

Bericht
Internet-Sicherheit
Österreich 2022

Inhaltsverzeichnis

1	CERT.at und GovCERT Austria	1
1.1	CERT.at – Österreichs nationales CERT	1
1.1.1	CERT-Beirat – Strategische Leitplanken	2
1.1.2	Vernetzung	3
1.1.3	Gesetzlicher Auftrag von CERT.at	3
1.2	GovCERT Austria – Expertise im Behördenbereich	3
1.2.1	Public-Private-Partnership mit vielen Vorteilen	4
1.3	Kernaufgaben von CERT.at und GovCERT Austria	4
1.4	Zertifizierungen 2022	5
1.4.1	ISO 27001 Zertifizierung	5
1.4.2	TI Zertifizierung	6
2	Das IT-Sicherheitsjahr 2022	7
2.1	NIS Meldungen	7
2.2	Incident Reports, Incidents und Investigations	9
2.3	Taxonomie	11
2.3.1	Reference Security Incident Taxonomy – ein kurzer Überblick	12
2.4	2022 im Detail	13
2.4.1	Taxonomie “vulnerable”	14
2.4.2	Probleme im Web	16
2.4.3	Veraltete Kryptographie	18
2.4.4	Malware	19
2.5	Datenbasis	19
2.5.1	Eigene Erhebungen	19
2.5.2	Externe Quellen	21
2.6	Tooling	23
2.6.1	IntelMQ	23
2.6.2	MISP	24
2.7	Bedrohungen 2022	25
2.7.1	Ukrainekrieg	25
2.7.2	Relevante Schwachstellen	26
2.8	Hilfe bei Vorfällen	28
2.8.1	DDoS gegen kritische Infrastruktur	28

2.8.2	Unterstützung bei Ransomware-Incidents	28
3	Kooperationen und Networking	30
3.1	Vernetzung als Grundvoraussetzung für Vertrauensbildung	30
3.2	Vernetzung auf nationaler Ebene	31
3.2.1	Austrian Trust Circle (ATC)	31
3.2.2	CERT-Verbund	31
3.2.3	IKDOK/OpKoord	32
3.2.4	Austrian Energy CERT – AEC	32
3.3	Vernetzung auf internationaler Ebene	33
3.3.1	Bilaterale Vernetzung	33
3.3.2	Task Force CSIRT	33
3.3.3	CSIRTs Network	33
3.3.4	European GovCERT Group	34
3.3.5	FIRST	34
4	Drittmittelprojekte	36
4.1	Connecting Europe Facilities (CEF)	36
4.1.1	AWAKE (2020-AT-IA-0254)	36
4.1.2	JTAN (2020-EU-IA-0260)	37
4.1.3	MeliCERTes 2 (SMART-2018-2014)	37
4.1.4	Mitarbeit an Forschungsprojekten	38
5	Rechtsgrundlage	39
5.1	Netz- und Informationssicherheitsgesetz (NISG)	39
5.1.1	Strategisches NIS-Büro	39
5.1.2	Aktivitäten auf EU-Ebene	40

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, Mai 2023.

Vorwort: Wolfgang Rosenkranz (CERT.at)

Der Beginn des Jahres 2022 war geprägt von der Sorge, dass die IT-Security-Verantwortlichen der Welt die Zeit rund um den Jahreswechsel damit verbringen würden, den Untergang der Digitalisierung zu verhindern - ausgelöst durch eine Schwachstelle in log4j, einer vergleichsweise irrelevanten Komponente im Open Source Universum. Viele der älteren IT-Security-Experten werden sich an Y2k¹ erinnert gefühlt haben, auch wenn sich die Aufregung bei log4j auf den Security-Bereich fokussiert hat und der Rest der Welt sich dazu weniger Sorgen gemacht hat als um den "Millennium Bug".

Dabei wäre eine größere Aufregung durchaus gerechtfertigt gewesen, denn erstens sind wir im Jahr 2022 wesentlich stärker vernetzt und massiv abhängiger von der Digitalisierung als im Jahr 2000. Und zweitens ist log4j kein technischer Defekt sondern eine Schwachstelle, deren Ausnutzung davon abhängt, ob ein Mensch beschließt, sie für seine Zwecke zu nutzen und der damit verbunden entscheidet, wie viel Schaden er damit anrichten will. Weiterhin leidet die Diskussion rund um das Thema Cybersecurity darunter, dass außerhalb des Expertenkreises nicht ausreichend verstanden wird, dass wir es mit Menschen als Gegnern zu tun haben, auch wenn sie uns über Maschinen angreifen. Und dass diese Tatsache die Bedrohung, die wir versuchen einzudämmen, so bedrohlich macht. Denn gegen einen technischen Defekt wie Y2k kann ich Maßnahmen ergreifen, die - wenn sie gut sind - die Auswirkungen des Defekts verhindern. Gegen einen menschlichen Gegner kann ich auch Maßnahmen ergreifen. Aber wenn er merkt, dass seine erste Idee nicht funktioniert, wird er einen anderen Weg suchen, anzugreifen.

Das Verständnis, dass Menschen gefährlich sein können, wurde aber bald nach dem Jahreswechsel durch ein anderes Ereignis deutlich dargestellt. Der Ausbruch des Ukrainekrieges, der uns auch 2023 noch beschäftigt, war für die meisten von uns überraschend. Nicht, weil sich der Krieg nicht angekündigt hat - das hat er seit 2014 getan. Sondern weil dann tatsächlich eingetreten ist, was für viele in Europa und darüber hinaus undenkbar erschien. Im CERT-Umfeld war der physische Kriegsausbruch dabei gar nicht das Initialereignis für eine erhöhte Aktivität. Denn schon Wochen und Monate davor wurden IT- und OT-Systeme in der Ukraine angegriffen und es war aus reiner Vorsicht notwendig, dass auch Angriffe auf die EU, als Unterstützer der Ukraine, erwartet werden. Wir hatten deshalb schon seit Jahresbeginn das Ukraine-Thema auf der Agenda jedes Abstimmungstreffens, ob intern oder mit unseren Partnern bei Behörden und der Wirtschaft.

Eine der Kernaufgaben des CERT ist die Rolle als Informationsdrehscheibe und damit als Bereitsteller von Daten und Fakten für die Lagebilderstellung. Deshalb war unser Fokus in der ersten Jahreshälfte alles, was nur marginal auf direkte oder indirekte Angriffe auf Systeme in Österreich oder der EU hindeutete. Der ATC Jahreskongress in Loipersdorf hatte auch einen Ukraine-Schwerpunkt und wir waren unter den ersten, die Oberst Markus Reisner, der seit damals Dauergast bei allen Veranstaltungen und Sendungen zum Ukraine-Krieg ist, zu einem Ukraine-Vortrag eingeladen haben. Die Absicht war damals, die Akteure des hybriden Kriegsschauplatzes - physisch und digital - zusammenzubringen, denn wir haben fix damit gerechnet, dass wir bald zusammenarbeiten müssten.

Angekündigte Katastrophen finden nicht statt, sagt das Sprichwort. In der Ukraine wird man das so nicht sehen, aber im Cyberbereich außerhalb der Ukraine war es - im Vergleich dazu, was

¹<https://de.wikipedia.org/wiki/Jahr-2000-Problem>

erwartet wurde - still. Einzelne Ereignisse konnten direkt oder indirekt mit dem Krieg verbunden werden. Aber von der geballten Macht der russischen Cyberangriffsmaschine war in Europa bei weitem nicht so viel zu bemerken, wie wir alle befürchtet haben. Die Ursache dafür ist immer noch nicht eindeutig feststellbar und wird vermutlich erst durch Historiker beleuchtet werden.

