GovCERT Austria

CERT.at

BERICHT

INTERNET-SICHERHEIT

ÖSTERREICH 2019

Inhaltsverzeichnis

Impressum

Medieninhaber und Verleger: nic.at GmbH, Computer Emergency Response Team Austria, Karlsplatz 1/3, 1010 Wien. Diese Publikation wurde in Kooperation mit dem Bundeskanzleramt erstellt.

Projektleitung: Dimitri Robl, BA, CERT.at

Konzeption und Redaktion: CERT.at (Dimitri Robl, BA)

Herstellungsort: Wien, April 2019.

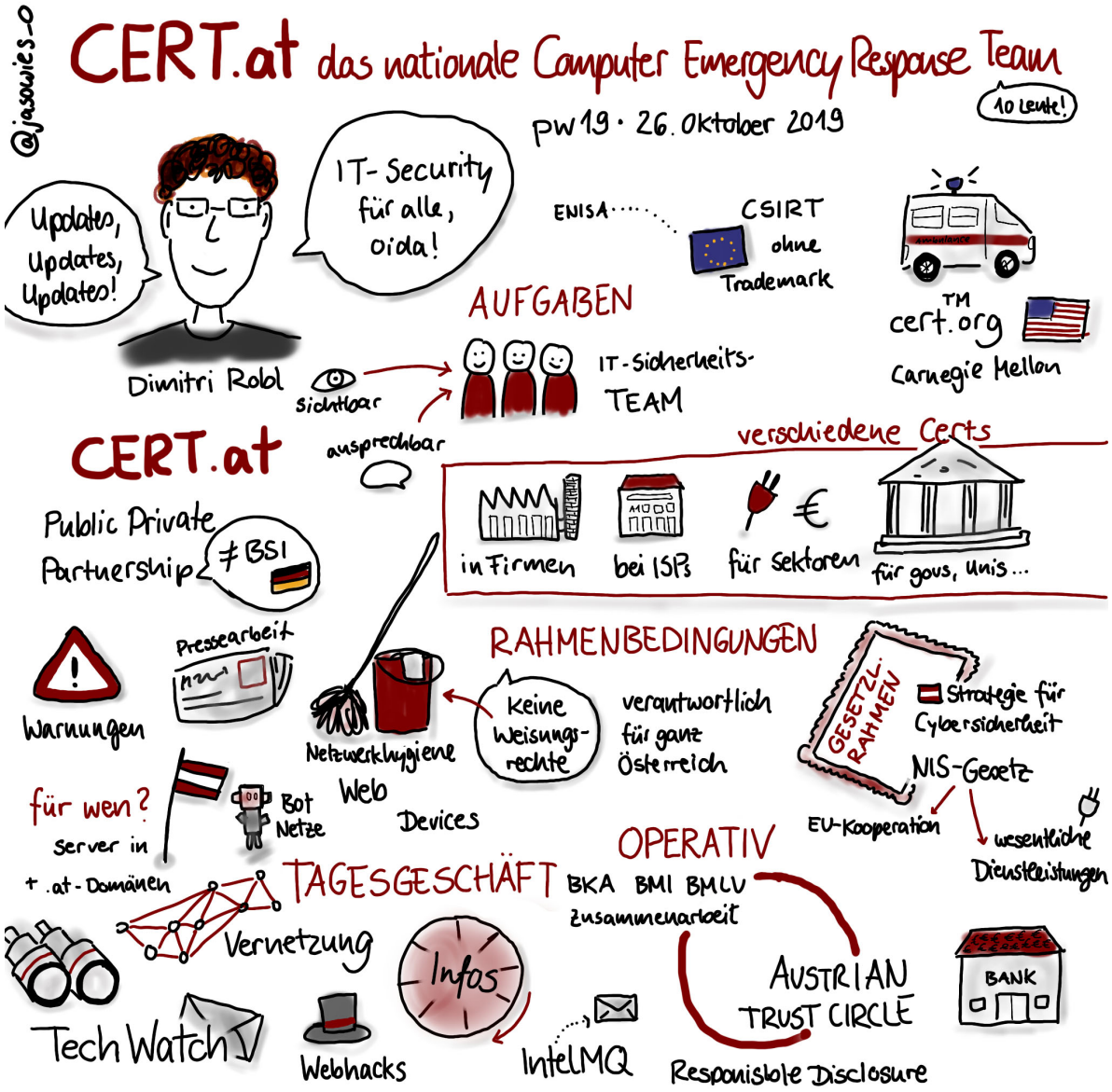


Abbildung 1: CERT.at bildlich dargestellt

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 Emergency Response Team, 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 der Ansprechpartner 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 (siehe dazu 1.1.3: Gesetzlicher Auftrag von CERT.at). Dadurch ist die Zusammenarbeit mit Betreibern wesentlicher Dienste, der kritischen Infrastruktur und relevanten staatlichen Einrichtungen noch enger geworden. Abbildung 1 entstand als Sketchnotes zu einem Vortrag über CERT.at bei der PrivacyWeek 2019 und fasst unsere Arbeit bildlich zusammen.

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 private Personen heraus. Bei Angriffen auf IKT auf nationaler Ebene koordiniert CERT.at die Reaktion auf den Vorfall und informiert die jeweiligen Netzbetreiber 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 eines Public-Private-Partnerships 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, Vorbereitung 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 neun Personen und wird von Robert Schischka gelei-

tet. 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 CERT-Beirat unterstützt. Dieser bringt als beratendes Organ Input in Bezug auf Sichtweisen und Themenvorschlägen ein. Die Mitglieder des Beirats repräsentieren dabei einen Querschnitt der Internet-Community in Österreich, fungieren als BotschafterInnen für CERT.at und stellen sicher, dass CERT.at im Sinne des ganzen Landes agiert.

Die Mitglieder des CERT-Beirats sind:

- Ing. MSc. Franz Hoheiser-Pförtner (MAGWien)
- Erich Albrechtowitz (BKA)
- Ing. Clemens Möslinger, BA MSc (BKA)
- Mag. Wolfgang Ebner (BMDW)
- Mag. Markus Popolari (BMI)
- Ing. Robert Scharinger, MBCS (Sozialministerium)
- GenMjr. Mag. Helmut Habermayer, MSc (BMLV)
- DI Philipp Blauensteiner (BVT)
- Ing. Thomas Mandl (CDCE)
- Univ. Prof. Dr. Nikolaus Forgo (Universität Wien)
- Univ. Prof. Dr. Reinhard Posch (TU Graz)
- Ing. Dr. iur Christof Tschohl (Research Institute & Co. KG
- Christian Panigl (UniVie/ACOnet/VIX)

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 Netzbetreibern und zuständigen Security Teams in Kontakt tritt. Ein ExpertInnen-Team, das im Falle des Falles Hilfe zur Verfügung steht 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 den 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. Siehe dazu auch Kapitel 3: Kooperationen und Networking.

