GovCERT Austria

CERT.at

Bericht

Internet-Sicherheit

Österreich 2021

Inhaltsverzeichnis

Impressum

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

Konzeption und Redaktion: CERT.at

Herstellungsort: Wien, Mai 2023.

Vorwort: Wolfgang Rosenkranz (CERT.at)

Nach dem Ausbruch der Pandemie im Jahr 2020 war die Sorge groß, dass die damit massiv angestiegene Abhängigkeit von Videokonferenzen, Cloudspeichern, VPN-Verbindungen, etc. von kriminiellen Kräften und von staatlich unterstützten Akteuren ausgenutzt werden könnte, um ihre Ziele noch skrupelloser zu erreichen. Die Angriffe wurden tatsächlich intensiver, Ransomware wurde auch in Österreich häufiger gesehen. Aber das Jahr endete mit einer guten Nachricht: eine internationale Razzia konnte Personen, die als das Netzwerk hinter Emotet vermutet wurden, verhaften.

Die Freude währte aber nicht lange, denn 2021 war die Pandemie zwar nicht vorbei, aber dafür der Rest an Zurückhaltung, der 2020 vielleicht noch vorhanden war. So war 2021 in den Medien oft zu lesen, dass große österreichische Unternehmen durch Ransomwareangriffe betroffen oder sogar lahmgelegt wurden. Palfinger, Salzburg Milch und die Sattler Gruppe waren prominente Beispiele dafür, dass Österreich keine Cyberinsel ist, die von Angriffen verschont wird.

Damit setzte sich mehr und mehr die Erkenntnis durch, dass es jeden treffen könnte – eine Aussage, die seit Beginn der Cybersecurity-Awarenesskampagnen fixer Bestandteil jeder Präsentation ist, aber deshalb nicht unbedingt ernst genommen wurde. Immer mehr auch große Unternehmen stellten fest, dass sie nicht genug Personal und Fachwissen hatten, um im Fall des Falles alleine auf einen solchen Angriff reagieren zu können. Deshalb wurden Unternehmen, Interessensvertretungen und Kammern aktiv und suchten Antworten von staatlicher Seite, wie mit der Situation umgegangen werden sollte. Die Empfehlung, die von allen Seiten kam – auch von Seite von CERT.at – war: suchen Sie sich jetzt einen Dienstleister oder jede andere Art der Unterstützung, noch bevor ein Angriff stattfindet.

Die Erkenntnis aus dieser Zeit war, dass zwar viele einzelne Organisationen existieren, sowohl von staatlicher als auch von privater Seite, die eine Rolle in der Cyberangriffsbehandlung spielen. Aber keine davon hat ausreichend Personal, um einzelnen Organisationen über mehrere Wochen helfen zu können, damit diese sich von einem Ransomwareangriff erholen. Das reduziert nicht ihre Rolle oder ihren Nutzen, denn im Falle eines Angriffs wird Information zur wichtigsten Maßnahme (gibt es einen Decryptor, wer kennt Organisationen und Personen, die diese Art von Angriff bewältigt haben, etc.). Aber die besten Information nützt nichts, wenn niemand da ist, um sie umzusetzen.

In diesem Sinne war 2021 ein wichtiger Wendepunkt im Verständnis, wie Österreich auf Cyberangriffe vorbereitet ist und wo Handlungsbedarf besteht. CERT.at, als nationales Computernotfallteam, hat in diesem Jahr vor allem seine Rolle als Informationsdrehscheibe stark ausgebaut. Die Philosophie dahinter ist, dass wir besser helfen können, wenn wir möglichst viele Organisationen darüber informieren, was bei aktuellen Cyberangriffen gerade passiert und wovor sie sich dementsprechend schützen sollten. Das erfordert ein Team, das täglich analysiert, informiert und dokumentiert und das nicht müde wird, die Digitalisierung vor Angriffen schützen zu wollen. Und wir denken, dass uns das auch 2021 gelungen ist.

In diesem Sinne wünsche ich Ihnen viel Vergnügen bei der Lektüre des Jahresberichtes 2021!

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 CERT 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 NetzbetreiberInnen 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 14 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 2021:

- Erich Albrechtowitz (BKA)
- DI Philipp Blauensteiner (BVT)
- Christina Buttinger (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 **N**etwork and **I**nformation **S**ystems”. 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 der OpKoord[1] und IKDOK und die Teilnahme an Expert:innenworkshops, Trainings und sonstigen einschlägigen Fach- und Netzwerkveranstaltungen.

Der initiale Vertrag zwischen dem BKA und nic.at von 2007 war auf Grund der noch unklaren Aufgabenabgrenzung und der sich entwickelnden Materie noch sehr generisch gehalten, um in der Aufbauphase die nötige Flexibilität zu gewährleisten. Mit der ersten ÖSCS von 2013 und erst recht durch das NIS Gesetz von 2018 entstanden klare Vorgaben, welche Rolle das GovCERT in der nationalen Struktur der Cybersicherheit spielen soll. Das Bundeskanzleramt hat das zum Anlass genommen, Anfang 2020 die Dienstleistung ”Operative Unterstützungsleistungen für das GovCERT” (L-720574-9c20) in einem Vergabeverfahren neu auszuschreiben. Dieser Prozess führte dazu, dass mit 1. Jänner 2021 die Zusammenarbeit von BKA und nic.at auf eine neue, den aktuellen Herausforderungen angepasste Basis gestellt wurde.

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:

[1] Operative Koordinierungsstrukturen im Cybersicherheitsfall. Siehe auch Kapitel 5 Rechtsgrundlage

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 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 fehlkonfigurierte Server. Dazu stützen sich CERT.at und GovCERT Austria neben selbst entwickelter Sensorik auf Quellen[2] innerhalb der internationalen Gemeinschaft derIT-Sicherheitsbranche. Ziel ist es, das Niveau der Netzwerksicherheit in Österreich durch die Übermittlung von Informationen über Sicherheitsprobleme an Betroffene laufend zu heben.

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

Vernetzung: Neben der reinen technischen Rolle der CERTs als Informationsdrehscheibe und Hilfe bei Vorfällen fungieren sie auch als Kristallisationspunkt für die Vernetzung der in diesem Bereich arbeitenden Fachleute. Das reicht von selbst organisierten Foren wie dem Austrian Trust Circle oder dem IT Security Stammtisch, der aktiven Teilnahme an anderen Events der IT Security Community bis hin zur Mitarbeit bei Forschungsprojekten.

1.4 Zertifizierungen 2021

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

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

Ansporn für die Sicherstellung der eigenen Sicherheit nach innen. Jährliche Audits bei CERT.at stellen sicher, dass dieser Standard auch gehalten wird.

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. 2021 wurden weitere Maßnahmen gesetzt, um das Sicherheitsniveau auch künftig zu erhalten.

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 2021) eines von neun 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.

Kapitel 2

Das IT-Sicherheitsjahr 2021

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 Domain .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

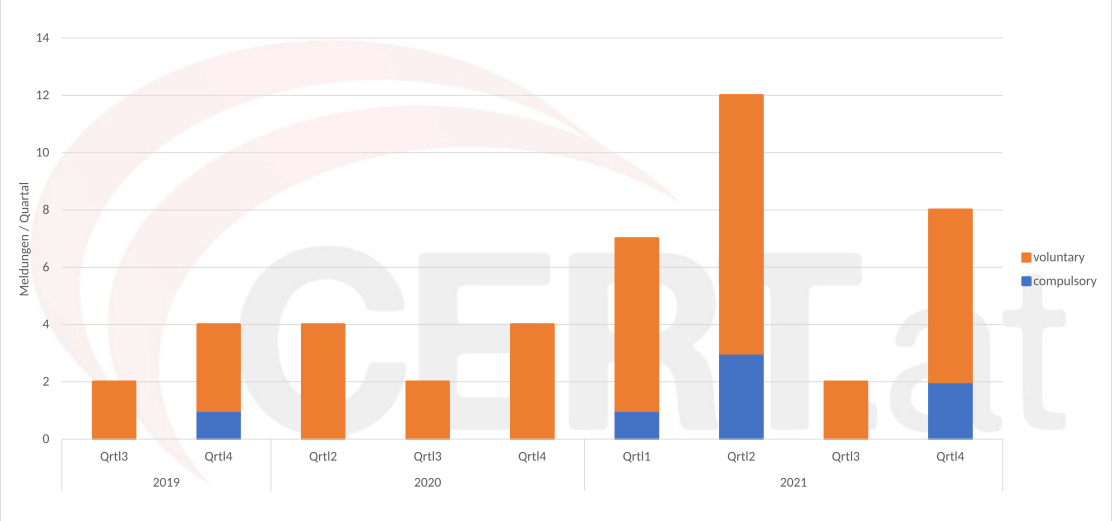


Abbildung 2.1: NIS Meldungen 2019 - 2021: Meldungsart

an das Innenministerium weiterleiten.

Die Zahl der Meldungen liegt unter den Erwartungen, insbesonders bei den freiwilligen Meldungen bestand die Hoffnung, dass diese die Grundlage für das nationale Lagebild zur Cybersicherheit in Österreich bilden werden. Mit in Summe 29 Meldungen in 2021 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.