Aber das Ausbleiben der großen Angriffe hat gezeigt, dass wir eine Informationslücke haben. War der Aufwand für Angriffe innerhalb der Ukraine zu groß für die vorhandenen Kapazitäten, so dass sie keine anderen Ziele mehr angreifen konnten? War die Sorge vor Gegenangriffen die Ursache? Oder überschätzen wir die Fähigkeiten der bisher bekannten Gruppen an staatlich unterstützten Angreifern? Auch 2023 gibt es dazu noch keine eindeutigen Antworten. Und wir hatten 2022 ausreichend andere Cyberangriffe in Österreich, so dass leicht belegt werden kann, dass Cybersecurity eine Pflichtaufgabe ist, unabhängig von einem Krieg in der Nachbarschaft.

Aber es bleibt der unangenehme Nachgeschmack, dass wir und viele andere uns mit unseren ersten Einschätzungen geirrt haben und darüber werden wir auch 2023 noch diskutieren. Jetzt, 2023, ist der Krieg noch voll im Gange. Sofern er hoffentlich bald endet, wird es spannend sein zu sehen, ob die dann freiwerdenden Cyber-Angriffskapazitäten dann auf andere Ziele gerichtet werden. Als nationales CERT, als Betreiber des Austrian Energy CERT und durch unsere Zusammenarbeit mit dem Government CERT sind wir weiterhin auf der Hut.

Ob der nächste Angriff mit dem Krieg in der Ukraine zu tun hat oder ob ein Cyberkrimineller nur den Tank für seinen Sportwagen mit Erpressungsgeld füllen will: unsere Aufmerksamkeit haben sie alle. Und alle Informationen, die wir dazu erhalten oder durch Analysen selbst erzeugen, senden wir an weiterhin an jene, die sie benötigen. Wie wir das 2022 im Detail gemacht haben, darüber gibt dieser Jahresbericht Auskunft. Viel Vergnügen bei der Lektüre!

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 Kontaktpunkt 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 2022:

- Erich Albrechtowitz (BKA)
- DI Philipp Blauensteiner (BVT)
- Christina Buttlinger (BMLV)
- 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)

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 Network and Information Systems”. 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 Cyber Angriffs. 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 österreichische Kontaktstelle 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 Frühwarnungen 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 OpKoord¹ und IKDOK² 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 diesen Bedrohungsanstieg effektiv zu managen:

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

¹Operative Koordinierungsstrukturen im Cybersicherheitsfall.

²Der Inneren Kreis der operativen Koordinierungsstrukturen 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 fehlerkonfigurierte Server. Dazu stützen sich CERT.at und GovCERT Austria neben selbst entwickelter Sensorik auf Quellen³ 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. Domain Eigentümer beschränkt, agieren CERT.at und GovCERT Austria bei größeren Vorfällen als Koordinationsstelle und Schnittstelle zwischen den Betroffenen und anderen relevanten Akteuren 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 Events der IT Security Community bis hin zur Mitarbeit bei Forschungsprojekten.

1.4 Zertifizierungen 2022

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.

³Eine 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. Nachdem in den letzten beiden Vorjahren nur Zwischenaudits nötig waren, fand 2022 eine volle Re-Zertifizierung statt. Diese bestätigte, dass wir das geforderte Sicherheitsniveau eingehalten haben.

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 2022) eines von **acht** 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 "listed" geführt.

Im Rahmen des CSIRTs Network wurden 2022 SIM3 Peer-Reviews durchgeführt. Für CERT.at war der Partner unseren Kollegen vom deutschen CERT-Bund, für das GovCERT war es SK-CERT.

Kapitel 2

Das IT-Sicherheitsjahr 2022

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.

Pflichtmeldungen laut §19 (Betreiber wesentlicher Dienste) und §21 (Anbieter digitaler Dienste) NISG sind dann vorgeschrieben, 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

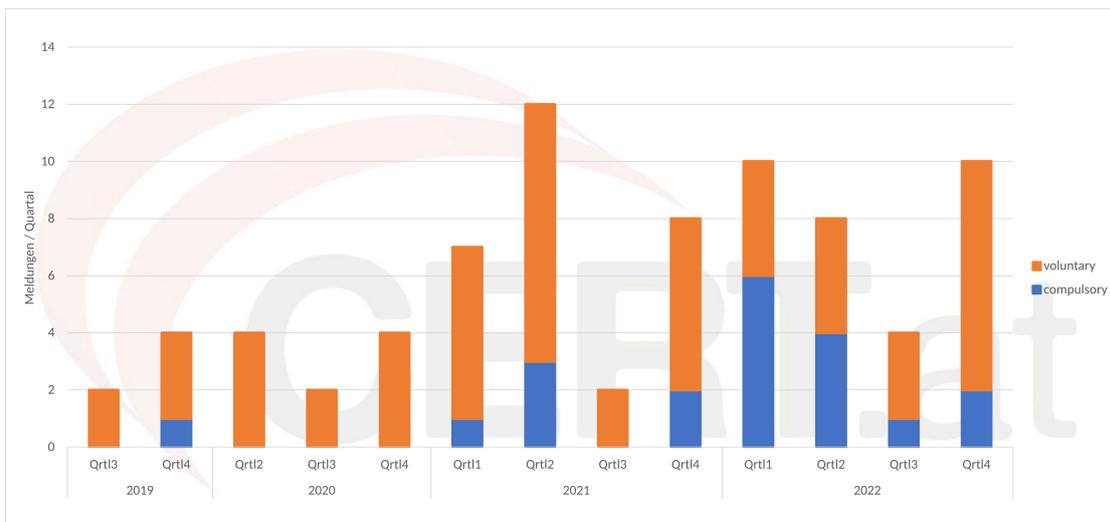


Abbildung 2.1: NIS Meldungen 2019 - 2022: Meldungsart

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. Mit in Summe 32 Meldungen in 2022 liefert diese Informationsquelle keine ausreichende Zahlenbasis, 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.

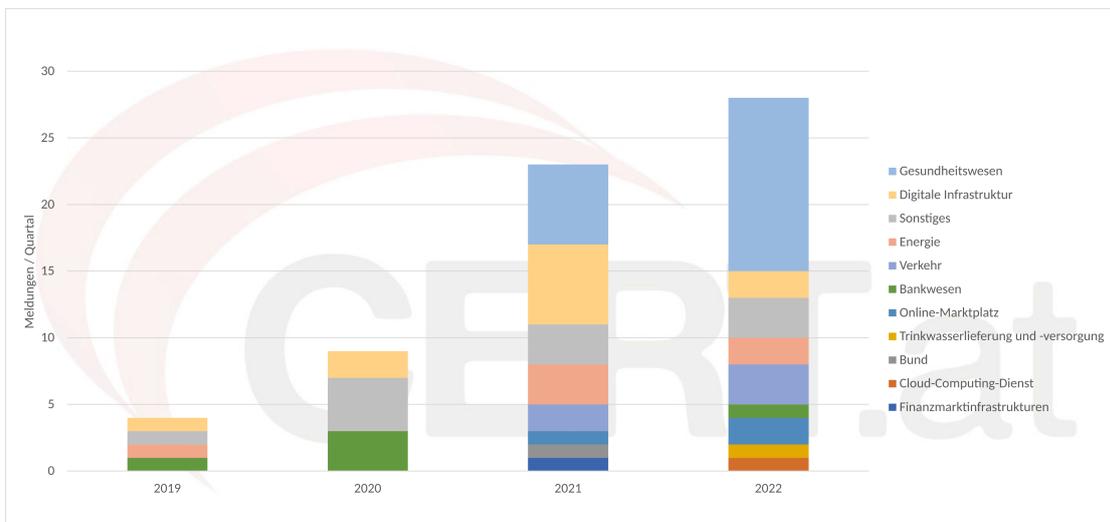


Abbildung 2.2: NIS Meldungen 2019 - 2022: Sektorenverteilung

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 CERT.ats mit Betroffenen. Auch diese kann automatisiert, wie im Falle von ISPs (Internet Service Providern), oder persönlich, wie bei einer Responsible Disclosure, erfolgen.