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, innerhalb dessen jedes Land Kapazitäten für die Cyber-Sicherheit aufbauen muss. Zudem formuliert sie Mindestsicherheitsanforderungen und Meldepflichten für kritische Infrastrukturen und für Anbieter 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. Damit hat das BKA als zuständige NIS-Behörde im April 2019 CERT.at betraut und einen gesetzlichen Auftrag erteilt, ohne ihre Unabhängigkeit und Vertraulichkeit anzutasten. Das zeigt eindrücklich die Rolle, die das Team für die IT-Sicherheit in Österreich spielt, um das Internet im Land gesund zu halten.

1.1.4 Fragebogen “Aufgaben eines nationalen CERTs”

“Was sind Ihrer Meinung nach Aufgaben eines nationales CERTs?” – Das ist die Frage, die wir im Rahmen der IT-Security-Konferenz DeepSec am 28. und 29. Dezember in Wien den BesucherInnen gestellt haben. Circa 30% davon haben ihre Einschätzung auf Fragebögen, die wir sowohl auf Deutsch als auch auf Englisch zur Verfügung stellten, mit uns geteilt. Zentrale Tätigkeiten, die wir als unser täglich Brot erachten, wie etwa die Arbeit als neutrale Informationsdrehscheibe, Koordination und aktive Benachrichtigungen, führten in der Zustimmung deutlich.

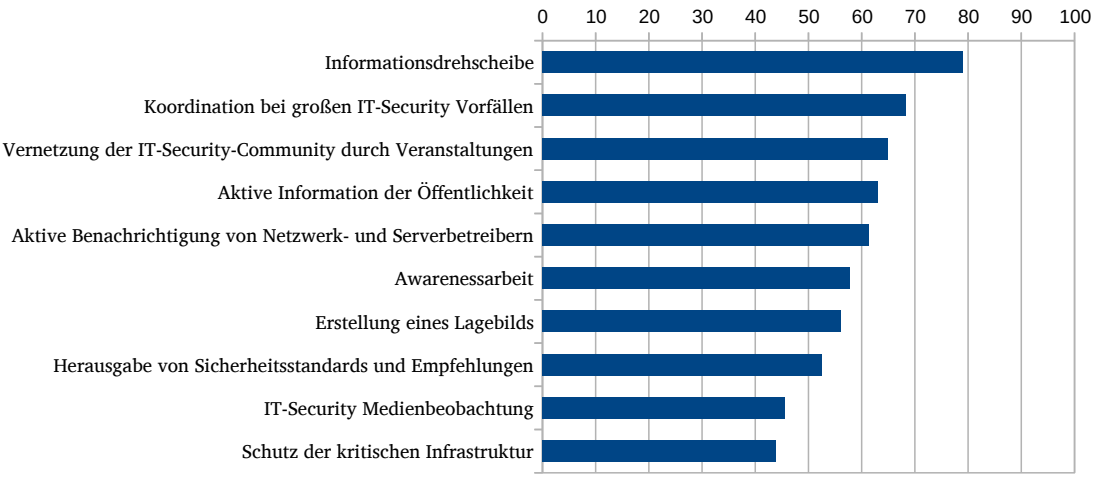


Abbildung 1.1: Top 10 Antworten mit “ja” auf die Umfrage

Tätigkeiten, die weniger Zustimmung erhielten sind aber Voraussetzung für oder Teil von anderen Aufgaben, was für Außenstehende nicht immer ersichtlich ist. Dies betrifft etwa Incident Response, Responsible Disclosure oder die Medienbeobachtung im Bereich der IT-Sicherheit.

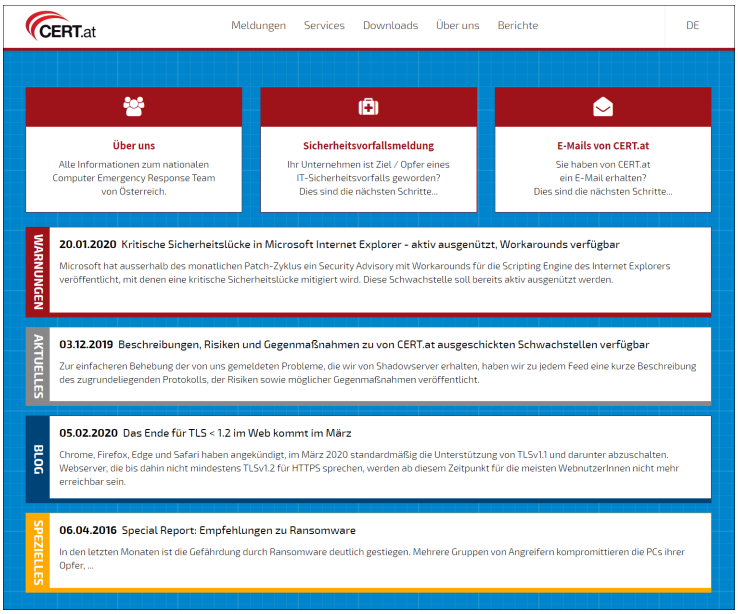
Aus den Ergebnissen lässt sich auch ein klarer Wunsch nach der Herausgabe von Sicherheitsstandards und Empfehlungen durch nationale CERTs/CSIRTs ablesen.

Obwohl der Name “CERT” vermuten lässt, dass auch die Ausstellung von Zertifikaten (insbesondere TLS-Zertifikate) eine unserer Aufgabe sein könnte, wird dieser Bereich von keinem uns bekannten CERT abgedeckt. Der Vorschlag fand bei den Teilnehmenden ebenfalls kaum Zuspruch.

Die Idee eines solchen “Realitätsabgleichs” stieß nach einer Präsentation unserer Umfrage und deren Ergebnisse vor europäischen Partnern im CSIRTs Network auf Zustimmung und könnte bald im Ausland wiederholt werden.

