zusammenarbeiten. Im Gegensatz zum CSIRTs Network ist EGC eine Initiative der CERTs selbst und basiert nicht auf einem gesetzlichen Auftrag.

Die EGC konzentriert sich auf den Austausch zwischen Sicherheitsteams in Bezug auf aktuelle Vorfälle, Gefahrenpotentiale sowie Projekte und Werkzeuge der Teilnehmenden. Neben den regelmäßigen Treffen von VertreterInnen der GovCERTs gibt es auch eine laufende niederschwellige Kommunikation zwischen den Teams. Die Unabhängigkeit von politischen Einflussnahmen und die interne Vertrauensbasis zwischen den Beteiligten garantieren einen effizienten Austausch zu Problemlagen und neuen Entwicklungen.

Mitglieder sind auch CERTs aus Norwegen, der Schweiz und dem Vereinigten Königreich. Dies ermöglicht uns auch eine direkte Zusammenarbeit mit Organisationen die nicht Teil des CSIRTs Network der Europäischen Union sind.

3.3.5 FIRST

FIRST (Forum of Incident Response and Security Teams) ist der anerkannte, globale Verband von CERTs. Die Mitgliedschaft in FIRST gibt Incident Response Teams den Zugriff auf ein globales Kontaktnetzwerk und Wissensbasis, was eine effektivere Reaktion auf Sicherheitsvorfälle ermöglicht.

Auf Grund der Größe (FIRST hat mehr als 700 Mitglieder) stehen nicht mehr einzelne Vorfälle im Fokus von FIRST, sondern vielmehr der Erfahrungsaustausch, Lobbying und das gemeinsame

[1] Konkret unter anderem MISP und IntelMQ.

Entwickeln von Standards. So werden etwa das Traffic Light Protocol (TLP), i.e. das System zur Kennzeichnung, wie Information weitergegeben werden darf und das Common Vulnerability Scoring System (CVSS), also die Metrik zur Bewertung von Schwachstellen von FIRST betreut. Weitere Informationen dazu finden Sie auf der Webseite von FIRST, zu TLP und zu CVSS.

2023 nahm CERT.at am 2023 FIRST Regional Symposium for Europe, das gemeinsam mit einem TF-CSIRT Meeting ausgerichtet wurde, und der Annual FIRST Conference teil.

Kapitel 4

Drittmittelprojekte

Um die Finanzierung des Teams auf eine breitere Basis zu stellen, und um spezielle Projekte umsetzen zu können, nutzt CERT.at die Möglichkeiten, die sich durch EU-Programme und nationalen Förderungen ergeben.

4.1 Connecting Europe Facilities (CEF)

Co-financed by the European Union
Connecting Europe Facility

4.1.1 AWAKE (2020-AT-IA-0254)

Im CEF-kofinanzierten Projekt AWAKE ("Cyber situational awareness for collaborative knowledge and joint preparedness") arbeiten wir seit September 2021 gemeinsam mit dem Austrian Institute of Technology (AIT) als Koordinator, dem Bundesministerium für Inneres (BMI) sowie dem Bundeskanzleramt (BKA) an Werkzeugen für die kooperative Erstellung eines Lagebildes. Primär geht es hier um zwei der drei Ebenen in der Cybersicherheitsstrategie der EU (technisch: CERTs, operativ: CyCLONe; die dritte wäre die strategische), die sich in Österreich gut abbilden lassen.

Bei uns im CERT, auf der technische Ebene, geht es um die Details, was die (technischen) Bedrohungen sind, was aktuell ausgenutzt wird und was wo verwundbar ist. In Österreich ist die operative Ebene die entsprechende NIS Behörde im Innenministerium (das NIS Büro in der Sektion IV), wo es primär um die Auswirkungsdimension geht. Wir tauschen uns fallbezogen und laufend im Rahmen der OpKoord (siehe 5.1 NIS-Gesetz) aus. Das wollen wir mit diesem Projekt verbessern.