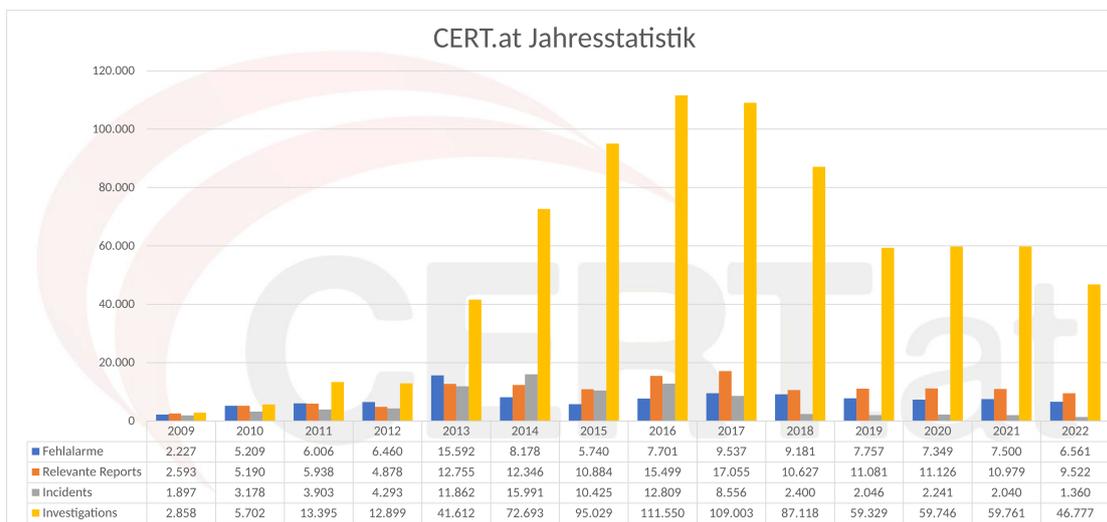


Abbildung 2.3: Incident Reports, Incidents und Investigations im Überblick

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 stärker auf Meldungen von Privatpersonen oder auch Firmen zu konzentrieren, anstatt täglich

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

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 befallenen 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.

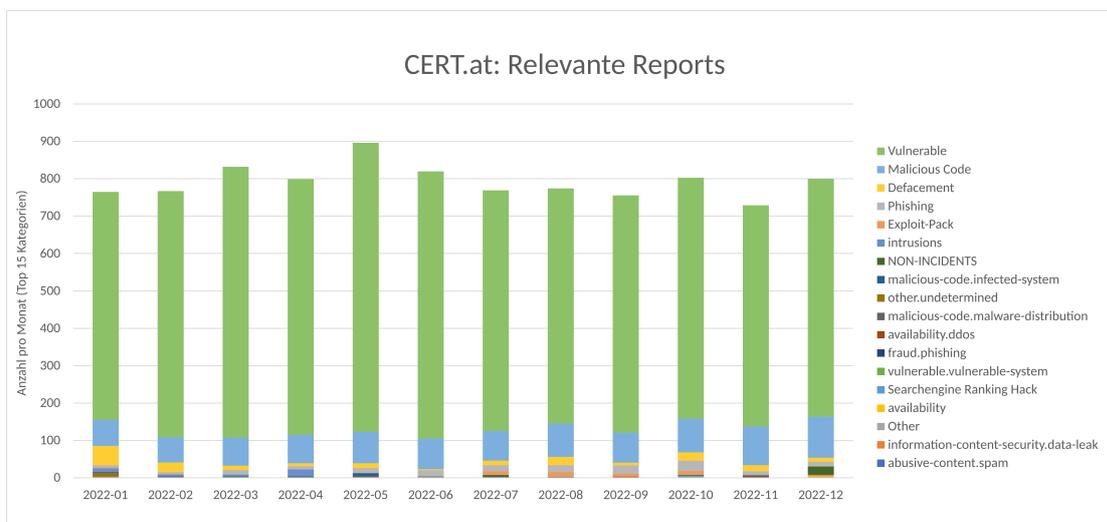


Abbildung 2.4: Incident Reports

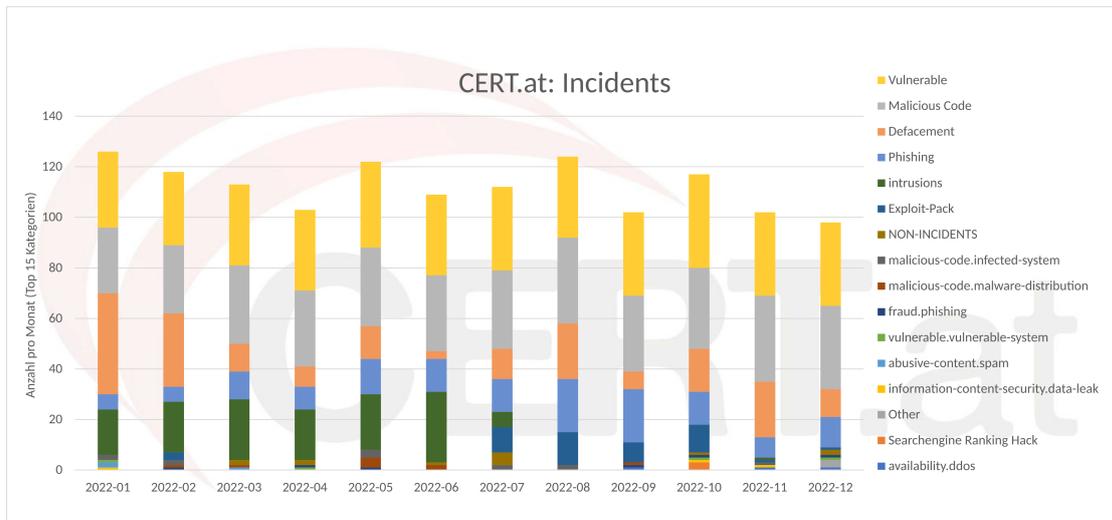


Abbildung 2.5: Incidents

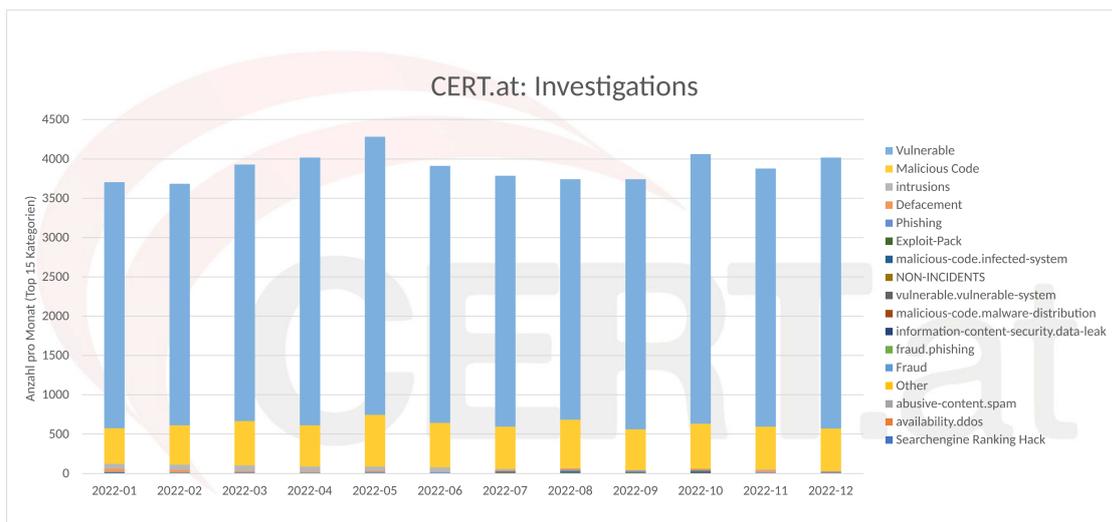


Abbildung 2.6: Investigations

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, siehe dazu [2.4.2](#).