1.1.5 Start der neuen Webseite

Nach dem 10-jährigen Jubiläum von CERT.at 2018 wurde 2019 das Projekt ”Neue CERT Website” in Angriff genommen. Unser Webauftritt war mittlerweile schon ziemlich in die Jahre gekommen und sollte neben einem frischeren Design auch an das Layout und die Technologie der nic.at-Website herangeführt werden. Einer der Hauptbeweggründe dafür war auch die fehlende Kompatibilität des alten Layouts mit kleinen Bildschirmen wie beispielsweise auf Smartphones. Darüber hinaus – und dabei nicht minder wichtig – sollte mit der neuen Website auch den einzelnen Gründen für einen Besuch unserer Website Rechnung getragen werden. Gelöst wurde dies über die neue, sich vom Grundaufbau der restlichen Seiten deutlich abhebende, Homepage:



BesucherInnen finden hier also direkt Links zu Informationen

- über CERT.at,
- wie sie einen Sicherheitsvorfall melden können,
- was zu tun ist, wenn sie eine E-Mail von uns erhalten haben und
- zu aktuellen Vorgängen in der IT-Sicherheitsbranche.

Die bestehenden Informationskategorien “Warnungen”, “Blog” und “Spezielles” wurden um eine weitere ergänzt: “Aktuelles”. Diese deckt den Graubereich zwischen Warnung und Blog ab. Dabei geht es einerseits darum, Meldungen die (noch) nicht unsere Kriterien für eine Warnung[1] erfüllen, aber kritisch genug erscheinen, bereits vor dem regulären End-of-Day zu verbreiten, und andererseits soll damit das Zeitfenster zwischen dem Finden einer potentiellen Warnung bis zu dessen Veröffentlichung überbrückt werden, also quasi eine Frühwarnung noch bevor Recherche und Ausformulierung des eigentlichen Warnings abgeschlossen sind.

[1] Eine Auflistung derselben finden Sie unter https://cert.at/de/meldungen/warnungen/.

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 ausländische Regierungen und internationale Organisationen bei Fragen der IKT-Sicherheit. Es tauscht Informationen und Warnungen mit diesen aus und leitet sie bei Bedarf an inländische InteressentInnen weiter. GovCERT Austria erfüllt dabei seine Arbeit und Aufgaben in enger 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 Bekanntmachung über Risiken und Vorfälle heraus. Es reagiert auf Sicherheitsvorfälle, unterstützt bei Bedarf auch vor Ort und erweitert sein Wissen und Netzwerk durch die Koordination und Teilnahme an nationalen und internationalen Cyber-Übungen.

1.2.1 Public-Private-Partnership mit vielen Vorteilen

Da das GovCERT als Public-Private Partnership (PPP) des Bundeskanzleramtes mit nic.at eingerichtet wurde und auf das gleiche technische Team wie CERT.at zurückgreift, erhält der Staat Zugriff auf qualifizierte, technische Cybersicherheitsexpertise aus dem Privatsektor sowie auf das Kontaktnetzwerk von CERT.at, welches nationales und internationales Know-how und relevante Sicherheitsinformationen (z.B. klassifizierte Dokumente, White Papers usw.) bereithält. Hinzu kommt die Mitarbeit an und das Teilen von gesamtstaatlichen Cyberlagebildern im Rahmen von OpKoord[2] und IKDOK[3] und die Teilnahme an ExpertInnenworkshops, Trainings und sonstigen einschlägigen Fach- und Netzwerkveranstaltungen.

1.3 Kernaufgaben von CERT.at und GovCERT Austria

Die Notwendigkeit der von CERT.at und GovCERT Austria wahrgenommenen Aufgaben wird durch die gestiegenen IT-Sicherheitsbedrohungen der letzten Jahre deutlich: Systeme werden immer komplexer, immer mehr Geräte sind online erreichbar und AngreiferInnen agieren immer professioneller (vgl. dazu 2.6.1 Emotet, Trickbot und Ryuk).

[2] Operative Koordinierungsstrukturen im Cybersicherheitsfall.

[3] Der **I**nneren **K**reis **d**er **o**perativen **K**oordinierungsstrukturen nimmt zentrale Aufgaben der OpKoord wahr.

In den letzten Jahren sind die Bedrohungen immer zahlreicher geworden, was auch zu mehr Aktivität von CERT.at und GovCERT Austria geführt hat. Die Gründe hierfür sind vielfältig; nicht zuletzt liegt aber der ausgesprochen positive Umstand von erhöhter Sichtbarkeit zugrunde, d.h. wir wissen heute viel besser über kriminelle Aktivitäten bescheid weil sich eine viel größere Anzahl an Personen ihrer Bekämpfung verschrieben hat.

CERT.at und GovCERT Austria erfüllen, zusammen und in ihrem jeweiligen Zuständigkeitsbereich, eine Reihe unverzichtbarer Aufgaben, um diesen Bedrohungsanstieg effektiv zu managen:

Information in allen Bereichen: CERT.at und GovCERT Austria verfolgen laufend die Nachrichtenlage zur globalen IT-Sicherheit. Daraus entstehen Warnungen (via Web, Mail, RSS, Presse, Twitter) für potentiell Betroffene, wenn akuter Handlungsbedarf aufgrund neuer Erkenntnisse 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 neben selbst entwickelter Sensorik auf Quellen innerhalb der internationalen Gemeinschaft der IT-Sicherheitsbranche.[4] 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 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.

1.4 Zertifizierungen 2019

1.4.1 ISO 27001 Zertifizierung

Unternehmen müssen sich umfassend gegen Angriffe auf ihre Daten und Netzwerke absichern. Auch CERT.at muss nicht nur für die Sicherheit im Internet in Österreich sorgen; auch die Sicherheit der eigenen IT-Systeme und der eigenen Infrastruktur ist ein entscheidender Faktor. Eine Zertifizierung nach ISO 27001/2013 ist der Nachweis, dass IT-Sicherheit in einem Unternehmen umfassend behandelt wird und umfasst, neben der Prüfung der Sicherheit der technischen Systeme und der Sicherheit der physischen Infrastruktur, auch organisatorische Aspekte. Die ISO 27001 Zertifizierung ist ein Gütesiegel nach außen und zum anderen auch ein laufender Ansporn für die Sicherstellung der eigenen Sicherheit nach innen. Jährliche Audits bei CERT.at stellen sicher, dass dieser Standard auch gehalten wird.

[4] Eine ausführliche Beschreibung der verwendeten Quellen findet sich in 2.4 Datenbasis.