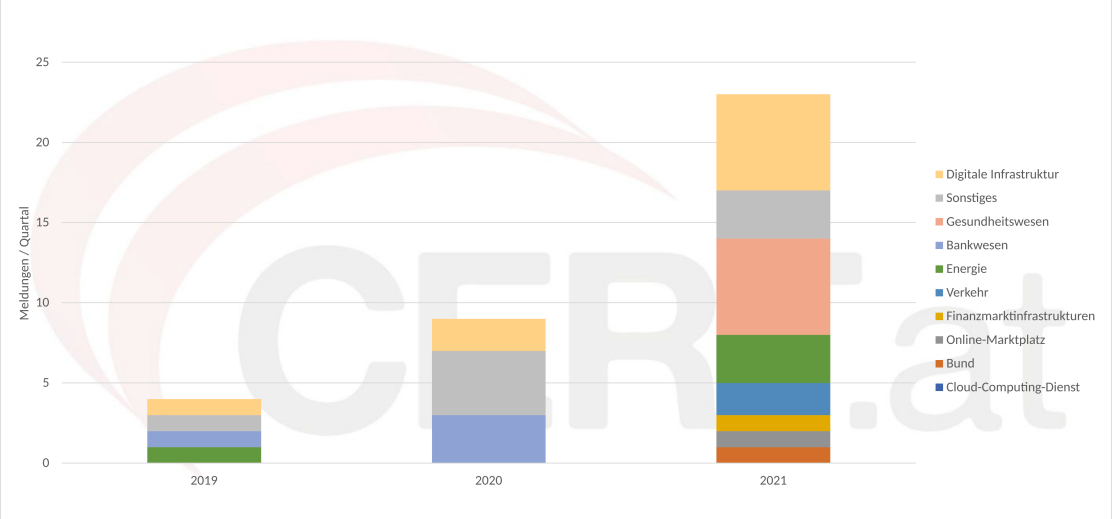


Abbildung 2.2: NIS Meldungen 2019 - 2021: Sektorenverteilung

2.2 Incident Reports, Incidents und Investigations

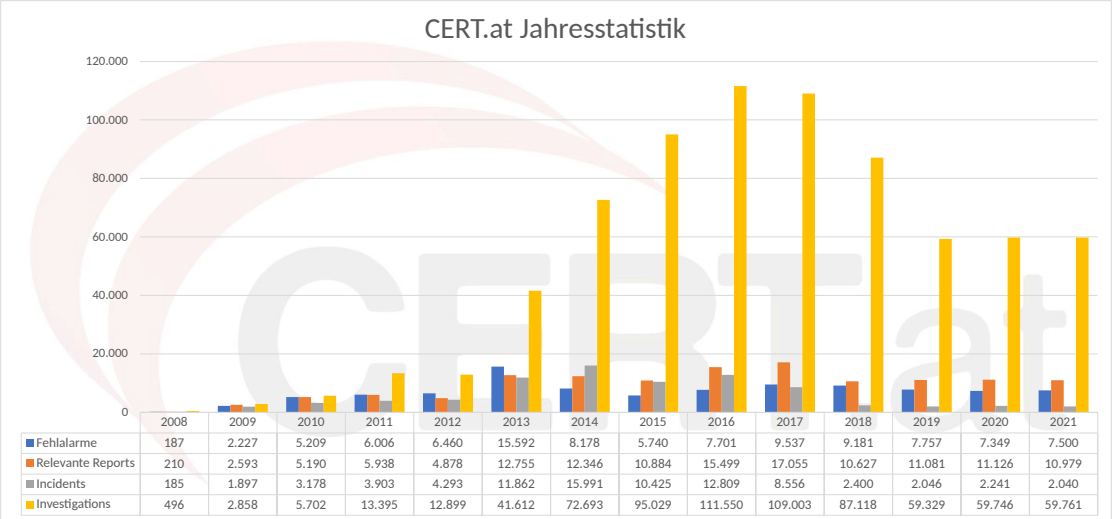
Eingehende und ausgehende Informationen werden bei CERT.at und GovCERT Austria über ein Ticketsystem (aktuell Request Tracker for Incident Response a.k.a. RTIR) abgehandelt. Dabei wird bei Vorfällen zwischen Incident Reports, Incidents und Investigations unterschieden:

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.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Fehlalarme	187	2.227	5.209	6.006	6.460	15.592	8.178	5.740	7.701	9.537	9.181	7.757	7.349	7.500
Relevante Reports	210	2.593	5.190	5.938	4.878	12.755	12.346	10.884	15.499	17.055	10.627	11.081	11.126	10.979
Incidents	185	1.897	3.178	3.903	4.293	11.862	15.991	10.425	12.809	8.556	2.400	2.046	2.241	2.040
Investigations	496	2.858	5.702	13.395	12.899	41.612	72.693	95.029	111.550	109.003	87.118	59.329	59.746	59.761

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

[1] Unsere 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.

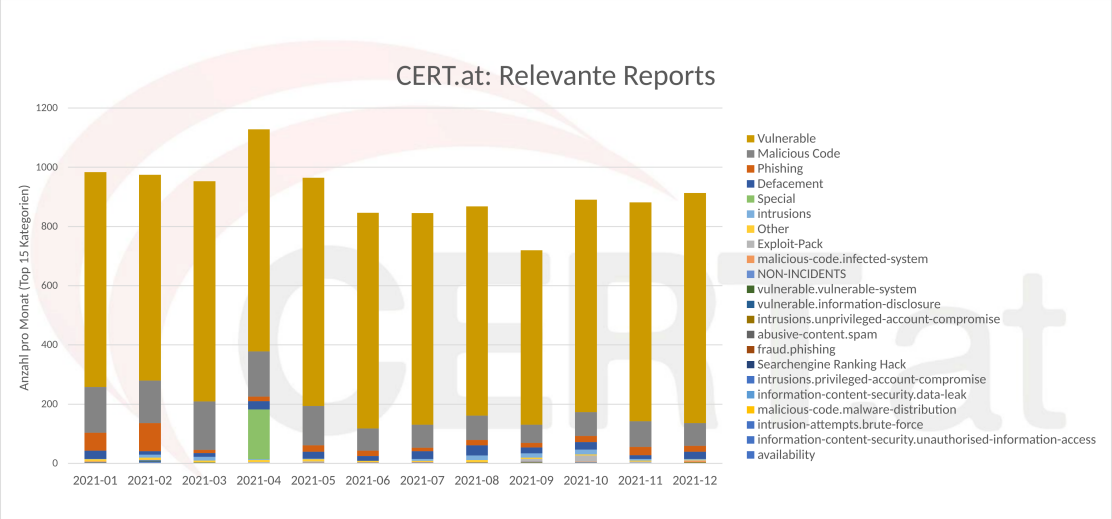


Abbildung 2.4: Incident Reports

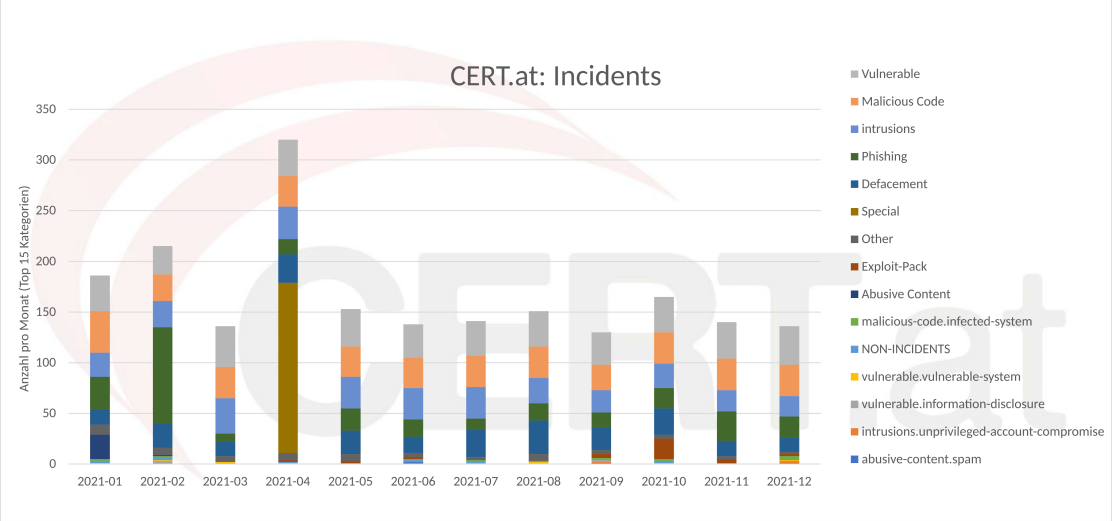


Abbildung 2.5: Incidents

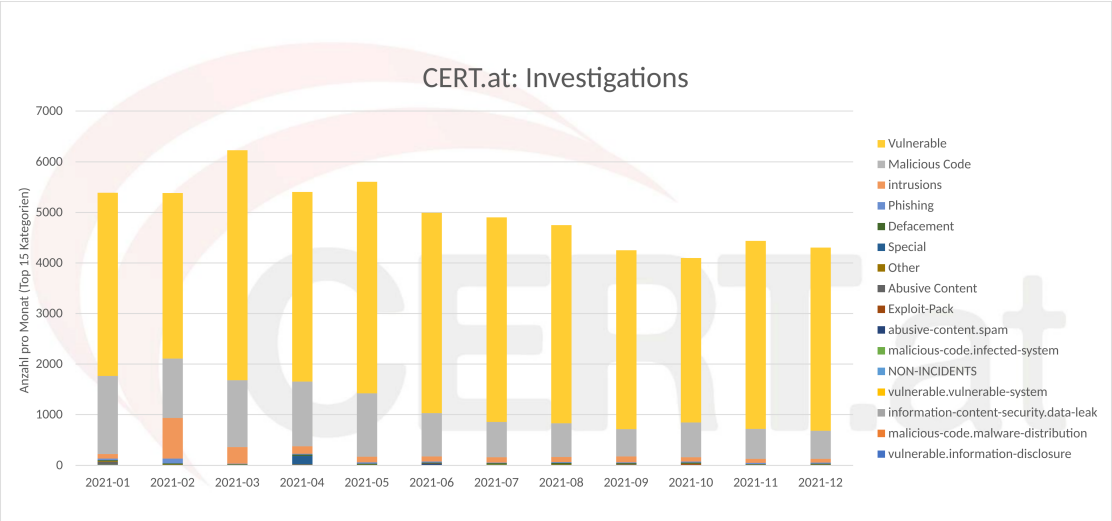


Abbildung 2.6: Investigations

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 Passwörter oder das Ausnützen (un)bekannter Schwachstellen.