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 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 Passwörtern oder das Ausnutzen (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 autorisierte 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 2022 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.

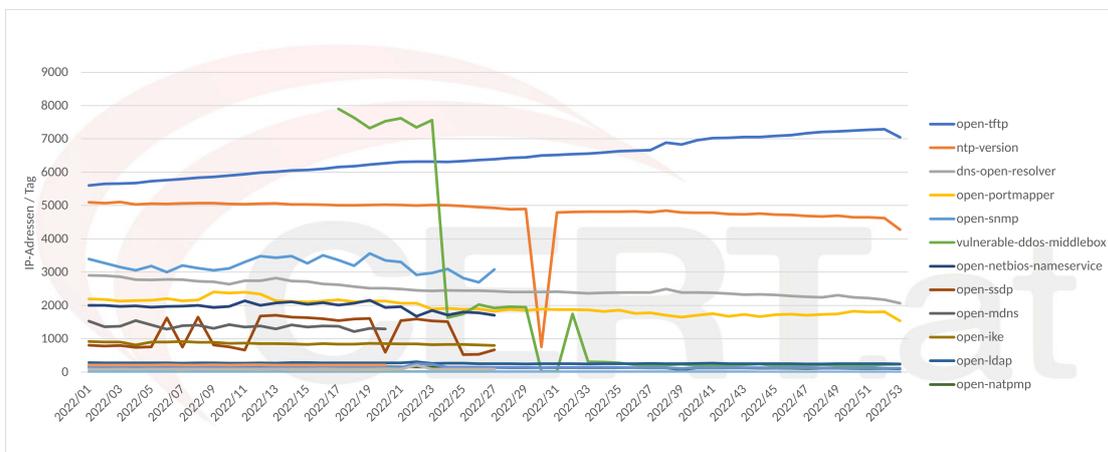


Abbildung 2.7: Events nach **Taxonomie** (logarithmische Skala)

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.

Mitte 2022 kam es wegen Umstellungen bei den Quellen mancher Datenfeeds zu Aussetzern in der Verarbeitung.

²Für eine genauere Beschreibung siehe [2.5 Datenbasis](#).

2.4.1 Taxonomie “vulnerable”

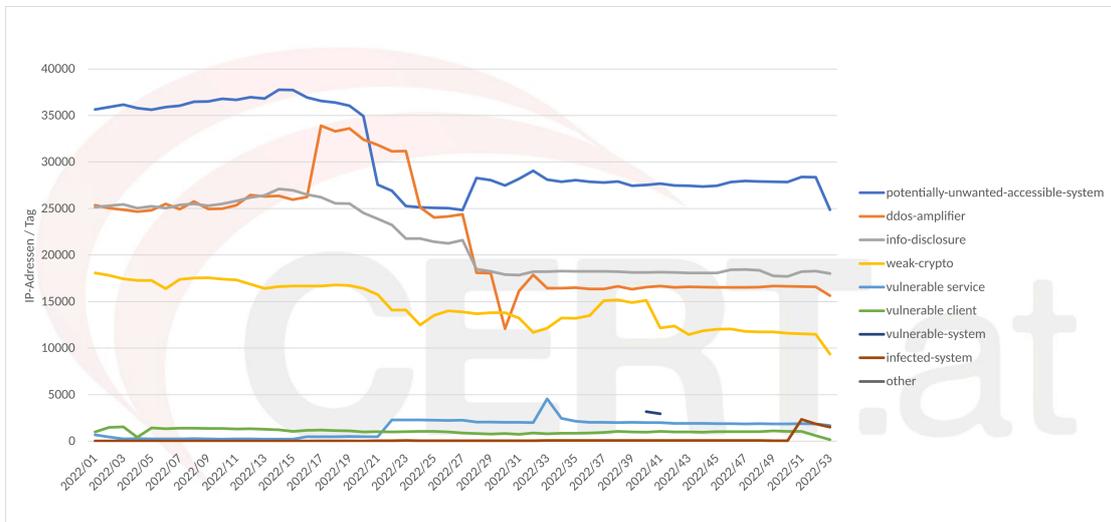


Abbildung 2.8: Alle Events der Taxonomie “vulnerable”

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)

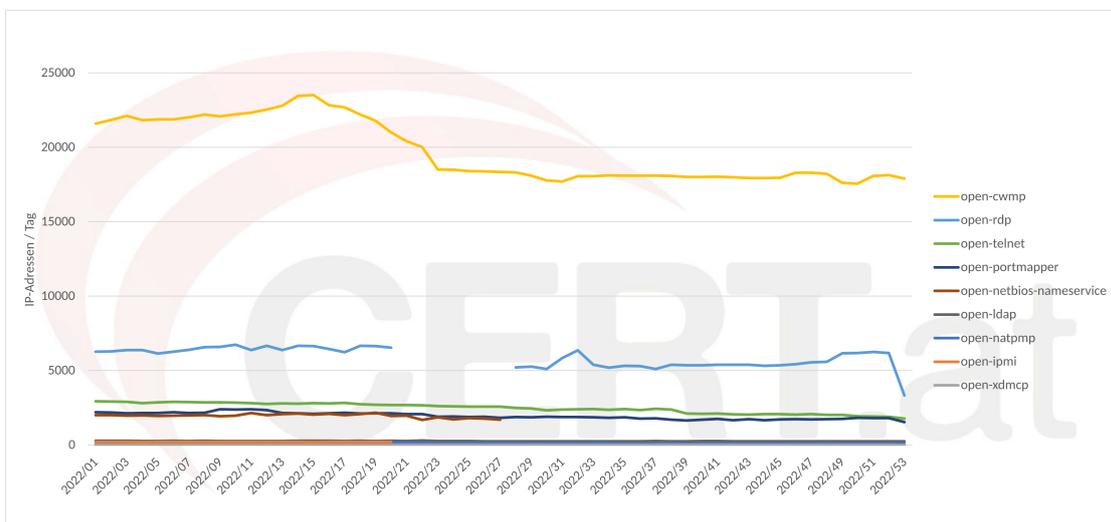


Abbildung 2.9: Ports, die nicht öffentlich erreichbar sein sollten

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

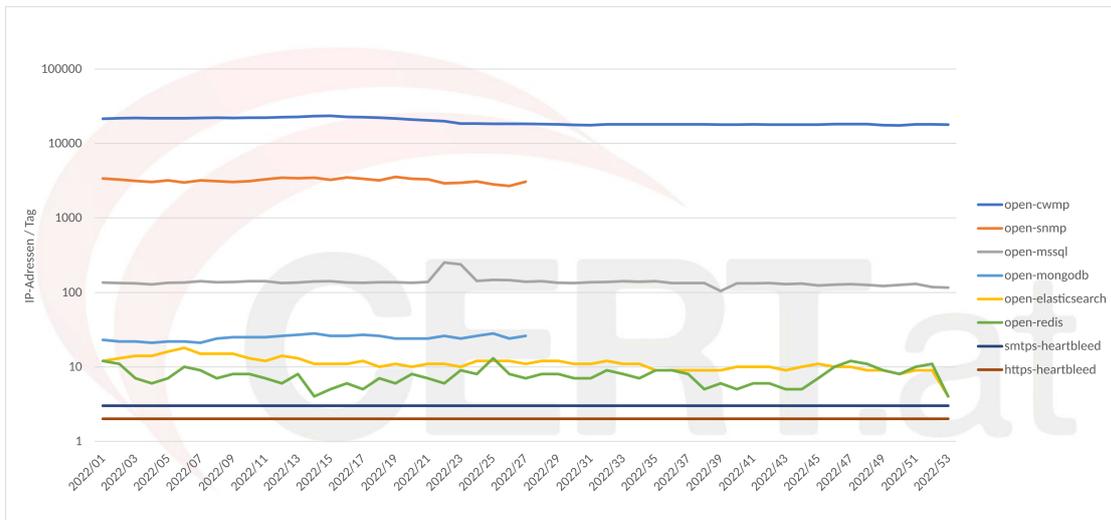


Abbildung 2.10: Services, über die sensible Informationen gewonnen werden können

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](#))