Einerseits geht es um eine Verbesserung des OSINT Prozesses: Mitarbeiter von CERT.at beobachten jeden Arbeitstag, was sich in der Welt zum Thema Cybersecurity tut: werden neue Schwachstellen bekannt, was gibt es Neues bei Werkzeugen, Taktiken und Prozeduren; welche

Neuerungen haben sich die Tätergruppen ausgedacht und was haben sich die Verteidiger an Verbesserungen einfallen lassen. Aktuell wird von CERT.at noch Taranis 3 (von GovCERT NL, später NCSC-NL entwickelt) für diesen Workflow benutzt; das Ergebnis kann man am Ende jeden Arbeitstages in der Tageszusammenfassung sehen.

In AWAKE setzen wir auf Taranis NG auf, was eine Neuimplementierung des Taranis Konzeptes mit einem aktuellen Softwarestack ist. Auf dieser Basis implementiert AWAKE neue Features, primär ein Clustering der Nachrichtenartikel in Stories. Wegen einiger grundlegender Umbauten und Verzögerungen bei der Annahme von Pull-Requests durch das Taranis NG Projekt war ein Code-Fork leider unvermeidlich, die AWAKE-Version heißt jetzt Taranis_AI. Einige der initial geplanten Neuerungen werden leider nicht mehr in der Projektlaufzeit umgesetzt; wir hoffen, dass wir das in Nachfolgeprojekte (etwa ENSOC, siehe 4.2.1) unterbringen können.

Andererseits geht es auch um das aktive Einholen von Statusberichten durch Umfragen. Hier können wir stark auf die Vorarbeiten aus dem ACCSA Projekt zurückgreifen. Das dort entwickelte Koord-Tool kann genau das: eine dauerhaft laufende Webumfrage, bei der sich die Fragen und Antworten mit der Zeit ändern dürfen, und wo jeweils eine aktuelle Zusammenfassung der Ergebnisse angezeigt wird. Im Nachhinein kann man sich auch anzeigen lassen, was der Wissensstand zu bestimmten Zeitpunkten war.

Beiden Modi gemeinsam ist die theoretische Möglichkeit, das System nicht nur als Brücke zwischen Layern, sondern auch im gleichen Layer zwischen geografischen Einheiten zu verwenden. Wir denken an, dass damit auch eine Aggregation der Information von EU Mitgliedstaaten auf EU Ebene möglich sein sollte.

Den Projektfortschritt kann man in den Repositories auf Github verfolgen: Taranis_AI und Koord-Tool.

4.1.2 JTAN (2020-EU-IA-0260)

Das Joint Threat Analysis Network (JTAN) Projekt ist eine Kooperation mehrerer CERTs in der EU. Für uns ist primär die R&D Abteilung der nic.at (CERT.at Mutterfirma) eingebunden. Es geht für uns darum, Risikofaktoren für Domains zu finden und diese auf Basis der Daten, die in der Registry vorhanden sind, für konkrete Domains zu ermitteln. Die Vorgabe aus der NIS2 Direktive, dass die Identitäten von Domaininhabern validiert werden müssen, gibt dem Projekt auch auf Seite der nic.at Druck, denn wenn in diesem Vorgang eine Risikoeinschätzung einer Domainregistierung einfließen könnte, sind Prozessoptimierungen möglich.

Da wir im Frühjahr 2023 endlich die Stelle eines ”Research Engineer Internet” besetzen konnten, kam deutlich mehr Schwung in das Projekt. Es wurden viele Rohdaten (aus Cyber Threat Informationen, dem Verhalten von Registranten und Registraren, sowie dem Volumen des DNS-Verkehrs) zu Risikobewertungen von Domains gesammelt, um dann daraus mit Hilfe von Machine Learning (ML) Methoden ein Modell zu entwickeln, damit wir für neue Domains gute Risikoabschätzungen geben können.

Gemeinsam mit den Kollegen von NASK, dem Betreiber von .pl und dem CERT-PL, arbeiten wir noch an einer Berechnung vergleichbarer Risikofaktoren für Domains der TLD .at und .pl sowie an der statistischen Analyse der Ergebnisse.

4.2 Digital Europe Program (DEP)

Bisher war CEF das für CERT.at relevante Förderprogramm der EU, mit 2023 kam es hier zu Änderungen. Mit der Etablierung des ECCC (European Cybersecurity Competence Centre) und des Netzwerkes der nationalen Gegenstücke (bei uns Nationales Koordinierungszentrum Cybersicherheit (NCC-AT)) wurde das Digital Europe Program (DEP) das zentrale Förderinstrument für Cybersicherheit der Europäischen Union.