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

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

Information Content Security: Hierunter fallen nicht authorisierte Zugriffe und Änderungen an Daten sowie Datenverlust. Wiederum gibt es unterschiedlichste Wege, wie so etwas

zustande kommt, unter anderem durch gestohlene Zugangsdaten, fehlende Zugriffsbeschränkungen, kaputte Hardware, etc.

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

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

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

Test: Für Testfälle.

2.4 2021 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.

[2] Für eine genauere Beschreibung siehe 2.5 Datenbasis.

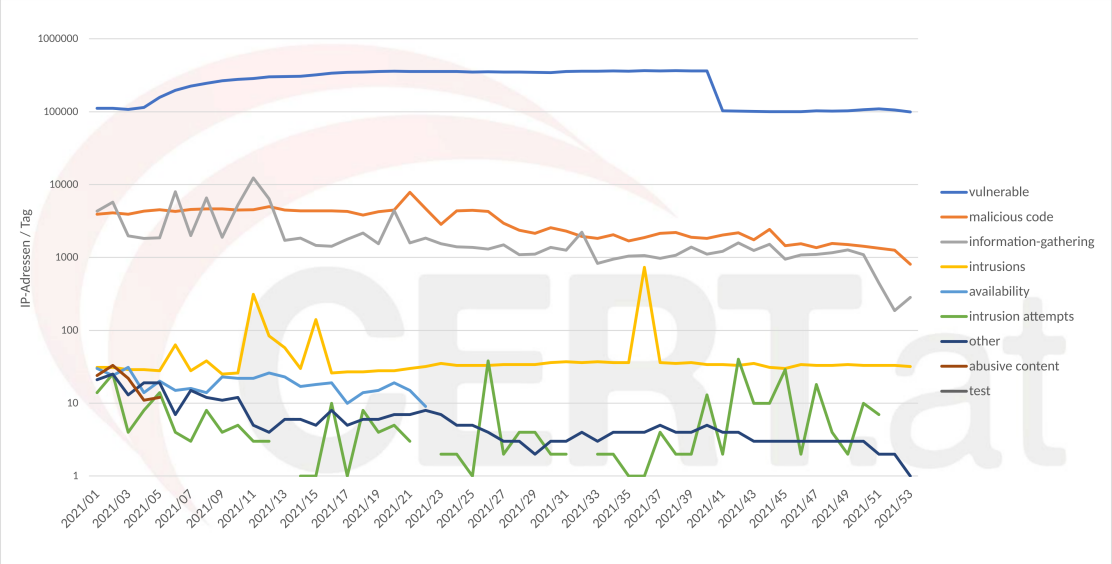


Abbildung 2.7: Events nach Taxonomie (logarithmische Skala)

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. Der Effekt ist bei Abbildung 2.8 besonders ausgeprägt. Man kann gut erkennen, dass "`open-cwmp`"[3] sowohl in der Unterkategorie "potentially-unwanted-accessible-system" als auch unter "info-disclosure" fällt.

2.4.1 Taxonomie "vulnerable"

Im Bereich der missbrauchbaren ("vulnerable") services sticht ein temporärer, aber massiver (rund 140.000 IP-Adressen) Anstieg zwischen Februar und September heraus. Es handelte sich dabei um Kabel/DSL Modems, die von einem Provider an seine Kunden verteilt wurden. Bei diesen war der Port des Management-Interfaces CWMP/TR-69 von außen aus erreichbar. Ein direkter Missbrauch war – dank eines gesetzten Passworts – nicht möglich, die Erfahrung hat aber gezeigt, dass diese Schnittstellen besser nicht offen aus dem Internet erreichbar sein sollten. (Abb. 2.8)

[3] Für mehr Informationen siehe https://cert.at/de/services/daten-feeds/vulnerable/#open-cwmp

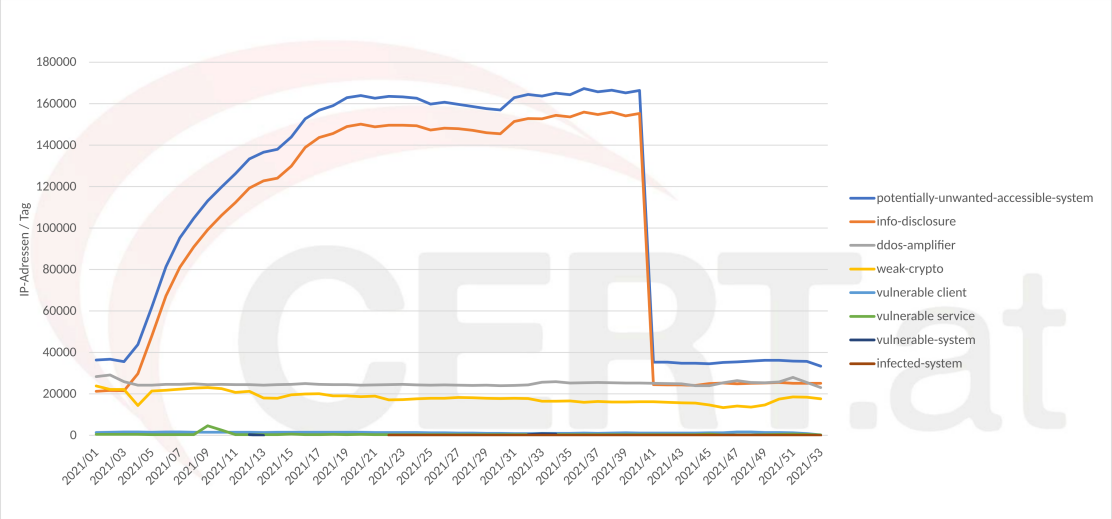


Abbildung 2.8: Alle Events der Taxonomie “vulnerable”