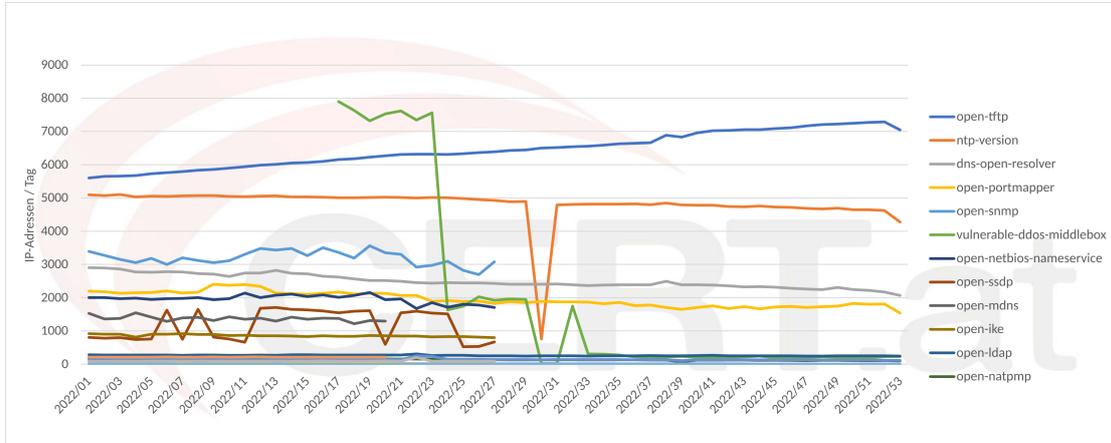


Abbildung 2.11: Geräte, die für UDP DDoS Amplifikation missbraucht werden können

Wie auch in den Jahren zuvor, fiel 2022 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 "potenziell 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 dem/der BetreiberIn 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 Probleme im Web

Das World Wide Web stellt zwar nur einen Teil des Internets dar, ist aber dennoch für viele der Inbegriff des Netzes. Webseiten sind komplex und die möglichen Probleme damit vielseitig. Im Jahr 2021 geht es hier bei weitem nicht mehr nur simple Visitenkarten im Web, oder einfache Webshops, sondern auch um komplexe Software-as-a-Service Angebote, die ganze Anwendungssuites als Webapplikation implementieren.

Einerseits geht es um die Verwundbarkeiten der Servers und der darauf laufenden Software, andererseits geht es um die maliziöse Inhalte, die vom Webserver ausgeliefert werden. Diese sind oft nicht trivial von automatischen Systemen erkennbar, sondern brauchen eine manuelle Einschätzung durch die Experten.

Das hat auch damit zu tun, dass das Web extrem schnelllebig ist, was zur Folge hat, dass viele Probleme, die vor einigen Stunden gemeldet wurden, bereits behoben sind und daher immer eine Person direkt vor dem Aussenden kontrollieren muss, ob das Problem noch besteht. Nur so können große Mengen an Falschmeldungen unsererseits verhindert werden.

Ein weiterer Grund, warum Automatisierung bei Problemen im Web nicht immer gut funktioniert, ist, dass es in vielen Fällen um die Beurteilung der Legitimität von Inhalten geht. So ist der Schriftzug "defaced by" zwar eine Phrase, sie sehr häufig bei Defacements (s.u.) auftritt, aber gleichzeitig oft auf Seiten von Museen oder Ausstellungen vorkommt, auf denen Kunstwerke

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

beschrieben werden, die irgendwann “defaced”, d.h. verunstaltet bzw. mutwillig beschädigt wurden. Hin und wieder treffen wir sogar auf Webseiten, bei denen sich im Nachhinein herausstellt, dass der augenscheinliche Hack eine Kunstinstallation ist, die ein Defacement imitiert oder eine angebliche Phishing-Seite in Wahrheit Teil eines gerade laufenden Pentests ist.

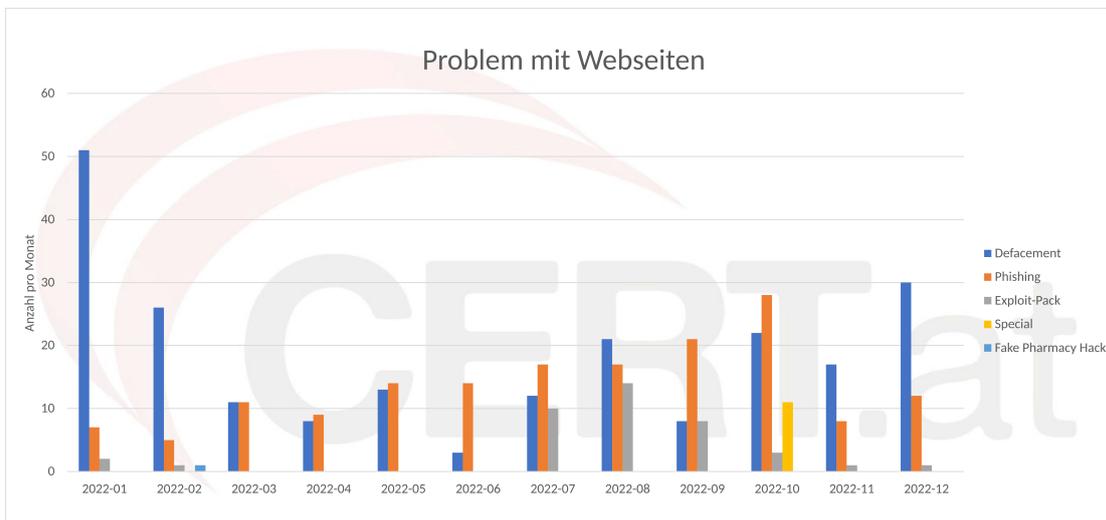


Abbildung 2.12: Probleme mit Webservern

Defacements

Bei diesen auch als “Web-Graffiti” bezeichneten Angriffen, wird das Aussehen bzw. Design einer Webseite verändert. Oft wird einfach der Spruch “Hacked by” oder “Defaced by” gefolgt von einem Namen prominent auf der Startseite platziert. Andere, politisch motivierte Tätergruppen, hinterlassen hingegen martialische Sprüche und Bilder. Insbesondere während geopolitischer Spannungen versuchen “Hacktivist:innen” der Konfliktparteien, möglichst viele Webseiten im Land des Gegners zu verunstalten.

Diese Art von Angriffen hat in den letzten Jahren in Österreich kontinuierlich an Bedeutung verloren, was wohl einerseits daran liegt, dass Standardsoftware zum Anlegen von Webseiten (wie z.B. WordPress) wesentlich sicherer ist als früher und Updates automatisch eingespielt werden, andererseits aber auch mit dem erhöhten Bewusstsein bei Firmen zu tun hat, dass ihre Webseiten potentielle Angriffsziele sind und diese daher besser abgesichert werden.