4.2.1 ENSOC (101127660)

Die EU Kommission fördert im Rahmen des Digital Europe Programms Initiativen in Mitgliedsstaaten, die die Cybersicherheit der EU verbessern. Im Call DIGITAL-ECCC-2022-CYBER-03 werden insbesondere Projekte kofinanziert, die eine grenzüberschreitenden Zusammenarbeit von Security Operations Centres (SOCs) etablieren.

Die so gebildeten Konsortien können einerseits um Grants ansuchen, durch die eigene Kosten (Personal, Reisen, Hardware) zu 50% erstattet werden, andererseits können die Konsortien im Rahmen eines gemeinsamen Einkaufs mit dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung (ECCC) nötige Ausgaben im Bereich Hardware, Informationsquellen (etwa Cyber Threat Intelligence Feeds) oder Software(-Entwicklung) zu 75% ersetzt bekommen.

Wir erwarten für 2024, dass die EU dieses Schema über den Cyber Solidarity Act gesetzlich verankern und die Finanzierung langfristig sichern wird.

ENSOC ist ein Konsortium von Cybersicherheitsagenturen aus mehreren EU Mitgliedstaaten unter der Leitung von CCN-CERT, dem für die öffentliche Verwaltung zuständigem spanischen CERT. Als Mitglieder werden folgende Einrichtungen genannt:

- Directoratul National de Securitate Cibernetica (DNSC, Rumänien)
- Computer Incident Response Center Luxembourg (CIRCL,Luxemburg)
- Agenzia per la Cybersicurezza Nationale (ACN, Italien)
- Centro National de Ciberseguranca (CERT.PT, Portugal)
- Centro Criptológico Nacional (CCN-CERT, Spanien)
- NIS Büro Innenministerium (BMI, Österreich)
- NCSC-NL (Niederlande)

In der Ausschreibung waren die Teilnehmer auf ”public bodies” eingeschränkt, was eine direkte Teilnahme von CERT.at an diesem Projekt verhindert hat. Daher ist das offizielles Mitglied Österreichs das Innenministerium und CERT.at tritt nur als Subcontractor auf.

Das Konsortium definiert seine Ziele so:

Through the ENSOC Crossborder Platform we aim at improving the collective security of EU stakeholders and support CSIRTs and SOCs by overlapping defensive capabilities.

- Cyber Intelligence sharing: for continuous improvement of detection.
- Incident Coordination: to limit the impact and scope of incidents. Necessary for incident visibility.
- Automation: sharing anonymized information of an anomaly from minute 0.
- Situation Awareness: to map the European cybersecurity situation. Based on:
  - Incidents (LUCIA)
  - Alerts (SIEM)
  - Suspicious events (MISP)
  - Vulnerabilities, social tension (PANORAMA)

4.2.2 Mitarbeit an Forschungsprojekten

SHIFT (KIRAS)

Das Austrian Energy CERT (AEC) nimmt am Projekt SHIFT teil. Es geht um sichere Simulationstechnologien für cyber-physische Systeme.

CyberMonoLog (KIRAS)

In CyberMonoLog geht es um Empfehlungen für möglichst sinnvolles Logging aus dem Blickwinkel IT-Sicherheit. Dieses Projekt wurde 2023 abgeschlossen.

Kapitel 5

Rechtsgrundlage

5.1 Netz- und Informationssicherheitsgesetz (NISG)

Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Um dies zu gewährleisten, wurde mit der Richtlinie (EU) 2016/1148 (“NIS-Richtlinie”) der erste EU-weite Rechtsakt über Cybersicherheit verabschiedet. Die NIS-Richtlinie wurde in Österreich mit dem am 29. Dezember 2018 in Kraft getretenen“NIS-Gesetz” umgesetzt.

Während das Bundeskanzleramt nach dem NIS-Gesetz strategische Aufgaben wahrnimmt, nimmt das Bundesministerium für Inneres operative Aufgaben wahr. Im Anwendungsbereich des Gesetzes befinden sich Einrichtungen mit einer hohen Bedeutung für das Funktionieren des Gemeinwesens, weshalb ihre Netz- und Informationssysteme besonders schützenswert sind.