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

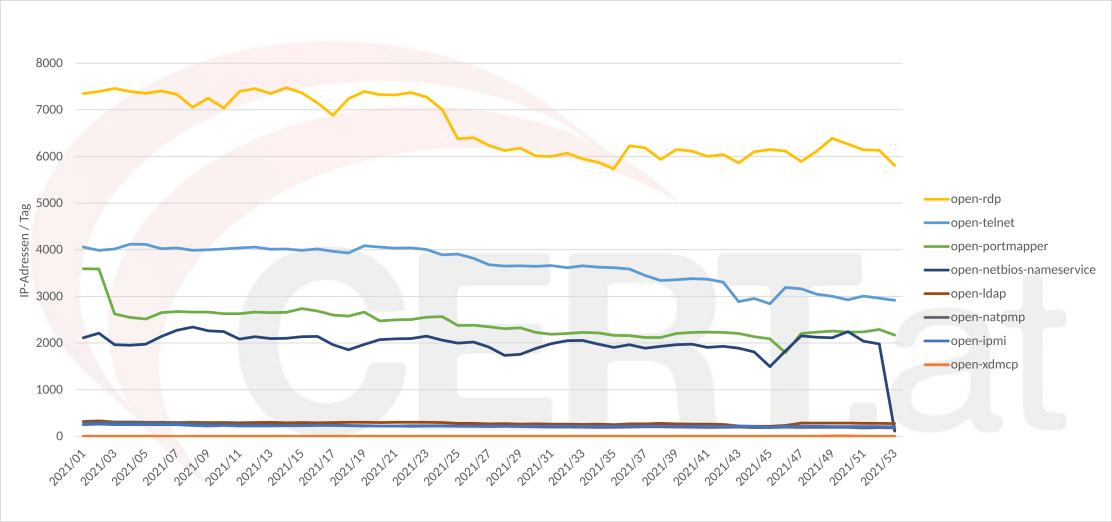


Abbildung 2.9: Ports, die nicht öffentlich erreichbar sein sollten

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

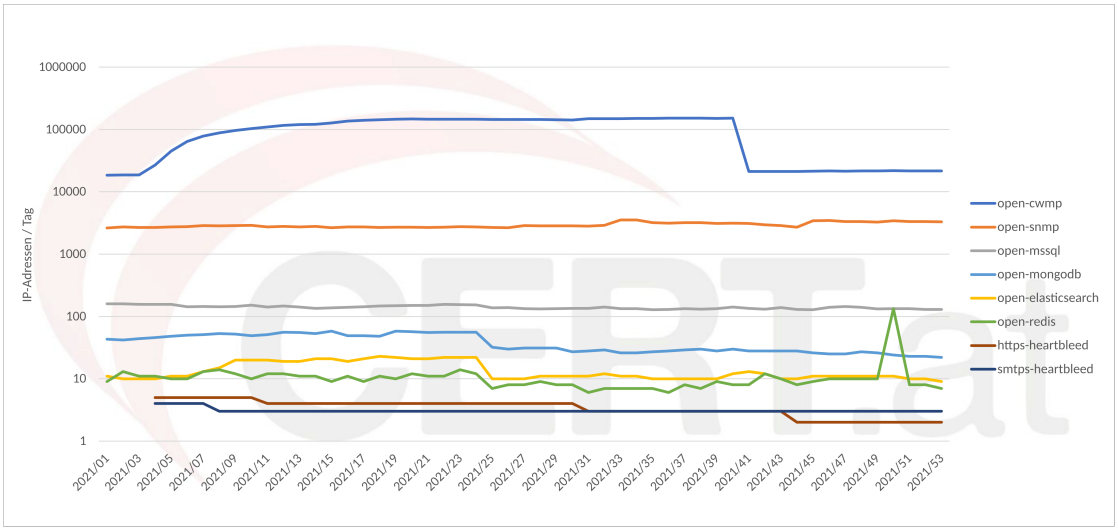


Abbildung 2.10: Services, über die sensible Informationen gewonnen werden können

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

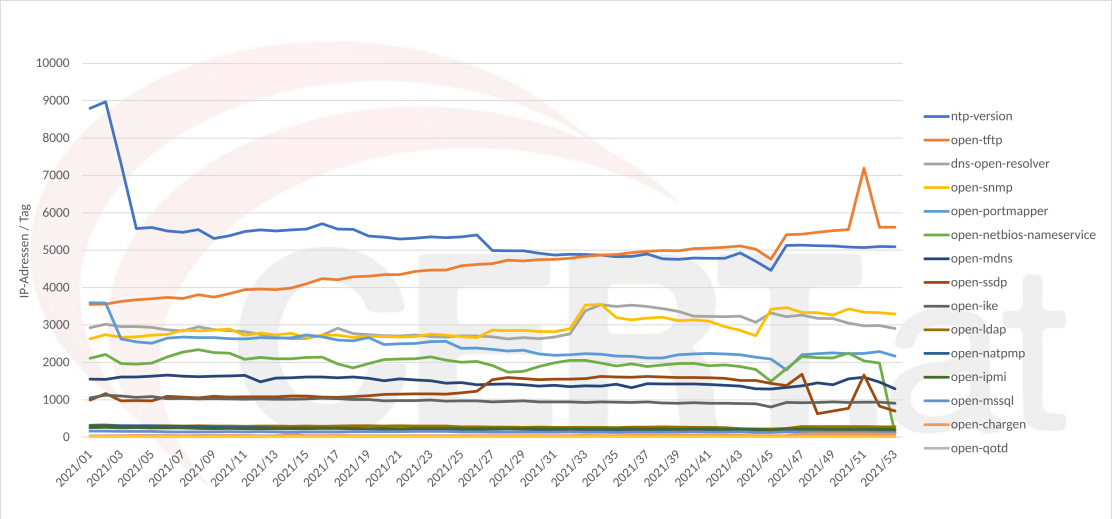


Abbildung 2.11: Geräte, die für UDP DDoS Amplifikation missbraucht werden können

Wie auch in den Jahren zuvor, fiel 2021 der größte Teil der von uns behandelten Meldungen in die Kategorie “vulnerable”, weshalb wir sie etwas näher vorstellen.

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

Default Konfigurationen: Vielfach ist es die voreingestellte Konfiguration von Software und

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

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

Risikoeinschätzung: Im Gegensatz zu Geräten, die mit Malware befallen sind, stufen viele die mit "potentiell verwundbaren" Computern verbundenen Gefahren als eher gering ein, v.a. wenn es sich z.B. um DDoS Amplifikatoren handelt – hier wird zwar das betroffene Gerät für einen Angriff missbraucht, der Schaden entsteht aber nicht bei 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.[4] 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

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

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 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.

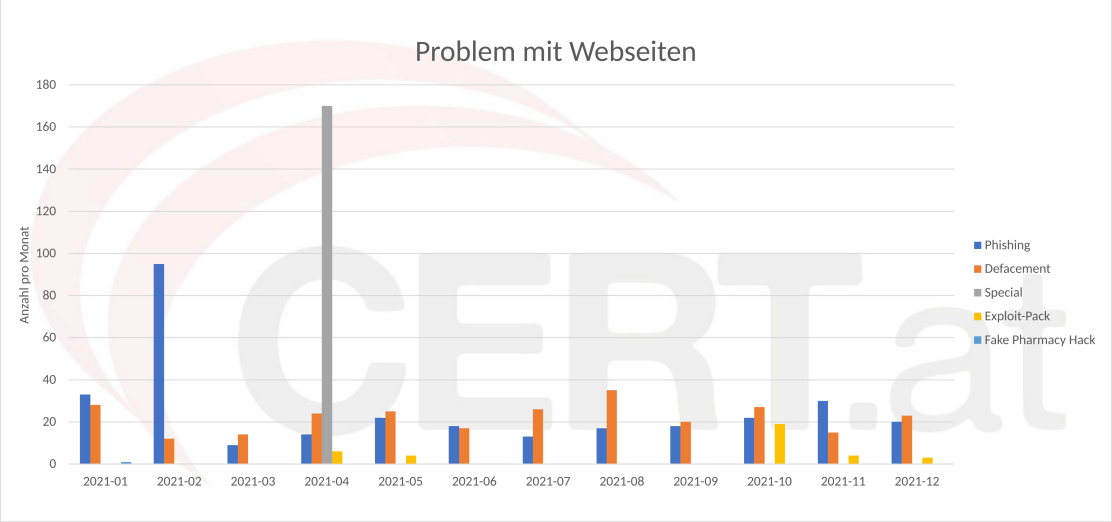


Abbildung 2.12: Probleme mit Webservern

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 “Hacktivisten” 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.

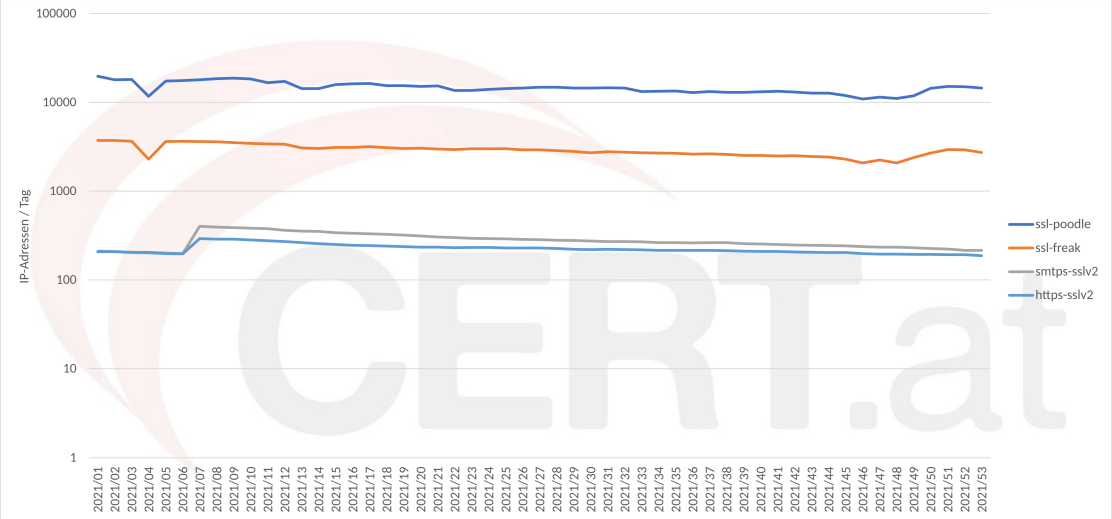


Abbildung 2.13: Unsichere Kryptographie

2.4.4 Malware

Im Jahr 2021 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 2021 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. Mit FluBot kam es 2021 zu einer Welle an Infektion von Android Handys. Interessant war hier, dass die Weiterverbreitung nicht über Schwachstellen, sondern rein über Massen-SMS und Social Engineering implementiert war. Der Schaden durch Onlinebanking-Fraud, was die eigentliche Funktionalität darstellte, hielt sich in Grenzen, während der Massenversand internationaler SMS massive Kosten für die Besitzer der infizierten Geräte verursachte. Die Netzbetreiber mussten eingreifen, um Schaden von ihren Kunden abzuhalten und die eigene Netzintegrität sicherzustellen.

2.5 Datenbasis

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

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

2.5.1 Eigene Erhebungen

Scanning Tools

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

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

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

Der Ablauf eines Scans stellt sich gewöhnlich folgendermaßen dar:

1. Aktuelle IP-Ranges/.at-Domains holen
2. Versuch eines initialen TCP Handshakes mit jedem so identifizierten Server auf dem/den Port(s) für den jeweiligen Scan.
3. Abspeichern, welche Handshakes erfolgreich waren, da dies auf eine mögliche Schwachstelle bzw. Infektion hinweist.
4. Verifikation der Schwachstelle,[5] 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.

2021 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

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

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. Laut unseren Scans (siehe Abb. 2.14) gab es Ende 2021 immer noch 34 (https) bzw. 10 (smtp) server unter der ccTLD .at, die immer noch verwundbar sind.