Dennoch kommt es immer wieder zu wellenartigen Angriffen dieser Art, beispielsweise wenn eine neue Schwachstelle in einem populären CMS bekannt wird.

Phishing

Während Defacements im Allgemeinen eher harmlos sind und wenn überhaupt zu einem Reputationsschaden führen, sind Phishingseiten immer problematisch. Hier versuchen Angreifer:innen Zugangsdaten von Besucher:innen zu stehlen, indem sie beispielsweise die Login-Seite

einer Bank nachbauen.

Dass die Anzahl der Phishings relativ stark schwankt, ist unter anderem mit dem Kampagnencharakter solcher Angriffe zu erklären: Kriminelle kompromittieren vor dem Aussenden der Phishing-Mails gleich eine größere Anzahl von Webseiten, damit das Bereinigen einzelner Phishingseiten nicht direkt den gesamten Angriff beendet. Nach dem Beginn einer solchen Kampagne gehen dann oft viele Meldungen zu Phishing-Seiten auf einmal ein.

Exploit Packs

Bei diesem Angriff werden auf einer (zumeist) legitimen Seite Inhalte eingebaut, die Schwachstellen im Webbrowser eines Besuchers ausnutzen, um dort Schadsoftware zu installieren.

Mit dem Aussterben der oft verwundbaren Browser-Erweiterungen (Flash, Java, Silverlight, ...) und den schnellen automatischen Updates der großen Browser sind Exploit Packs deutlich weniger effektiv geworden.

2.4.3 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.

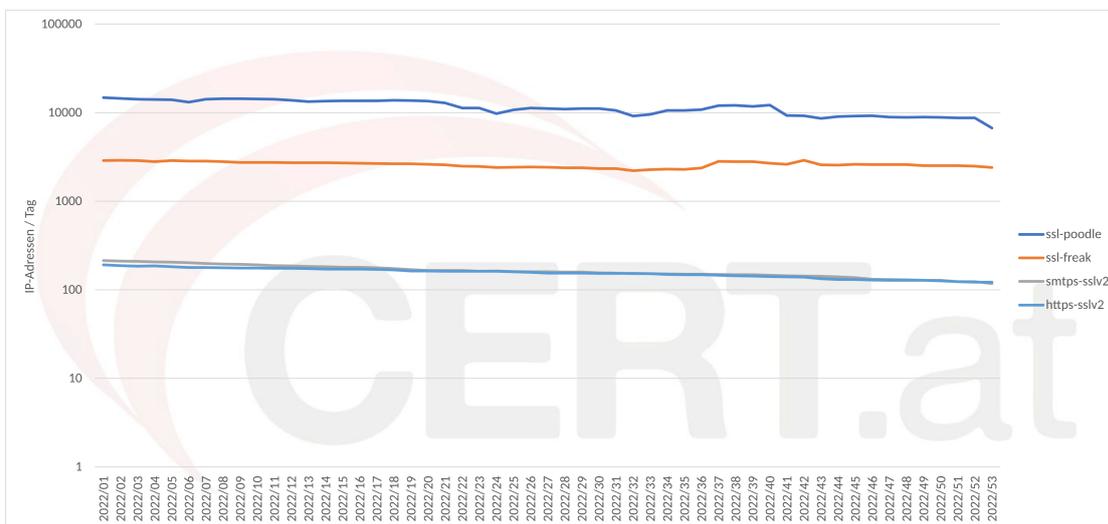


Abbildung 2.13: Unsichere Kryptographie

2.4.4 Malware

Im Jahr 2022 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.

Eine weitere Entwicklung war die Verwendung von "Living off the Land"-Techniken, bei denen Malware so konzipiert wird, dass sie schwer zu erkennen ist, indem sie legitime Systemtools und Dienstprogramme ausnutzt, die bereits auf den betroffenen Systemen vorhanden sind. Dies erschwert die Erkennung und Abwehr von Malware und ermöglicht es den Angreifern, länger unentdeckt zu bleiben.

Im Jahr 2022 wurden auch vermehrt mobile Malware-Angriffe beobachtet. Mit dem zunehmenden Einsatz von mobilen Geräten und der Popularität von mobilen Apps sind Cyberkriminelle verstärkt auf mobile Malware ausgerichtet, um sensible Informationen wie Passwörter, Bankdaten und persönliche Informationen von Benutzern zu stehlen. 2021 war [FluBot](#) ein heikles Thema; 2022 gelang es, die [Infrastruktur der Tätergruppe zu zerschlagen](#).

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 notwendig, 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.

2022 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 Schwachstelle, d.h. Angreifer:innen können dadurch auf Dateien außerhalb des Web-Root Verzeichnisses des Webserver 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-2021-26855 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.

CVE-2021-34473 besser bekannt als "ProxyShell", ist eine Sicherheitslücke, die es Angreifer:innen ermöglicht, ohne jegliche Authentifizierung beliebige Befehle als 'NT Authority\System'

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

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.

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 vor im Bereich Analyse von Botnetzen und Malware arbeitet. Dazu wurde ein riesiges Netzwerk aus Honeypots⁵ 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 viele der Informationen, die zur unseren Warnungen über verwundbare bzw. missbrauchbare Systeme (siehe Kapitel [2.4.1](#)) führen.

Eine weitere große NPO in diesem Bereich ist [Spamhaus](#). Diese Organisation hat sich auf den Kampf gegen Network Abuse spezialisiert.

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 Disclosures⁶ 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

⁵Das 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.

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

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.

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-Netztes 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 entwickelt, 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 IntelMQ⁷ 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 entwickeln, 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 verarbeiten, 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 2022

Nach der Veröffentlichung von IntelMQ 3.0.0 Vorjahr wurde 2022 signifikante Entwicklungsarbeit in Optimierungen hinsichtlich der Effizienz und Wartbarkeit des Codes investiert. Besonders hervorzuheben sind hierbei:

- Interne Anpassungen für Bots, für verbesserte Nutzung von Pipelines und effizienteres Load-Balancing

⁷Zusammengesetzt aus "Threat INTElligence" und "Message Queueing".

- Änderungen bei der Handhabung von Feeds, dadurch erleichtertes Einbinden neuer Datenquellen
- Refaktorisierung einiger Kernkomponenten

Eine Übersicht zu den Releases findet sich auf [GitHub](#).

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.

2022 wurde diese Funktion 23 Mal genutzt, unter anderem in folgenden Fällen:

- 10 mal zu [SystemBC](#) Infektionen
- 6 mal zu log4j bzw. log4shell
- 2 mal zu Problemen mit Microsoft Exchange Webinterfaces
- je 1 mal zu den Themen verwundbare Zyxel, Fortinet und BOA Webserver Systemen
- und ein mal, um die Ziele einer DDoS Kampagne vorzuwarnen

2.6.2 MISP

MISP⁸ 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

⁸Das 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.

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

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 2022

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.

2022 fielen darunter einerseits Schwachstellen in verbreiteten Softwarelösungen wie Atlassian Confluence, Magento, Zimbra sowie diversen Produkten von VMWare, als auch Sicherheitslücken in Netzwerkprodukten von Fortinet und Citrix.

Andererseits stellte der Krieg in der Ukraine eine neuartige Erweiterung der Bedrohungslandschaft dar, dessen Auswirkungen auch für Österreich neuartige Herausforderungen mit sich brachte, die neben weiterhin anhaltenden Ransomware-Angriffen zu bewältigen waren.

2.7.1 Ukrainekrieg

Der Angriff der Streitkräfte der Russischen Föderation auf die Ukraine am 24.02.2022 stellte und stellt Europa in jeder Hinsicht vor enorme Herausforderungen. Auch Österreich ist, als europäischer Staat und Teil der europäischen Union, trotz des Status als neutrales Land, mit den Auswirkungen dieses grössten Krieges auf europäischem Boden seit dem Ende des 2. Weltkrieges 1945 konfrontiert.