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 anzustreben. Eine gemeinsame Zertifizierung von nic.at und CERT.at im Jahr 2014 wäre wegen der unterschiedlichen Anforderungen und getrennten System zu aufwendig gewesen. Der notwendige Prozess und alle Maßnahmen zu ISO-Zertifizierung von CERT.at und GovCERT wurden im Jahr 2017 erfolgreich abgeschlossen. 2019 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 das wichtigste 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 2019) eines von sechs 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.


@jasowies_o
CERT.at 2019
incident reports
Fehlalarm
irrelevantes
INCIDENT
investigations
Automatisierung
FEED
who is
abuse contact
EVENTS
veraltete Protokolle
Ports fälschlich offen
Schadsoftware
Defacements
Leaks
vulnerable
malicious code
1
Defacement
2
3
händische Überprüfung
WEBSEITEN
Defacements
Fake Pharmacy Hacks
Phishing
Malware
Ferien
mirai
Bot-Net
absolut gozi
vulnerable
unwanted access
weak crypto
info disclosure
passwords
elastic search
availability
Ddos
information gathering
SSL TLS
veraltete Kryptografie
UDP Amplification
from:
to:
ABER:
false positives
intrusion attempts

Kapitel 2

Das IT-Sicherheitsjahr 2019

Wie schon in 1.1 CERT.at – Österreichs nationales CERT erläutert, fungiert CERT.at als Informationsdrehscheibe für Cyber-Sicherheitsprobleme in Österreich, ist also zuständig für Sicherheitsprobleme von IKT Geräten unter der Domäne `.at` und aller österreichischen IP-Adressen. Dabei hat es selbst kein Durchgriffsrecht und steht Betroffenen mit Informationen und Koordinationsleistungen zur Seite.

Unternehmen und Internet-Service-Provider sind grundsätzlich selbst an einer Behebung von Sicherheitsrisiken interessiert und haben ihre eigenen Ansprechpersonen für Cyber-Sicherheit. An diese wenden sich die ExpertInnen von CERT.at, wenn sie auf ein Sicherheitsrisiko oder einen bereits erfolgten Angriff stoßen.

Als öffentlich sichtbarer Ansprechpartner für das Thema Cyber-Sicherheit 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 Cyber-Sicherheitsprobleme, welche die öffentliche Infrastruktur betreffen.

Die Graphik auf der vorhergehenden Seite fasst die Tätigkeiten von CERT.at zusammen und verbildlicht dieses Kapitel des Berichts.

2.1 Incident Reports, Incidents und Investigations

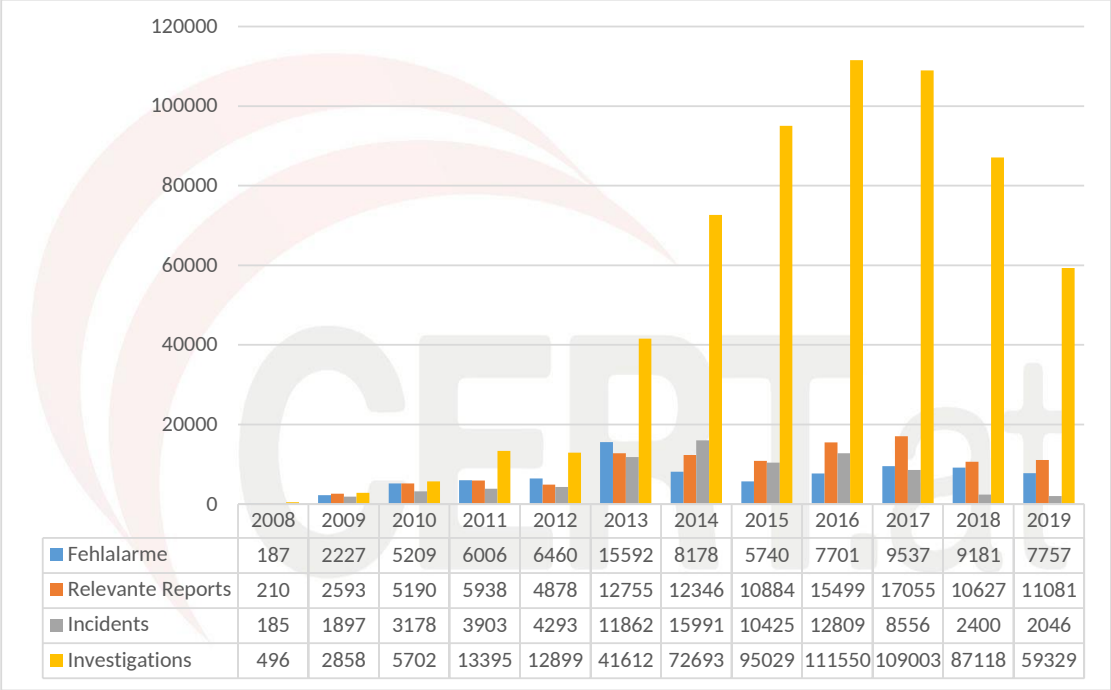
Eingehende und ausgehende Informationen werden bei CERT.at und GovCERT Austria über ein Ticketsystem (aktuell Request Tracker for Incident Response a.k.a. RTIR) abgehandelt. Dabei wird bei Vorfällen zwischen Incident Reports, Incidents und Investigations unterschieden:

Incident Reports sind Meldungen über Sicherheitsprobleme oder -vorfälle, die bei CERT.at eingehen. Diese werden anschließend als relevant, informativ oder 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 2.4 Datenbasis) als auch von Privatpersonen stammen. Sie werden grundsätzlich vertraulich behandelt und können auch per PGP-verschlüsselte E-Mail geschickt werden.[1]

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

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
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701	9537	9181	7757
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055	10627	11081
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556	2400	2046
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003	87118	59329

Abbildung 2.1: 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 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 2.5.1 IntelMQ.

Die Abbildungen 2.2, 2.3 und 2.4 zeigen die Top 5 Kategorien der von CERT.at als relevant eingestuften Incident Reports, der Incidents und aller Investigations.

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 beispielsweise in einem Monat ähnlich viele Incidents unter den Kategorien “vulnerable” und “malicious code” haben, zeigen die zugehörigen Incident Reports und Investigations, dass wir einerseits wesentlich mehr Meldungen in der Kategorie “vulnerable” bekommen haben, die dann unter einem Incident zusammengefasst wurden.

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 von einem bestimmten Trojaner befallenen Geräten (Taxonomie “malicious code”). 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, was zu 100 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 2.3 2019 im Detail näher eingegangen.