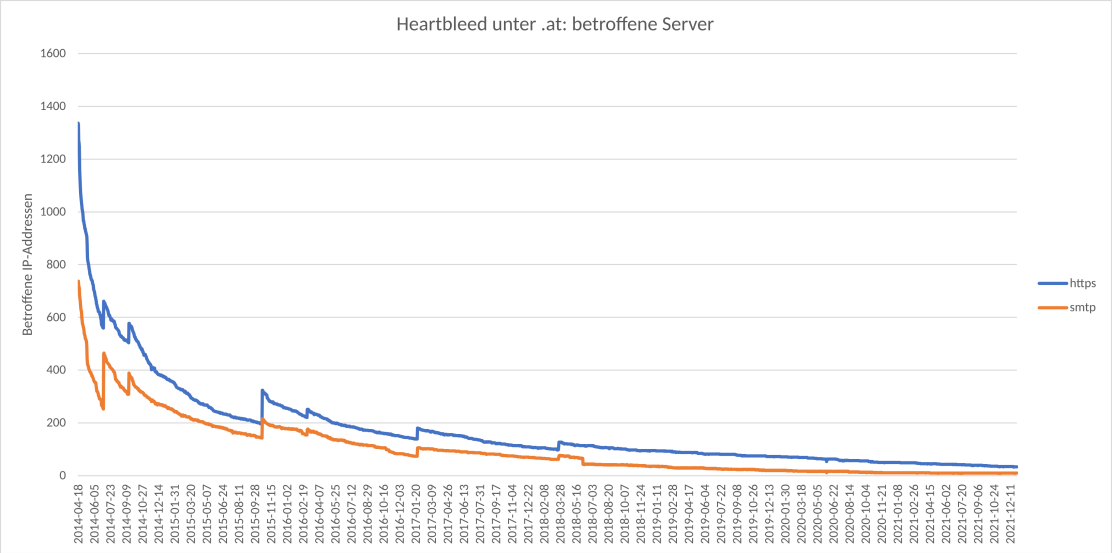


Abbildung 2.14: Status Heartbleed unter .at

CVE-2021-41773 ist eine schwere Sicherheitslücke im Apache Webserver, welche ausschließlich Version 2.4.49 betrifft. Dabei handelt es sich im Wesentlichen um eine Path-Traversal Schwachstelle, d.h. Angreifer:innen können dadurch auf Dateien außerhalb des Web-Root Verzeichnisses des Webservers zugreifen. Allerdings wurden innerhalb kurzer Zeit Exploits veröffentlicht, mit deren Hilfe die Lücke zu einer Remote Code Execution (RCE) ausgebaut werden kann, d.h. bei Angriffen können beliebige Befehle mit den Rechten des Dienstes ausgeführt werden.

CVE-2021-26855 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 ermöglich, ohne jegliche Authentifizierung beliebige Befehle als “NT Authority\System” über das Netzwerk auszuführen. Innerhalb weniger Tage wurde über Internet-weite Scans nach verwundbaren Servern berichtet. CERT.at sucht via Shodan nach potentiell

verwundbaren Installationen in Österreich und verifiziert die Ergebnisse mit Hilfe der Logik eines nmap NSE-Scripts eines Researchers. Zusätzlich haben wir alle Geräte, die uns im Zuge der Scans zu CVE-2021-26855 als Exchange Server gemeldet wurden, miteinbezogen.

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 allem im Bereich Analyse von Botnetzen und Malware arbeitet. Dazu wurde ein riesiges Netzwerk aus Honeypots[6] aufgebaut. Die Erkenntnisse daraus liefern wertvolle Analysedaten, um beispielsweise Botnetzen auf die Spur zu kommen und sie auszuschalten.

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 Disclosures[7] über uns ab.

Andere CERTs/CSIRTs

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

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

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

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 verteil über mehrere Länder und daher werden die so erfassten Daten – sofern es der rechtliche Rahmen erlaubt – an die zuständigen nationale CERTs/CSIRTs weitergeleitet, die diese dann wiederum im eigenen Land an die Betroffenen weitergeben können.

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

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

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

2.6 Tooling

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

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

2.6.1 IntelMQ

Das Projekt

Gestartet wurde der Entwicklungsprozess von IntelMQ[8] 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 verabeiten, erleichtert die Arbeit von CERTs/CSIRTs enorm. Bei CERT.at werden Dank IntelMQ täglich hunderte E-Mails verschickt, die BetreiberInnen von Internet-Diensten in Österreich auf Probleme in ihren Netzen hinweisen.

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

IntelMQ 2021

Im Jahr 2021 wurde IntelMQ 3.0.0 veröffentlicht. Diese Version hat einige interne Veränderungen und Verbesserungen gebracht. Das war der grösste Feature Release in diesem Jahr, danach folgten nur kleinere Bugfixes. Die Highlights der Version 3.0.0 sind:

- Bots werden jetzt dynamisch erfasst, wodurch das Einfügen neuer Bots erleichtert wurde
- In Konfigurationsfiles wurde JSON durch YAML ersetzt, um sie leichter les- und schreibbarer zu machen
- Das ”Data Harmonization Format” wurde in ”IntelMQ Data Format” umbenannt
- Das Parameter Handling einiger Bots wurde tiefgreifenden Veränderungen unterzogen

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

Eine Übersicht zu den Releases findet sich ebenfalls auf 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.

2021 wurde diese Funktion 73 Mal genutzt, unter anderem in folgenden Fällen:

- Um Betroffene von Schwachstellen in Microsoft Exchange und Exim4 zu informieren
- Mehrfach, um Ziele von Emotet zu warnen

2.6.2 MISP

MISP[9] 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.[10]

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.

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

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

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

2.7 Bedrohungen 2021

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. 2021 fielen darunter mehrere kritische Sicherheitslücken in Microsoft Exchange, und die als "Log4j / Log4Shell" benannten Schwachstellen in einer beliebten und weit verbreiteten Java-Bibliothek. Auch Angriffe mit Ransomware gingen leider nicht zurück, wohingegen koordinierte Strafverfolgungsmaßnahmen gegen die Schadsoftware-Familie Emotet zumindest einige Monate lang Wirkung zeigten.

2.7.1 Ransomware

Eine bemerkenswerte Entwicklung, die sich durch das vergangene Jahr hinweg kontinuierlich beobachten ließ, war die Professionalisierung von Ransomware-Banden. Der Trend geht immer mehr weg von einzelnen Täter:innen, hin zu gut organisierten und hochgradig spezialisierten kriminellen Organisationen, die als "Ransomware-as-a-Service" (RaaS) bezeichnet werden. Diese Gruppen bieten Ransomware als Dienstleistung an, bei der andere Kriminelle die Malware gegen eine Gebühr nutzen können, ohne selbst über detailliertes technisches Wissen oder Fähigkeiten zu verfügen. Dies hat zu einer erneuten Zunahme von Ransomware-Angriffen geführt, da die Barrieren für die Durchführung solcher Angriffe immer niedriger werden.

Leider haben auch die Angriffe dieser Art gegen Unternehmen und Organisationen im Bereich kritischer Infrastruktur, wie Energieversorgungen und Gesundheitswesen zugenommen. International konnten auch vermehrte Angriffe auf Behörden und Regierungsorganisationen verzeichnet werden. Österreich ist von dieser letzten Entwicklung bisher noch größtenteils verschont geblieben, es ist aber nicht davon auszugehen, dass wir hier als "Insel der Seligen" verbleiben werden.

Gleichzeitig haben Regierungen und Strafverfolgungsbehörden weltweit verstärkt Maßnahmen ergriffen, um Ransomware-Banden zu bekämpfen. Es gab intensivierte internationale Zusammenarbeit und koordinierte Aktionen zur Identifizierung und Strafverfolgung von Ransomware-Akteuren.

Nichtsdestotrotz bleibt Ransomware eine anhaltende Bedrohung, die nicht auf die leichte Schulter zu nehmen ist. In Anbetracht des potentiellen Schadens bei einem erfolgreichen Angriff gegen das eigene Netzwerk ist es nicht nur im philosophischen Sinn die richtige Entscheidung, Maßnahmen zur Stärkung der eigenen Sicherheit kontinuierlich voranzutreiben. Auch mit Hinblick auf den durch gestohlene Daten entstehenden Reputationsverlust und dessen wirtschaftliche Folgen sollten Unternehmen hier nicht unnötig sparen.

2.7.2 Emotet

Die Infrastruktur von Emotet, eine der anpassungsfähigsten Schadsoftware-Familien der letzten Jahre, wurde im Januar 2021 durch eine koordinierte Strafverfolgungsmaßnahme abgeschaltet, was in weiterer Folge zu einem merklichen Abfall im Infektionsgeschehen führte. Im November dieses Jahres kehrte Emotet jedoch zurück und entwickelt sich seitdem kontinuierlich weiter. Trotz dieser langen Pause verarbeitete CERT.at in diesem Jahr mehr als 8000 Meldungen über mögliche Infektionen und informierte die Betroffenen.

Erste Anzeichen für eine neuerliche Aktivität wurden von Sicherheitsforscher:innen am 14. November entdeckt, als eine Emotet-Binärdatei im Rahmen einer Trickbot-Infektion geliefert wurde. Schon kurz darauf wurden bereits große Mengen an bösartigen Nachrichten mit Emotet-Bezug vermeldet.

Die neue Emotet-Infrastruktur besteht aus zwei separaten Botnetzen, die als Epoche 4 und Epoche 5 bezeichnet (häufig abgekürzt als E4 und E5) werden. Initial enthielten die bösartigen Spam-Mails von Emotet eine von drei Arten von Anhängen: ein passwortgeschütztes ZIP-Archiv, ein Word-Dokument oder eine Excel-Tabelle. Dies entspricht der gleichen Methode, die bei früheren Emotet-Infektionen gesehen wurden. Im Laufe des Monats wurde dem Infektionsprozess eine Batch-Datei hinzugefügt. Die Ziele dieser Angriffe umfassten unterschiedlichste Sektoren weltweit, jedoch waren die Vorlagen für die Office-Dokumente immer noch in englischer Sprache gehalten, selbst wenn die Opfer keine englischsprachigen Personen waren.