Auch in unserer Rolle als nationales CERT mussten wir uns unerwarteten Entwicklungen und teils neuartigen Bedrohungen entgegen stellen. Diese geopolitische Ausnahmesituation hat hierzulande vielerorts allerlei Bedenken und Sorgen ausgelöst.

Glücklicherweise sind diese Befürchtungen bisher nicht eingetroffen, heraufbeschworene Horrorszenarien von landesweite Stromausfällen und eventuellen Versorgungsengpässen aufgrund von destruktiven Cyberangriffen gegen kritische Infrastruktur in Österreich sind ausgeblieben.

Dennoch waren sowohl wir als auch unsere nationalen und internationalen Partner:innen in erhöhtem Maß gefordert. Im Rahmen dieser Ereignisse hat sich erneut gezeigt, wie wichtig eingespielte Strukturen, Prozesse und Kommunikationswege im Krisenfall tatsächlich sind. Dies hat

uns ermöglicht, bei Angriffen gegen österreichische Ziele beziehungsweise Angriffen, die Auswirkungen auf österreichische Organisationen hatten, schnell und effizient zu reagieren, sowie Betroffene bestmöglich zu unterstützen.

Auch wenn Sicherheitsunternehmen, Forscher:innen, Journalist:innen und teilweise auch Regierungsinstitutionen seit Beginn des Krieges hunderte Artikel, Beiträge und wissenschaftliche Paper veröffentlicht haben, so kennen wir wahrscheinlich aktuell nur einen Bruchteil der Angriffe, zu denen es im Rahmen des Konflikts gekommen ist.

Das gilt sowohl für Angriffe gegen Ziele innerhalb der Ukraine als auch Angriffe gegen Systeme und Netzwerke außerhalb des Landes, wie diplomatische Vertretungen anderer europäischer Länder. Es ist davon auszugehen, dass uns auch trotz unserer grössten Bemühungen nicht alle Angriffe gegen österreichische IKT-Systeme bekannt sind. Hier wird es in der Zukunft noch viele Lektionen geben, die es zu lernen gibt.

Diese Angriffe stellen allerdings, vor allem was Österreich betrifft, nur einen Bruchteil der Angriffe und Angriffsversuche dar, denen IKT-Systeme Tag für Tag ausgesetzt sind. Bedrohungsakteure, die staatlichen Institutionen in anderen Ländern zugerechnet werden, sind weiterhin aktiv. Für diese Angreifer:innen ist die anderweitig ausgerichtete Aufmerksamkeit ein wahres Geschenk.

Und ganz abgesehen davon, auch alle anderen Bereiche der digitalen Kriminalität, sei es nun Erpressung durch Ransomware, der Missbrauch von kompromittierten Ressourcen zum Schürfen von Kryptowährung oder betrügerische Handlungen im Rahmen von 'Business Email Compromise' florieren leider weiterhin.

2.7.2 Relevante Schwachstellen

Im Jahr 2022 hatten Software-Unternehmen jede Menge Sicherheitslücken in ihren Produkten zu beheben. Zu folgenden Schwachstellen haben wir 2022 Warnungen und Blogposts veröffentlicht.

Webapplikationen

In dieser Kategorie fallen vorallem Zimbra (17 CVEs), Atlassian (11 CVEs), und Magento (9 CVEs) auf. Atlassian hatte mit Authentication-Bypasses zu kämpfen (insb. CVE-2022-26134, welche im Mai als 0-Day aktiv ausgenutzt wurde), Zimbra mit Information Disclosure (CVE-2022-32294), und Magento mit dem Einbau von sogenannten Digital-Skimmern¹⁰.

Microsofts Exchange-Server sticht dabei ebenfalls heraus: Darin wurden eine Vielzahl an Lücken¹¹ gefunden, die zu Information Disclosure, Privilege Escalation, und Remote Code Execu-

¹⁰ Abgreifen von Kreditkartendaten während des Bezahlvorgangs auf einer Webseite in digitaler Form; Pendant zu klassischem Skimming, bei dem Kartendaten über manipulierte Terminals abgefangen werden.

¹¹ CVE-2022-41123, CVE-2022-41082, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41040, CVE-2022-34692, CVE-2022-30134, CVE-2022-24516, CVE-2022-24477, CVE-2022-24463, CVE-2022-23277, CVE-2022-21980, CVE-2022-21979, CVE-2022-21978, CVE-2022-21969, CVE-2022-21855 und CVE-2022-21846 laut [CVE Details](#)

tion führen konnten.

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 Virtualisierungsplattformen.

Dabei auffallend waren Firewalls und Router mit Schwachstellen, die in weiterer Folge zur Remote Code Execution (RCE) führten. Anders als bei klassischen Applikationen und Services ist es oft schwierig, betroffene Geräte dieser Kategorie "einfach abzdrehen" – das rasche Einspielen verfügbarer Patches ist oft der einzige gangbare Weg.

Fortinet (CVE-2022-42475 & CVE-2022-40684), Cisco (CVE-2022-20842), und Zyxel (CVE-2022-30525) dienen hier als Beispiel: In allen Fällen wurde durch den Hersteller zum Zeitpunkt der Veröffentlichung der Schwachstelle 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 2022 mit kritischen Lücken zu kämpfen: Citrix (CVE-2022-27518) und VMware (CVE-2022-31685, CVE-2022-31686, CVE-2022-31687) mussten 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](#)".

2.8 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 im normalen 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

Gegen Ende des Jahres, konkret Anfang Dezember, wurden in Österreich staatliche und staatsnahe Organisationen sowie Unternehmen der kritischen Infrastruktur Opfer von DDoS-Angriffen. Betroffen waren dabei hauptsächlich die Nameserver der angegriffenen Ziele, jedoch wurden auch Schwächen in Webapplikationen missbraucht, um die darunterliegenden Webserver unter der Last der Anfragen in die Knie zu zwingen. Aufgrund des generell hohen Sicherheitsniveaus der Opfer war die Auswirkung der Angriffe auf die Verfügbarkeit der betroffenen Systeme und Services in den meisten Fällen sehr gering.

Zu den Angriffen bekannte sich ein hacktivistischer, pro-russisch orientierter Bedrohungsakteur, der unter dem Namen "Killnet" seit Beginn des Krieges in der Ukraine bereits vielfach vermeintlich "westliche" und "russlandfeindliche" Ziele in's Visier genommen hatte. Da die Angreifer:innen die Angriffe vor Beginn ankündigten, und dabei auch ihre Ziele veröffentlichten, war es uns in vielen Fällen möglich, zu erwartende Betroffene frühzeitig zu informieren und es diesen so zu ermöglichen, bereits vor den Angriffen erste Schritte zur Mitigation selbiger zu setzen.

In weiterer Folge informierten wir auf unserer Webseite über die erfolgten Angriffe um ein allgemeineres Bewusstsein für diese zu schaffen. Die in dieser Veröffentlichung inkludierten Empfehlungen basierten neben unserer Erfahrung vor allem auch auf im Rahmen der Vorfallsbehandlung gesammelten Erfahrungen, die betroffene Unternehmen und Organisationen mit uns geteilt haben. Dies ermöglichte es uns wiederum, potentiell zukünftig betroffenen Zielen einen Informationsvorsprung zu verschaffen.

2.8.2 Unterstützung bei Ransomware-Incidents

Leider ist das Phänomen von Verschlüsselungsangriffen auch dieses Jahr nicht von der Bildfläche verschwunden, unglücklicherweise scheint das Gegenteil der Fall zu sein. Dementsprechend waren bedauerlicherweise auch österreichische Unternehmen Opfer solcher Angriffe.