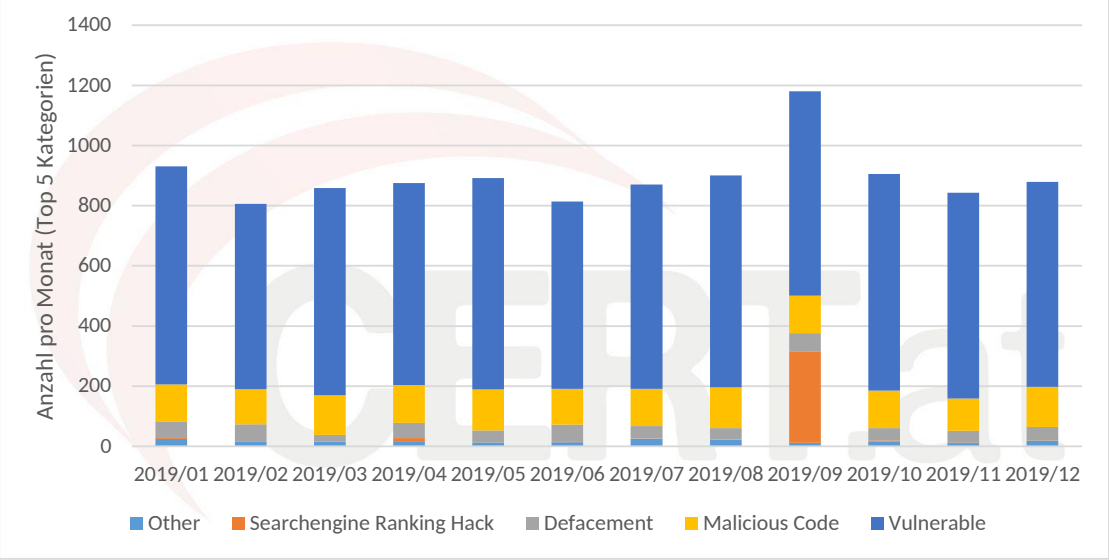


Abbildung 2.2: Top 5 Incident Reports Kategorien

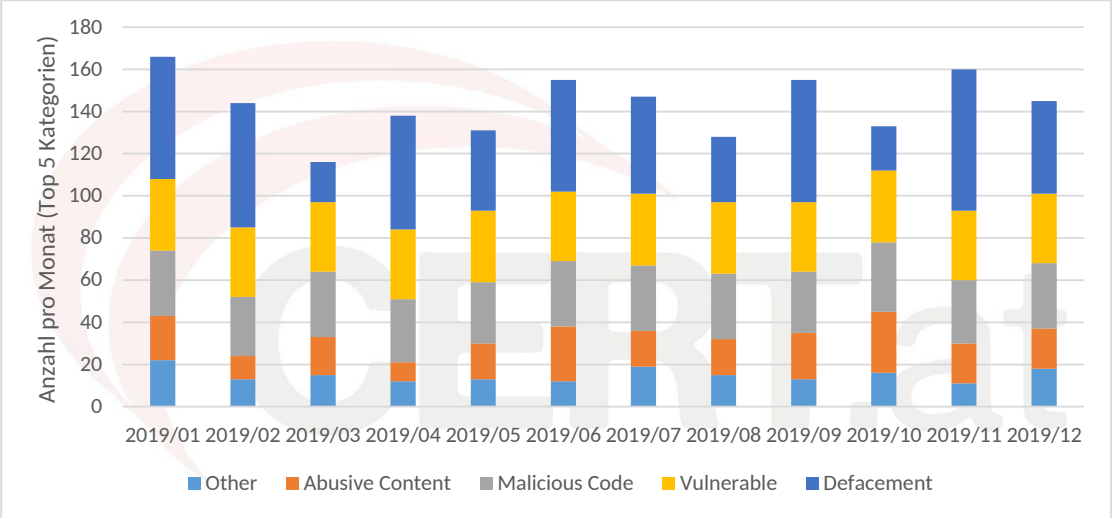


Abbildung 2.3: Top 5 Incident Kategorien

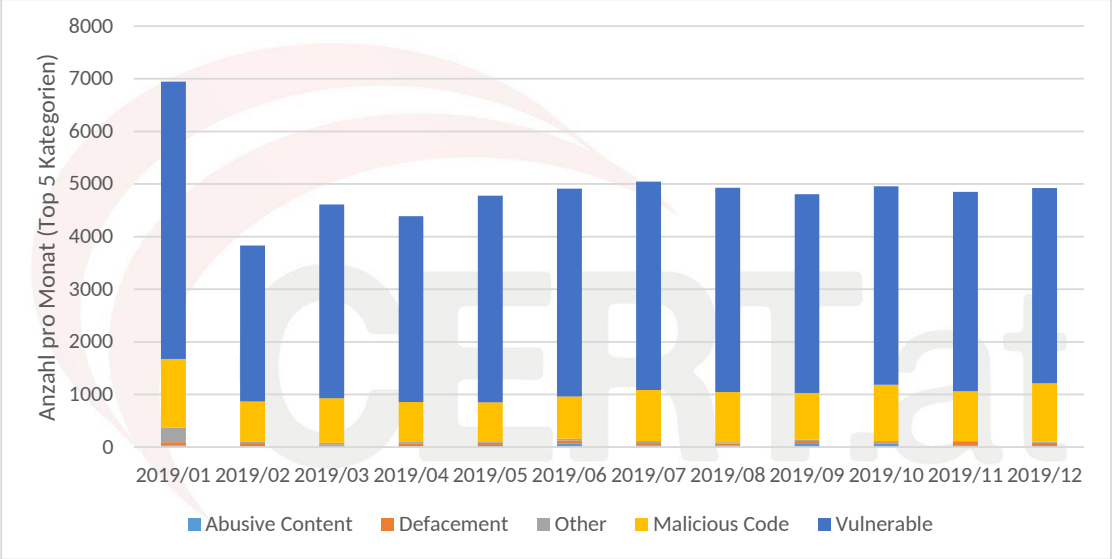


Abbildung 2.4: Top 5 Investigation Kategorien

2.2 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 die-

ser 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 2.3.2 Probleme im Web.

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.

2.2.1 Reference Security Incident Taxonomy – ein kurzer Überblick

Abusive Content: Darunter fallen z.B. Spam, Hate-Speech, gewaltverherrlichende oder auch kinderpornographische Inhalte.

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 nicht-bösartige Einflüsse 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 2.3.1 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 als ganze einer Überarbeitung bedarf.

Test: Für Testfälle.