Im selben Monat wurde auch eine Änderung im Infektionsablauf vorgenommen: Das Aktivieren von Makros führte nicht mehr direkt zum Herunterladen und Ausführen der Emotet-DLL. Stattdessen ließ der Makrocode eine Batch-Datei fallen, die anschließend ausgeführt wurde. Als eine Ausweichmethode erzeugte ein verschleiertes Skript in der Batch-Datei einen PowerShell-Befehl, um eine Emotet-DLL abzurufen und sie auf dem Computersystem des Opfers auszuführen. Die Emotet-DLL war ähnlich den Emotet-DLLs vor der Abschaltung im Januar 2021.

Ende November änderte Emotet seine Strategie erneut und begann, den Microsoft App Installer als Teil seiner Infektionskette zu nutzen. Dieser Schritt ermöglichte es Emotet, die Schadsoftware durch eine vermeintlich legitime Anwendung zu verbreiten und so die Entdeckung durch Sicherheitslösungen zu erschweren. Ab Dezember wurde Cobalt Strike auf Emotet-infizierten Windows-Hosts bereitgestellt, und mindestens eine weitere Welle von Emotet-E-Mails, die versuchten, das App Installer-Protokoll von Microsoft zu missbrauchen konnte beobachtet werden. Nachdem dies nicht den gewünschten Erfolg brauchte wechselten die Angreifer:innen jedoch schnell zu anderen Infektionsmustern und verwendete unterschiedliche Vorlagen für Office-Dokumente, hauptsächlich Excel-Tabellen. Nach dem 24. Dezember stellte Emotet das Versenden von Spam bis nach dem neuen Jahr ein.

Trotz der erfolgreichen Abschaltung im Januar 2021 und der anschließenden Pause hat Emotet seine Rückkehr geschafft und ist weiterhin eine ernstzunehmende Bedrohung. Die Entwickler:innen von Emotet haben ihre Taktik und Methoden angepasst, um ihre Schadsoftware effektiver zu verbreiten und Sicherheitsmechanismen zu umgehen. Es ist davon auszugehen, dass Emotet weiterhin neue Techniken entwickelt und seine Verbreitungsmethoden verändert, um die Wirksamkeit der Schadsoftware aufrechtzuerhalten und Gegenmassnahmen so effektiv wie möglich umgehen zu können. Die Zusammenarbeit von internationalen Strafverfolgungsbehörden und privaten Unternehmen bleibt entscheidend im Kampf gegen Emotet und andere Cyber-

bedrohungen. Unternehmen und Privatpersonen sollten darüber hinaus stets wachsam sein, ihre Systeme regelmäßig aktualisieren und sich über die neuesten Bedrohungen informieren, um sich bestmöglich vor Angriffen zu schützen.

2.7.3 Microsoft Exchange

Mit Proxylogon und Proxyshell wurden im März beziehungsweise August 2021 Sicherheitslücken in Microsofts E-Mail Server Exchange bekannt die weltweit für großes Aufsehen sorgten. Diese Sicherheitslücken wurden aktiv & großflächig ausgenutzt, und sorgten nicht nur bei den Betreiber:innen verwundbarer Exchange-Installationen für rauchende Köpfe. Die von kompromittierte Servern ausgehenden Folgeangriffe gegen Dritte, insbesondere durch Kampagnen mit Malspam, stellten Sicherheitsverantwortliche vor Herausforderungen.

In einigen Fällen konnten Angreifer:innen durch die Ausnutzung dieser Schwachstellen auf die E-Mail Infrastruktur einer Organisation zurückgreifen, und sich so in legitimate Kommunikationsverläufe schmuggeln, um ihre Schadsoftware zu verteilen oder betrügerische Handlungen zu setzen. Ein Vortäuschen bekannter Absender war so nicht mehr notwendig, Empfänger:innen währten sich in Sicherheit und konnten so einfacher zum Öffnen bösartiger Anhänge verleitet werden.

Als nationales CERT begegneten wir diesen Schwachstellen nicht nur durch die Veröffentlichung aufbereiteter Handlungsempfehlungen sowie aktuellen Lageinformationen, sondern auch durch zielgerichtete Information von Betreiber:innen von verwundbaren Exchange-Instanzen, um eine schnelle Behebung der Sicherheitslücke zu ermöglichen.

Betroffene Installationen in österreichischen Netzbereichen haben wir einerseits durch Netzwerkscans und andererseits anhand Informationen unseres internationalen Partnernetzwerks identifiziert.

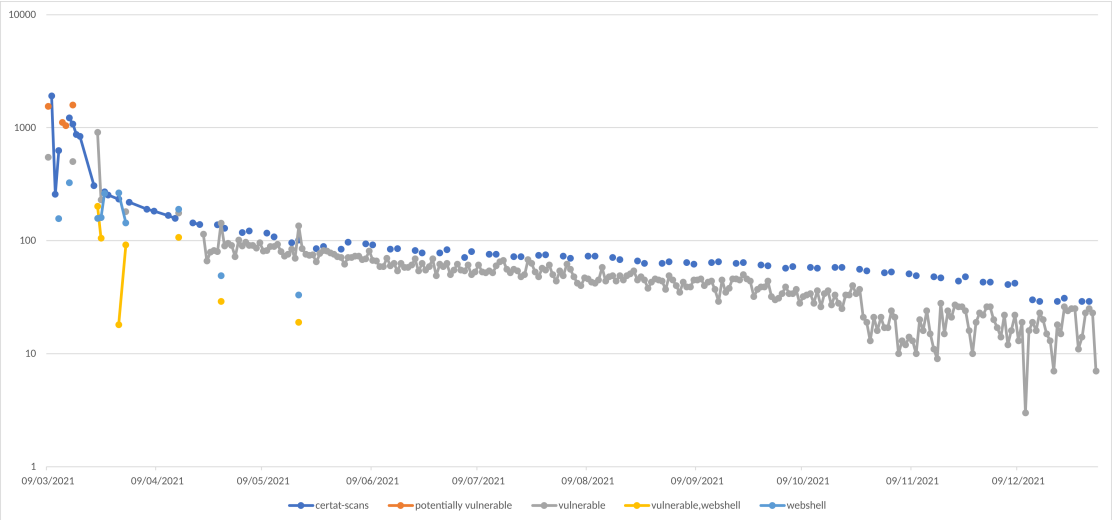


Abbildung 2.15: Datenbasis zu Proxylogon in Österreich: Verwundbare Systeme und erkannte Infektionen

2.7.4 Log4j

Gegen Ende des Jahres sorgte eine schwerwiegende Sicherheitslücke in einer verbreiteten Java-Bibliothek noch einmal für Aufruhr – Log4j. Dabei handelt es sich um ein Logging-Bibliothek, die in tausenden von Softwareprojekten eingebaut wurde, und daher – nicht immer bewusst – von vielen Unternehmen und Organisationen weltweit eingesetzt wird, um Protokolldaten in Anwendungen zu erfassen und zu verarbeiten. Die darin entdeckte Sicherheitslücke, die als Log4Shell oder CVE-2021-44228 bekannt wurde, ermöglicht es Angreifer:innen, schädlichen Code über speziell gestaltete Protokollnachrichten einzuführen und dadurch die betroffenen Systeme zu übernehmen.

Die vergleichsweise leichte Ausnutzbarkeit der Schwachstelle führte sehr schnell zu massiven Scans verschiedenster Akteure im Internet, von denen das Gros leider nicht nur nach der Präsenz der Lücke suchte, sondern diese dann bei Gelegenheit auch gleich nutzte um das verwundbare System zu kompromittieren.

Nach der Veröffentlichung reagierten die Entwickler:innen hinter Log4j relativ schnell mit der Bereitstellung von Sicherheitsaktualisierungen, um die Lücke zu beheben. Allerdings war das Einspielen dieser Updates keine triviale Angelegenheit, da die Bibliothek in vielen Anwendungen und Systemen verwendet wird. Das bedeutete, dass Aktualisierungen in diesem Fall umfassende Überprüfung und Aktualisierung in einer Vielzahl von Umgebungen und Anwendungen erforderte, was eine komplexe und zeitaufwändige Aufgabe war.

Durch eine enge Zusammenarbeit zwischen verschiedenen Akteuren, wie IT-Sicherheitsfirmen, Regierungsbehörden, CERTs (Computer Emergency Response Teams) und anderen Organisationen, konnten betroffene Unternehmen schnell über die Bedrohung informiert werden. Informationen über die Art des Angriffs, die Schwachstellen, betroffene Systeme oder mögliche Abwehrmaßnahmen wurden effizient und zeitnah geteilt, um den Unternehmen bei der Reaktion auf den Vorfall zu helfen.

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.

Aufgrund der Intensivität unseres Engagements seien hier unsere Aktivitäten rund um die DDoS-Angriffe im Sommer 2021 erwähnt. In den Monaten Mai und Juni kam es zu starken DDoS-Angriffen bei denen eine Gruppe, die sich ”Fancy Lazarus” nennt, unter Androhung von Folgeangriffen versuchte, Geld von den Betroffenen zu erpressen. Dieses Phänomen ist grundsätzlich nicht neu. Vergleichbare Angriffe gab es bereits 2020, durch einen Bedrohungsakteur mit ähnlichem Namen. Die Vorgehensweise der Täter:innen war immer gleich:

- Erpressung des potentiellen Angriffsziels per E-Mail, mit Ankündigung eines Demoangriffs

sowie einer Zahlungsfrist von 7 Tagen, bei Nichteinhaltung wurde mit schweren Angriffen gedroht.