In einer Anzahl von Fällen ist es uns glücklicherweise gelungen Unternehmen und Organisationen zu warnen, bevor es zu einem tatsächlichen Angriff beziehungsweise einer Durchführung der Verschlüsselung nach einer erfolgreichen Kompromittierung eines Netzwerkes durch Angreifer:innen kommen konnte. Hierbei war die Zusammenarbeit mit Partnerorganisationen und Sicherheitsexpert:innen von vorrangiger Bedeutung, die uns zeitnah über im Rahmen von polizeilichen Ermittlungen oder forensischen Untersuchungen gewonnene Erkenntnisse in Kenntnis

setzen.

Durch unsere Expertise und Erfahrung konnten wir allerdings auch einigen Betroffenen helfen, bei denen die Verschlüsselung bereits erfolgt war.

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 in ihrer Arbeit an jede Österreicherin und jeden Österreicher. Diese sind KundInnen – 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. Wegen der Pandemie haben sich einige Aktivitäten auch zu hybriden Formaten entwickelt.

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 bestehen 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 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.

Aufgrund der Pandemie war der ATC in seinen Treffen weiterhin eingeschränkt, jedoch war es mit dem Jahrestreffen in Loipersdorf sowie einigen Quartalstreffen einzelner Sektoren erstmals möglich, wieder in die Normalität zurückzukehren.

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 2022 fanden alle 6 Treffen wieder physisch statt. Mit Stand Ende 2022 nehmen weiterhin 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 bekamen 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 Koordination 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) wanderte diese Agenden gemeinsam mit den anderen der operativen NIS Behörde in die [Abteilung IV/10](#) des Innenministerium.

Damit sind die folgenden Akteure im IKDOK aktiv: Das Bundeskanzleramt (BKA) mit dem GovCERT, die Direktion für Staatsschutz und Nachrichtendienst (BMI/DSN), das Cybercrime Competence Center (BMI/BK), 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 sind alle nationalen CERTs (in diesem Kontext: CSIRTs, die laut §9 der NIS-Direktive akkreditiert sind) der EU-Mitgliedsländer, wobei es sich größtenteils um staatliche Stellen handelt. 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 (2022 war das erste Meeting im Februar noch virtuell, im Mai (Paris) und September (Brno) waren wieder physische Treffen möglich), 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. 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 Lösungen¹ und eine gemeinsame Taxonomie (siehe 2.3: Taxonomie) gesetzt. Im Rahmen des **Meli-CERTes 2 Projektes** haben Mitarbeiter von CERT.at beim Design und Implementation der IT-Infrastruktur des CSIRTs Networks mitgewirkt.

Im Rahmen der Europäischen Notfallsübung **Cyber Europe 2022** wurde im Sommer 2022 das Zusammenspiel der Teams im CSIRTs Network geübt.

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 400 Mitglieder) stehen nicht mehr einzelne Vorfälle im Fokus von FIRST, sondern vielmehr der Erfahrungsaustausch, Lobbying und das gemeinsame 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

¹Konkret unter anderem **MISP** und **IntelMQ**.

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](#).

Vom Traffic Light Protocol wurde 2022 die [neue Version 2.0 standardisiert](#): zu dem alten TLP:AMBER (Weitergabe im Team und an die Constituency auf "Need-to-know Basis") kam ein TLP:AMBER+Strict dazu, was zweiteres nicht erlaubt. Weiters wurde TLP:WHITE auf TLP:CLEAR umbenannt.

Das Netzwerk trifft sich zum einen bei der jährlichen internationalen Konferenz, welche 2022 zum ersten Mal seit 2019 wieder physisch stattfinden konnte, und zum anderen bei zahlreichen themen- oder regionspezifischen Treffen.

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-kofinanzierte 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 NIS-Gesetz) aus. Das wollen wir mit diesem Projekt verbessern.

Einerseits geht es um die Aufbereitung der bereits im CERT vorhandenen Daten, die aber in diversen Systemen verteilt sind. So etwa könnten Informationen zu einer DDoS-Kampagne auf folgende Systeme verteilt sein: Ticketsystem, OSINT, nationale und internationale IM-Systeme und MISP. Eine zentrale Suche über alle diese Systeme soll die Frage nach "Was wissen wir zu

Thema X?“ umfassend beantworten können. Ein automationsgestütztes Clustering kann dann zu einem funktionalen User-Interface führen, in dem unser Analyst einen Lagebericht zusammenstellen und manuell ergänzen kann. Diese soll dann über ein bidirektionales Interface mit der operativen Ebene geteilt werden können. Wir setzen hier auf das Tool [Taranis NG](#) auf, das von den Kollegen von SK-CERT entwickelt wurde.

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 NG - AWAKE Version](#) und [KoordTool](#).

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 eingebunden. Es geht für uns darum, Risikofaktoren für Domains zu entwickeln und diese auf Basis der Daten, die in der Registry vorhanden sind, zu ermitteln.

Die Vorgabe aus der NIS2 Direktive, dass die Identität von Domaininhabern validiert werden muss, gibt dem Projekt auch auf Seite der nic.at Druck, denn wenn in diesem Vorgang eine Risikoinschätzung einer Domainregistrierung einfließen könnte, sind Prozessoptimierungen möglich.

Da wir bei der Besetzung der Stelle eines ”Research Engineer Internet“ keine geeignete Bewerbungen bekamen, hat sich der Fortschritt des Projektes im Jahr 2022 in Grenzen gehalten.

4.1.3 MeliCERTes 2 (SMART-2018-2014)

Das im 2020 begonnene Projekt MeliCERTes 2 (siehe Jahresbericht 2020 für den ausführlichen Hintergrund) soll die Werkzeuge, die sowohl die einzelnen CSIRTs für die lokale Arbeit einsetzen, als auch die Kommunikationsmittel im CSIRTs Network weiterentwickeln und dabei die ENISA in ihrer Rolle als Sekretariat des Netzwerks unterstützen.

Im Bereich der ”local tools“ war für CERT.at weiterhin der Fokus auf der Pflege, Weiterentwicklung und dem Support von IntelMQ. Dazu wurde eine Serie von (online) Workshops abgehalten: ”IntelMQ - Introduction and Concepts“ und ”IntelMQ - Hands-on Tutorial“.

In einigen Fällen wurde auch direkte Hilfe geleistet, etwa im Oktober vor Ort bei NCSC-NL, weiters per Email und Videokonferenz (u.A. cert-se) geleistet.

Für die zentralen Tools (etwa [Cerebrate](#)) im CSIRTs Network ging es in die Umsetzungsphase, die überraschend mühsam war.

Das Projekt wurde im Dezember 2022 abgeschlossen.

4.1.4 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.

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, übernimmt 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](https://www.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 Informationssystemicherheit (“strategisches NIS-Büro”) hatte schon 2021 die Ermittlungen der Betreiber wesentlicher Dienste auf Grundlage der NIS-Verordnung abgeschlossen. Der Fokus 2022 war die Vertretung Österreichs in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, insbesondere die Koordination und Vertretung der österreichischen Position in den Verhandlungen zur NIS-2-Richtlinie.

5.1.2 Aktivitäten auf EU-Ebene

Die NIS-2-Richtlinie wurde im [November 2022 von der EU verabschiedet](#). Sie wird die Aufgaben der CSIRTs in den Mitgliedstaaten zwar nur leicht erweitern, aber die Zahl der von der Richtlinie erfassten Organisationen wird sich vervielfachen.

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.

Auch DORA ("digitale operationale Resilienz im Finanzsektor") wurde im [November 2022 verabschiedet](#).

Die Verhandlungen zur [Critical Entities Resilience \(CER\) Richtlinie](#) sind hingegen noch nicht abgeschlossen.

Der [Cyber Resilience Act \(CRA\)](#), der im September 2022 von der EU Kommission vorgeschlagen wurde, 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.