2.3 2019 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 nicht sein sollte, schicken wir das nicht täglich weiter, um die BetreiberInnen/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), schicken wir diese Information aggregiert an die Verantwortlichen weiter, d.h. hinter einer einzelnen Investigation können zahlreiche Datenbankeinträge stecken.

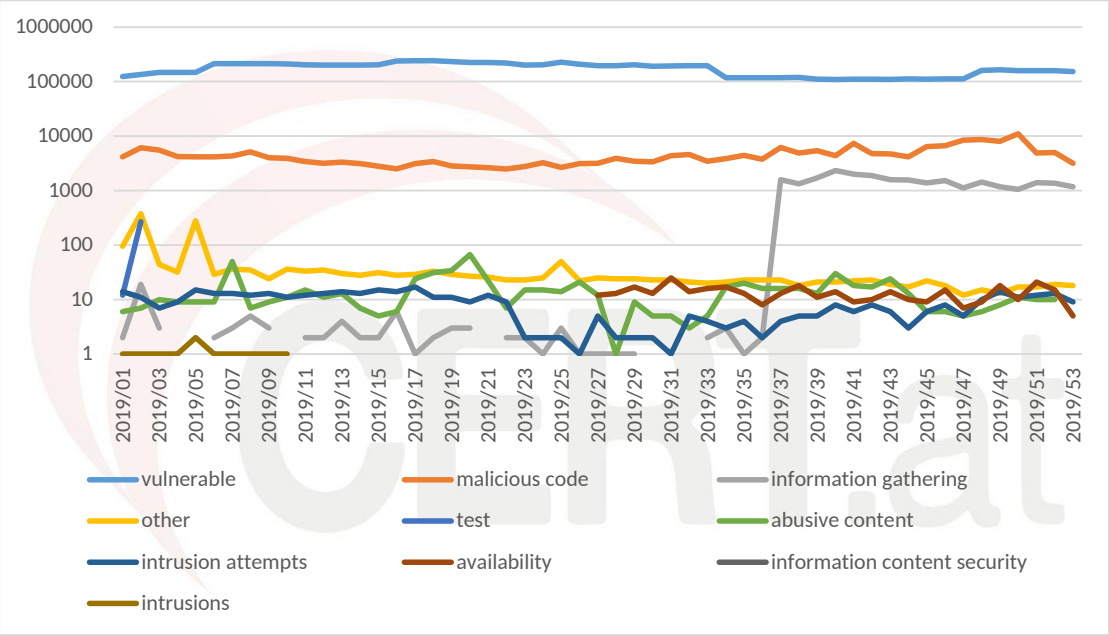


Abbildung 2.5: Events nach Taxonomie (logarithmische Skala)

Insgesamt ist noch zu bemerken, dass manche Events doppelt gezählt werden, da sie in zwei unterschiedliche Taxonomien fallen.

Abbildung 2.5 zeigt alle neuen Einträge in unsere Datenbank über das gesamte Jahr 2019. Wie auch schon in 2.1 Incident Reports, Incidents und Investigations sind Events mit der Taxonomie “vulnerable” mit Abstand am häufigsten. Entsprechend Abbildung 2.5 sind sie etwa zehn Mal soviele wie die zweithäufigste Kategorie, “malicious code”.

[2] Für eine genauere Beschreibung siehe 2.4 Datenbasis.

2.3.1 Taxonomie “vulnerable”

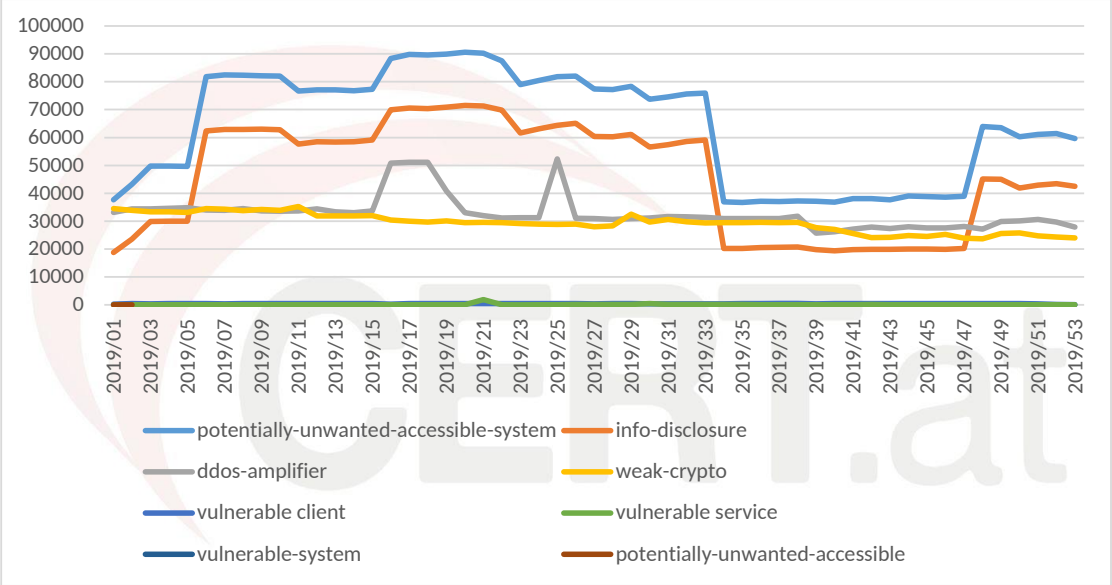


Abbildung 2.6: Alle Events der Taxonomie “vulnerable”