- Kurs darauf folgte ein DDoS-Angriff mit einer Bandbreite zwischen 30 und 250Gbit/s, meistens gegen die autoritativen Nameserver des Opfers, der meist um die zwei Stunden anhielt
- Nach diesem ”Demoangriff” kam es in keinem einzigen uns bekanntem Fall zu weiteren Angriffen

Die Angreifer:innen setzten offensichtlich darauf, durch Aufbau einer Drohkulisse ausreichend Angst zu erzeugen, um Opfer zur Zahlung zu bewegen - mit der Hoffnung, dass genügend Unternehmen eingeschüchtert genug sind, um die Kampagne finanziell lohnenswert zu machen.

Es gelang uns relativ schnell, ausreichend Informationen von betroffenen Unternehmen zu sammeln, um ein schlüssiges Bild über die Art der Angriffe, technische Details und mögliche Abwehrmaßnahmen zu erhalten, welches in weiterer Folge an andere Organisationen verteilt werden konnte.

Darüber hinaus wurde die Koordination von Maßnahmen zur Abwehr des Angriffs unterstützt. Dies umfasste die Bereitstellung von Leitfäden, Handlungsempfehlungen und bewährten Vorgehensweisen, um betroffenen Unternehmen bei der Umsetzung von Sofortmaßnahmen zur Eindämmung der Bedrohung zu helfen. Auch der Austausch von Erfahrungen und Erkenntnissen zwischen betroffenen Unternehmen wurde gefördert, um voneinander zu lernen und die Reaktion auf den Vorfall zu verbessern.

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 fanden 2021 weder das jährliche Treffen aller teilnehmenden Organisationen noch die regelmässigen Treffen der einzelnen Sektoren statt. Die Aktivitäten haben sich stattdessen hauptsächlich auf die Mailinglisten verlagert.

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 2021 gab es insgesamt 6 Treffen, drei davon physisch, der Rest fand aufgrund der Pandemie virtuell statt. Mit Stand Ende 2021 nehmen 17 Teams am österreichischen CERT-Verbund teil. Genauere Informationen finden Sie auf onlinesicherheit.gv.at.

3.2.3 IKDOK/OpKoord

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

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

Der IKDOK besteht (Siehe §3(4) NISG) aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres. Bis Dezember 2021 hatte das Cyber Security Center im BVT die Aufgabe, die Koordinationsstrukturen zu leiten. Mit der Etablierung der Direktion für Staatsschutz und Nachrichtendienst (DSN) 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 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.

Neben anderer Task-Forces zu Spezialthemen, hat sich eine auf CERTs konzentrierte Plattform entwickelt. 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 (2021 war das leider nur ein mal physisch 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 Lösungen[1] und eine gemeinsame Taxonomie (siehe 2.3: Taxonomie) gesetzt. Im Rahmen des MeliCERTes 2 Projektes haben Mitarbeiter von CERT.at beim Design und Implementation der IT-Infrastruktur des CSIRTs Networks mitgewirkt.

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 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.

Das Netzwerk trifft sich zum einen bei der jährlichen internationalen Konferenz und zum ande-

[1] Konkret unter anderem MISP und IntelMQ.

ren bei zahlreichen themen- oder regionsspezifischen Treffen. Viele davon fanden 2021 pandemiebedingt virtuell statt.

Kapitel 4

Drittmittelprojekte

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

4.1 Connecting Europe Facilities (CEF)

4.1.1 Enhancing Cybersecurity in Austria (2018-AT-IA-0111)

CERT.at reichte im Jahr 2018 ein weiteres EU Projekt “Enhancing Cybersecurity in Austria” (2018-AT-IA-0111) im Rahmen des Connecting Europe Facilities (CEF) Programm ein, das in vollem Umfang genehmigt wurde und das eine 75%-ige Förderung der Projektkosten durch die Europäische Union ab September 2019 beinhaltete. Diese Projekt wurde mit Ende August 2021 erfolgreich abgeschlossen.

Das Projekt umfasste sowohl interne Weiterentwicklungen als auch Anpassungen an internationale Anforderungen im Rahmen der Zusammenarbeit der europäischen CERTs/CSIRTs. So ist die Integration und Einbindung in “MeliCERTes”, einem EU geförderten Projekt zur internationalen Kooperation der europäischen CERTs, ein wichtiger Teil des Projektes.

International Relations

Im Projekt wurden Kosten, die bei internationalen Treffen und Schulungen auflaufen, gefördert. 2021 war die Reisetätigkeit pandemiebedingt noch stark eingeschränkt, die meisten Meetings fanden noch virtuell statt.

Dazu gehörten das 62. TF-CSIRT Meeting im Jänner, ein IHAP Meeting im Februar, das CSIRTs Network (CNW) Meeting im März, das 63. TF-CSIRT Meeting im Mai, und das nächste CNW Meeting und die FIRST Conference und das dazugehörige Capture The Flag (CTF) Event im Juni. Bei letzterem belegte zwei unserer Mitarbeiter den 9. Platz von 42 Teams. Dazu gibt es auch ein längeres Writeup auf Englisch.

Die initial geplante Serie von Hackathons wurde auch virtuell abgehalten, wir fokussierten auf RTIR und IntelMQ für die Mitglieder im CSIRTs Network.

Trainings und Schulungen standen auch am Programm: TRANSITS I (Die TRANSITS-Trainings richten sich speziell an CERT/CSIRT MitarbeiterInnen und dienen dem Austausch und der Vernetzung in diesem Bereich), ein mal SANS SEC402: Cybersecurity Writing: Hack the Reader, ein mal Windows Host Security Training des InfoSec Institutes und ein mal CompTIA Network+ Fundamentals.

Da dieses Projekt mit Ende August 2021 auslief, war die Arbeit im zweiten Jahresdrittel 2021 auf den Projektabschluss und die dabei abzugebenden Berichte fokussiert.

OpenINTEL

Im Februar 2021 konnten wir gemeinsam mit der Nic.at Research & Development Abteilung das „OpenINTEL-lookup“ Subprojekt erfolgreich umsetzen und veröffentlichen.

Bei OpenINTEL handelt es sich um ein Forschungsprojekt der Universität Twente (Niederlande) in Zusammenarbeit mit SURFnet, SIDN Labs und NLnet Labs., das eine Plattform zur Messung des Zustands großer Teile des globalen DNS (Domain Name System) darstellt.

Da das DNS eine Schlüsselrolle bei nahezu allen Internetdiensten spielt, entsteht dadurch eine Aufzeichnung von Veränderungen im Internet über längere Zeiträume. Die Messungen werden täglich durchgeführt: Dabei wird ein großer Ausschnitt des DNS Systems abgefragt, und die entstehenden Antworten der DNS Server werden analysiert. Der große Vorteil ist vor allem der zeitliche Verlauf, der es ermöglicht, Änderungen auch historisch nachzuverfolgen – etwa dann, wenn neue Technologien umgesetzt werden oder sich Änderungen am DNS durchsetzen.

Unsere Research & Development Abteilung erhält von OpenINTEL täglich jene Daten, die unsere .at-Zone betreffen. Um diese Daten für die Aufgaben des nic.at-CERT direkt nutzbar zu machen, wurde von uns eine Web-Oberfläche erstellt, über die Suchabfragen erfolgen können.

Für die Machine-to-Machine-Kommunikation steht auch noch ein Application Programming Interface (API) zur Verfügung. Die entstandene Software wird nun als Open-Source zur Verfügung gestellt, damit auch andere Organisationen von dieser Entwicklung profitieren können.

IntelMQ

Anfang März veröffentlichten wir IntelMQ 2.3.0 inklusive dazugehöriger Tools wie dem IntelMQ Manager und der neuen IntelMQ API. Es war auch das erste Release mit einem Docker Image verfügbar auf Dockerhub unter certat/intelmq-full. Details zu allen Neuerungen finden Sie im

dazugehörigen Blogpost.

Im April wurde mit IntelMQ 2.3.2 das letzte Maintenance Release für das erste Drittel 2021 veröffentlicht, welches Bugfixes sowie Verbessungen für Shadowserver and Shodan enthielt. Am 2. Juli wurde mit IntelMQ 3.0.0 eine rundum überarbeitete Version von IntelMQ veröffentlicht und damit auch ein wesentlicher Milestone für das Projekt erreicht. Einen Überblick zu den Änderungen und Umbauten findet man auf unserem Blog.

tag2domain

Im April 2021 gab es einige Neuerungen bei tag2domain im Zusammenhang mit flexibleren Taxonomien. Ausführliche Beschreibungen finden sich in unserem Blog Post.

Constituency-Portal NG („tuency“)

Neben IntelMQ 3.0 wurde zeitgleich die erste stabile Version von ”Tuency”, unserem neuen “Constituency-Portal”, veröffentlicht. Das Portal ist ein Kontaktmanagementtool mit Self-Service Funktionen und verwendet als Authentifizerungslösung Keycloak. Dadurch können die dort hinterlegten Zugangsdaten auch bei anderen, zukünftigen Diensten verwendet werden.