Dies betrifft zum einen Einrichtungen in den sieben Sektoren Energie, Verkehr, Bankwesen, Finanzmarkt, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur (“Betreiber wesentlicher Dienste”), zum anderen Einrichtungen, die bestimmte digitale Dienste zur Verfügung stellen (“Anbieter digitaler Dienste”) sowie “Einrichtungen der öffentlichen Verwaltung”.

Unter nis.gv.at veröffentlichen das BKA und das BMI gemeinsam die relevanten Informationen (Verweis auf den Gesetzestext, Erläuterungen, Verordnungen, Factsheets, Mappingtabelle, FAQs, etc.) zum NIS Gesetz und seiner Umsetzung in Österreich.

5.1.1 Strategisches NIS-Büro

Das im Bundeskanzleramt angesiedelte Büro für strategische Netz- und Informationssystemsicherheit (“strategisches NIS-Büro”) hatte schon 2021 die Ermittlungen der Betreiber wesentlicher Dienste auf Grundlage der NIS-Verordnung abgeschlossen. Der Fokus war 2022 die Vertretung Österreichs in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, insbesondere die Koordinierung und Vertretung der österreichischen Position in den Verhandlungen zur NIS-2-Richtlinie.

Aus den EU-Verhandlungen zu NIS2 wurde dann 2023 die Arbeit an einem Entwurf für ein neues NIS-Gesetz, das die NIS-2 Direktive in österreichisches Recht überführen wird. Bei Redaktionsschluss dieses Jahresberichtes ist der Entwurf noch nicht öffentlich, auf nis.gv.at wurden aber schon erste Informationen dazu publiziert.

5.1.2 Aktivitäten auf EU-Ebene

Nach dem die NIS-2-Richtline noch im November 2022 verabschiedet wurde, arbeitet die EU Kommission selber (es fehlen noch delegierten Rechtsakte) und ihre Mitgliedstaaten an der Umsetzung.

Was das genau für CERT.at und das GovCERT bedeuten wird, ist noch nicht ganz klar, und wird auch von Details der Umsetzung in ein nationales Gesetz abhängen. Eines ist aber klar: weniger Verantwortung und Arbeit werden wir dadurch nicht haben. Laut Zeitplan hat Österreich bis Oktober 2024 Zeit, ein Anpassung des NIS Gesetzes zu verabschieden.

Am 18. April 2023 hat die EU Kommission den Vorschlag für einen "Cyber Solidarity Act" präsentiert. Dieser soll einige Initiativen der Kommission dauerhaft absichern. Dazu gehört die Finanzierung von Plattformen für die Zusammenarbeit von Security Operations Centers (SOCs) und eine "Cyber Reserve", über die Mitgliedstaaten Cyber Security Dienstleistungen abrufen können. Es gibt hier deutliche Überschneidungen zu den Aufgaben eines nationalen CERT, daher hat sich CERT.at mit einem Whitepaper zu Wort gemeldet und auch eine Stellungnahmen innerhalb des CSIRTs Network koordiniert. Es ist zu erwarten, dass der Cyber Solidarity Act noch 2024 in Kraft treten wird.

Auch DORA ("Digitale operationale Resilienz im Finanzsektor") wurde im November 2022 verabschiedet und befindet sich im Stadium der Umsetzung.

Die Critical Entities Resilience (CER) Richtlinie ist mit 16. Jänner 2023 in Kraft getreten, dazu gibt es schon delegierte Rechtsakte.

Zum Cyber Resilience Act (CRA) gab es Ende 2023 eine politische Einigung, die formelle Annahme wird im Laufe von 2024 erwaret. Er soll für Hardware- und Softwareprodukte verbindliche Cybersicherheitsanforderungen einführen und so Verbraucher:innen und Unternehmen vor digitalen Produkten mit unzureichenden Sicherheitsmerkmalen schützen und unionsweit digitale Standards harmonisieren.

Eine umfassende Zusammenfassung der Cybersecurity-Agenda auf EU-Ebene enthält der Bericht Cybersicherheit, der vom Bundeskanzleramt veröffentlicht wird.