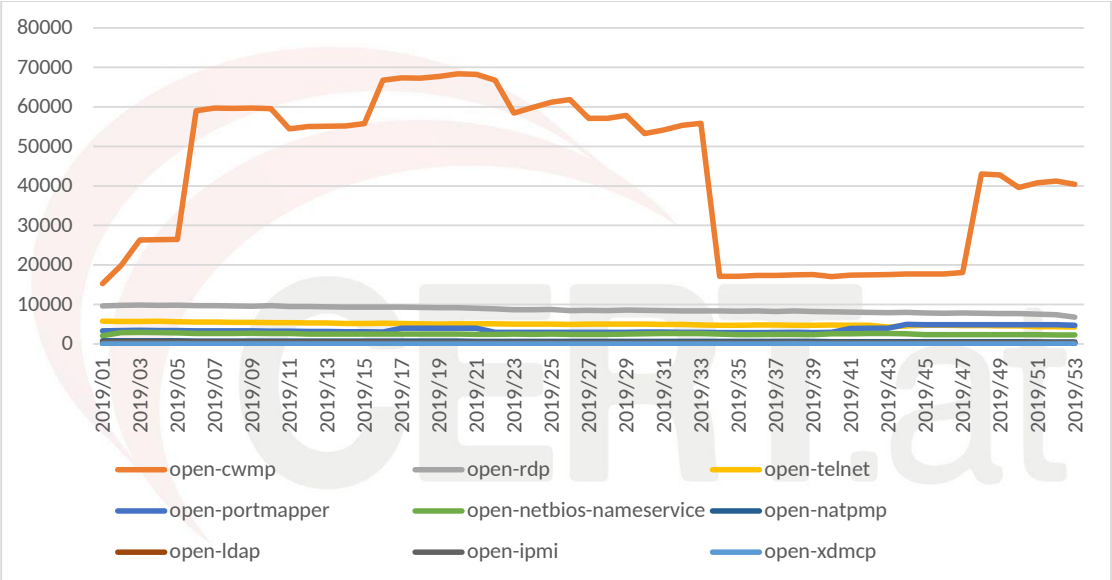


Abbildung 2.7: Ports die nicht öffentlich erreichbar sein sollten

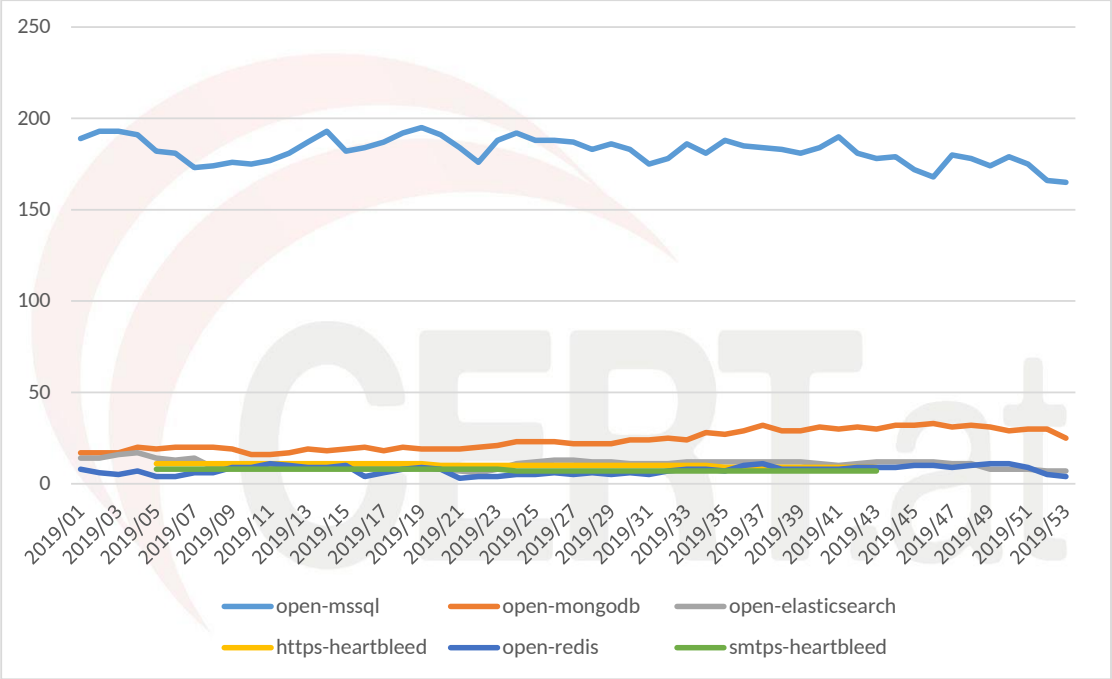


Abbildung 2.8: Services über die sensible Informationen gewonnen werden können

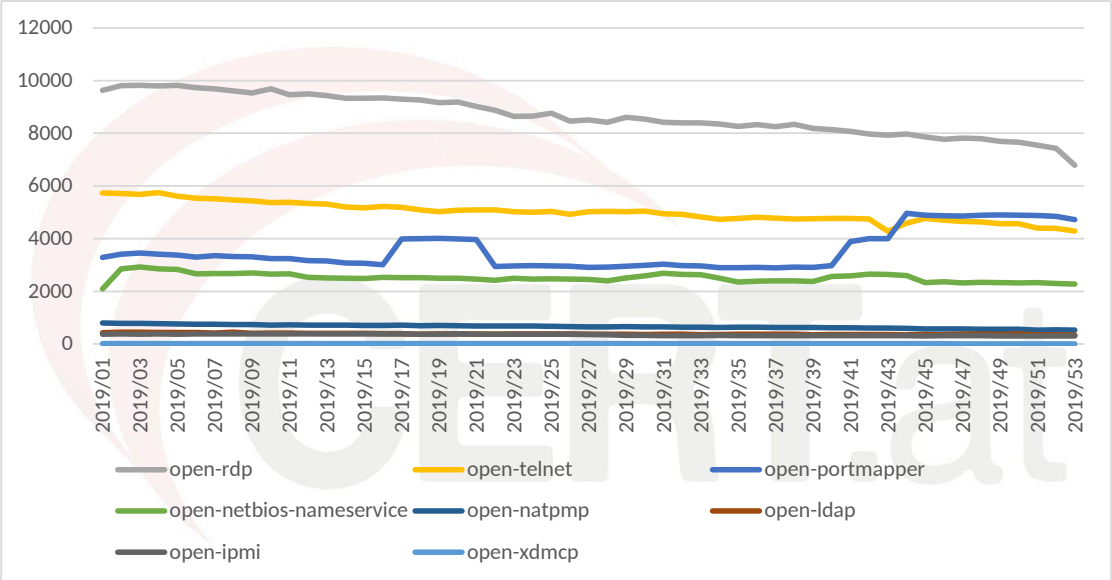


Abbildung 2.9: Wie Abbildung 2.7 nur ohne CWMP

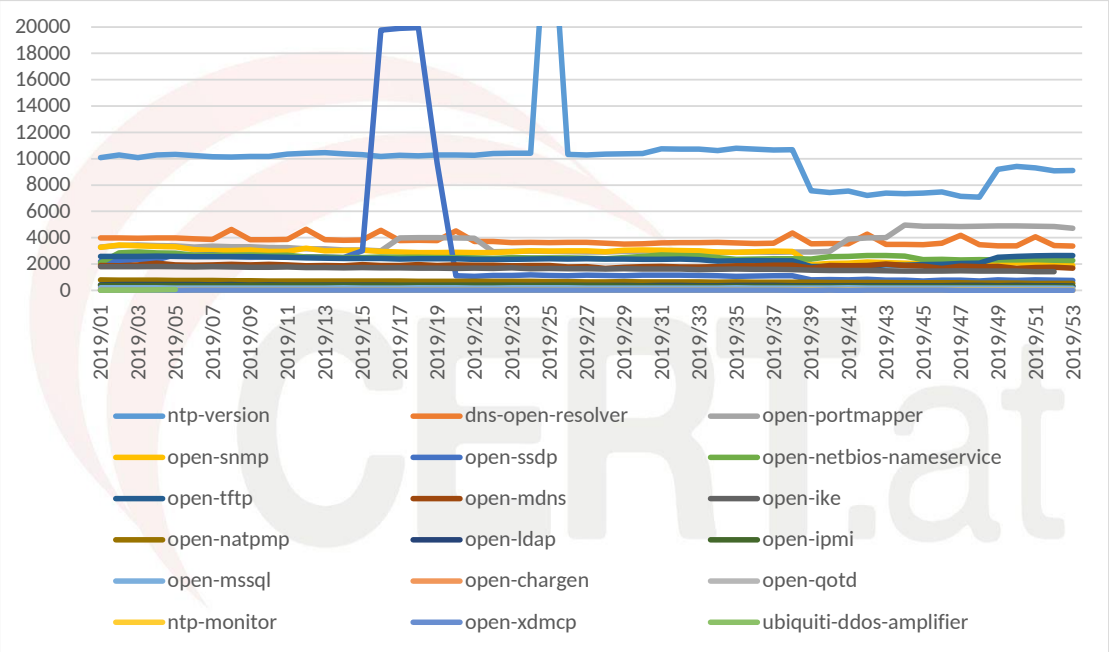


Abbildung 2.10: Geräte die für UDP DDoS Amplifikation missbraucht werden können

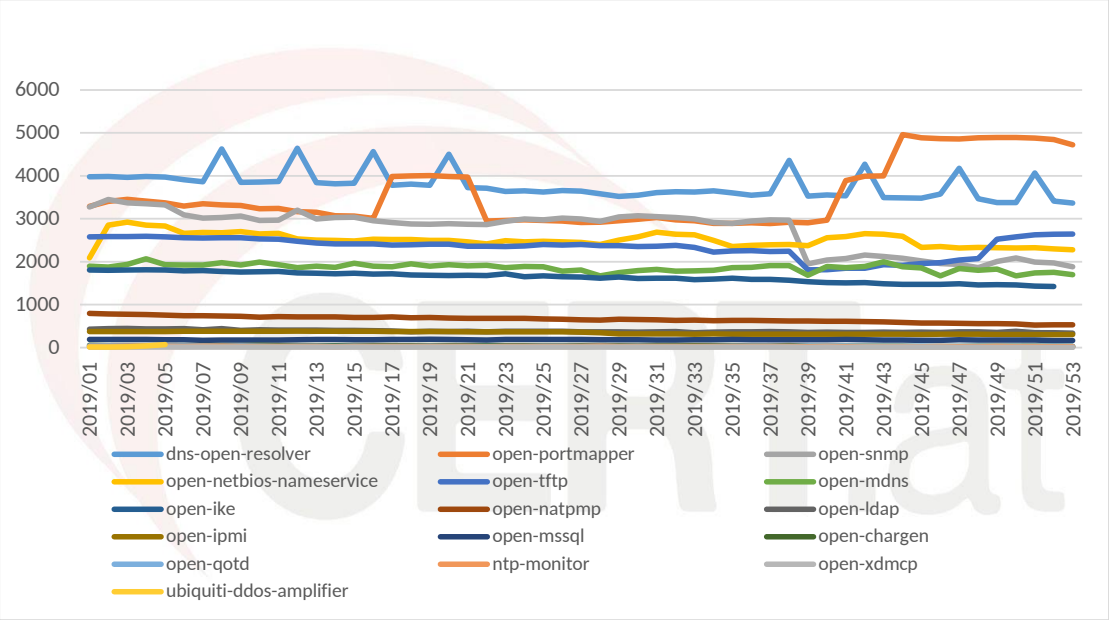


Abbildung 2.11: Abbildung 2.10 ohne NTP und SSDP

Da sich die meisten Events, von denen CERT.at Kenntnis hat, in diese Kategorie einordnen lassen, lohnt sich ein etwas genauerer Blick auf die Daten.

In Abbildung 2.6 zeigt sich, dass auch innerhalb der Taxonomie “vulnerable” nur ein kleiner Teil von Schwachstellen für den Großteil der Events verantwortlich ist. Konkret sind das Protokolle, deren Erreichbarkeit aus dem offenen Internet mit ho-

her Wahrscheinlichkeit unbeabsichtigt ist, wie beispielsweise RDP-Server oder IPMI[3] (Abbildung 2.7), sowie Protokolle mit deren Hilfe potentiell sensible Informationen über das dahinterliegende Netzwerk gewonnen werden können (Abbildung 2.8).