Das Portal verbessert und erweitert außerdem die Adressierung unserer täglichen Benachrichtigungen an Netzbetreiber:innen über Probleme in deren Netzen, die wir via IntelMQ ausschicken. Eine genauere Beschreibung der Funktionen finden Sie in unserem Blogpost dazu. Der Source-Code von Tuency ist öffentlich auf GitLab einsehbar.

Vor der Veröffentlichung wurde ein Pentest durch Externe durchgeführt, der kleine Verbesserungsmöglichkeiten fand, insgesamt aber das sichere Design und die robuste Ausführung des Projekts bestätigte. Außerdem haben wir im zweiten Jahresdrittel umgesetzt, dass unsere öffentlichen Datenfeeds via IntelMQ in unser SIEM eingespeist werden. Entsprechend ist es jetzt möglich, dessen Logs mit den Feeds zu korrelieren und effizienter auf Probleme zu reagieren.

MeliCERTes

Ebenfalls abschließen konnten wir die Integration der MeliCERTes Plattform, unter anderem durch die Installation von Cerebrate. Für die erfolgreiche Umsetzung war es notwendig, im IT Betrieb technische Grundlagen und Kompetenzen zu schaffen und auszubauen.

4.1.2 CyberExchange (2017-EU-IA-0118)

Das von der europäischen Kommission unterstützte CyberExchange Projekt ist ein Erasmus-Äquivalent für nationale CERTs/CSIRTs der EU. Mitarbeiter:innen können für drei Tage bis zu zwei Wochen in einem anderen CERT/CSIRT arbeiten und so die Vernetzung innerhalb der Community verbessern sowie das Teilen von Know-How vereinfachen.

Dabei sind zwei Arten des Austausches möglich: Einmal in Form eines “Fellowships” bei dem eine Mitarbeiterin oder ein Mitarbeiter zu einem anderen CERT/CSIRT geschickt wird, um dort neue Fähigkeiten zu lernen und diese dann nach der Rückkehr auch zu Hause zu verbreiten.

Andererseits sind auch sog. “Technical Assistance Visits” möglich, bei denen eine Person zu einem anderen CERT/CSIRT reist, um dort Wissen zu einem oder mehreren Tools zu vermitteln. CERT.at wirkt als sendende als auch empfangende Stelle an diesem Projekt mit.

Die Covid-19 Pandemie hat diese Projekt leider massiv getroffen und eingschränkt. Auf Grund der Reise- und Kontakteinschränkungen seit Beginn der Covid-19 Pandemie sind Reisen und Austauschbesuche mit anderen CERTs defacto unmöglich geworden – in der Hoffnung auf eine Besserung der Lage wurde das Projekt mehrmals verlängert. Leider hat sich bis Sommer 2021 keine Gelegenheit ergeben, weitere Besuche durchzuführen und wir sind daher mit Herbst 2021 final aus dem Projekt ausgeschieden.

4.1.3 AWAKE ”Cyber situational awareness for collaborative knowledge and joint preparedness” (2020-AT-IA-0254)

Seit September 2021 arbeiten wir gemeinsam mit dem Austrian Institute of Technology (AIT) als Koordinator, dem Bundesministerium für Inneres (BMI) sowie dem Bundeskanzleramt (BKA) an ”AWAKE” mit einem geplante Ende mit August 2024.

In diesem Projekt geht um das Thema Lagebild: wie kann man eine Einschätzung der aktuellen Sicherheitslage erstellen und wie kann man dieses am besten kommunizieren. Primär geht es hier um die drei Ebenen in der Cybersicherheitsstrategie der EU (technisch: CERTs, operativ: CyCLONe, strategisch), 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 (bis Dezember 2021 hatte das CSC im BVT diese Rolle, danach 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.

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 Wis-

sensstand 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.

Der Herbst 2021 war geprägt von ersten Analysen im Bereich von National Cyber Security Centre (NCSC) , CSIRT-Tools und -Taktiken sowie der bestehenden Forschung und der Erstellung von ersten Requirements für ein ”inter-organizational case management” in Form eines Cyber Common Operating Picture System (CYClOPS) sowie CCOP inquiries in Form eines Cyber Common Operating Picture Query (CCOP-Q).

4.1.4 JTAN ”Joint Threat Analysis Network” (2020-EU-IA-0260)

Das Joint Threat Analysis Network 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.

Eines der Projektziele des JTAN-Projekts besteht darin, ein Framework zu schaffen, dass einerseits eine Definition von „Risikofaktoren“ für Domains enthält sowie eine Methodik, um solche domain-basierten „Risikofaktoren“ über eine Reihe von Domains hinweg zu aggregieren.

Bei ersten Arbeiten der Nic.at R&D Abteilung zur Definition von „Risiko“ im Kontext eines Domainnamens haben wir festgestellt, dass diese Risiken mehrdimensional sind, verschiedene Einheiten betreffen sowie die Wahrscheinlichkeit verschiedener Schadensarten beschreiben können.

Dies kann beispielsweise ein „finanzielles Risiko“, ein „Reputationsrisiko“ oder auch ein „Informationsverlust“ sein und betrifft haupstsächlich Registrierungsstellen, Registrare, Inhaber von Domainnamen oder auch die Nutzer von Diensten.

4.2 “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.

Stand 2020 noch die Überprüfung bzw. Neuerhebung der Anforderung im Vordergrund, so ging es 2021 in Richung Umsetzung.

Im Bereich der ”local tools” war für CERT.at der Fokus auf der Pflege, Weiterentwicklung und dem Support von IntelMQ. Dazu wurde eine Serie von (online) Workshops abgehalten: ”IntelMQ - Introduction and Concepts” am 27. April 2021, ”IntelMQ - Hands-on Tutorial” am 25. Mai 2021 und 9. Dezember 2021 und ”IntelMQ - Integration and Output options” am 22. Juni 2021. In

einigen Fällen wurde auch direkte Hilfe per Email und Videokonferenz geleistet.

Das Design der Werkzeuge für die Zusammenarbeit im CSIRTs Network wurde parallel dazu weiter getrieben. Im Frühjahr 2021 ging es primär um die Auswahl eines passenden Produktes für das Identity and Access Management (IAM) im Netzwerk. Dazu wurden 12 Softwarepakete auf der Basis der Spezifikation verglichen, die Top 3 danach auch noch in einem Testsetup. Um das Ganze dann bei der ENISA zu installieren und Konfigurieren war es – laut ENISA Policy – nötig, für alle Open Source Komponenten Wartungsverträge aufzutreiben. Parallel dazu wurde von den Kollegen aus Luxemburg Cerebrate weiterentwickelt, das dann als Directory und Self-Service Portal für das CSIRTs Network agieren wird.

4.3 Mitarbeit an Forschungsprojekten

4.3.1 InduSec

Mit dem 31. August endete 2021 das Projekt InduSec der SBA Research, das seit 2019 ein Qualifizierungsnetzwerk für die Sicherheit von IT/OT Konvergenznetzen mit einer Serie an Schulungen betrieben hat. Abgeschlossen wurde diese mit einer größeren Übung, dem Besuch bei der Industrie 4.0 Pilotfabrik der TU Wien und einem Workshop zu Diversität.

4.3.2 SHIFT (KIRAS)

Das Austrian Energy CERT (AEC) nimmt am Projekt SHIFT teil, das wegen Verzögerungen im Konsortium erst 2022 starten wird. Es wird um sichere Simulationstechnologien für cyber-physische Systeme gehen.

4.3.3 CyberMonoLog (KIRAS)

Parallel zu SHIFT liefen 2021 auch die Vorarbeiten für ein weiteres KIRAS Projekt. In CyberMonoLog wird es ab Jänner 2022 dann um Empfehlungen für möglichst sinnvolles Looging aus dem Blickwinkel Sicherheit gehen.

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 (Netz- und Informationssystemsicherheitsgesetz, kurz: NISG).

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

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

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

5.1.1 Strategisches NIS-Büro

Das im Bundeskanzleramt angesiedelte Büro für strategische Netz- und Informationssystemsicherheit ("strategisches NIS-Büro") führte seine Arbeit im Jahr 2021 – trotz der schwierigen Umstände angesichts der COVID-19 Pandemie – erfolgreich fort. Auch konnten die Ermittlungen der Betreiber wesentlicher Dienste auf Grundlage der NIS-Verordnung abgeschlossen werden.

Im Hinblick auf die Vertretung Österreichs in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind, wurden umfangreiche Aktivitäten gesetzt. Den Schwerpunkt bildete dabei die Koordinierung und Vertretung der österreichischen Position in den Verhandlungen zur NIS-2-Richtlinie

5.1.2 Aktivitäten auf EU-Ebene

Im Dezember 2020 wurde von der Europäische Kommission ein Paket an Dokumenten veröffentlicht: die neue Cybersicherheitsstrategie, der Entwurf für die NIS-2-Richtlinie und der Entwurf für die Critical Entities Resilience (CER) Richtlinie. Schon im September wurde der Entwurf für die digitale operationale Resilienz im Finanzsektor (DORA) präsentiert.

Damit wurde 2021 zu einem Jahr der Verhandlungen zu EU Rechtsakten: Die im Rat dafür zuständige Horizontal Working Party on Cyber Issues (HWP Cyber) traf sich zu rekordverdächtigen 60 Sitzungen, und schaffte es, bis Ende 2021 eine abgestimmte Position zu der für CERT.at und GovCERT relevanten NIS-2 Richtlinie zu formulieren. Rechnet man ein Jahr für den Trilog zwischen Kommission, Rat und Parlament, dann kann man mit einer Verabschiedung von NIS-2 im Laufe von 2022 rechnen.

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