Beim Vergleich des Verlaufs der beiden Graphen in Abbildung 2.6 fällt auf, dass sie quasi identisch sind, was daran liegt, dass das Protokoll CWMP (CPE WAN Management Protocol) in beide Kategorien fällt. Dabei handelt es sich um ein Protokoll, das ISPs ermöglicht, Endgeräte bei KundInnen über das Netzwerk zu konfigurieren. Dies ist einerseits mit hoher Wahrscheinlichkeit nicht absichtlich aus dem ganzen Internet erreichbar und andererseits können darüber potentiell Informationen zur Konfiguration ausgelesen werden.

Da CWMP wiederum viel häufiger als die anderen Probleme in den jeweiligen Taxonomien ist, finden sich in Abbildung 2.8 und Abbildung 2.9 Graphen ohne dieses Protokoll.

Eine weitere wichtige Gruppe innerhalb der Taxonomie “vulnerable” sind jene Geräte, die für UDP DDoS Amplifikation missbraucht werden können. Bei diesen Angriffen wird folgendes Problem ausgenutzt: Bei Protokollen die als Transport Layer UDP verwenden, wird keine längerfristige Verbindung zwischen den Geräten aufgebaut, sondern Pakete werden geschickt und sofort wieder vergessen. Aus diesem Grund ist es beim Empfang solcher Pakete auch nicht möglich, die Absendeadresse zu verifizieren; Antworten werden quasi “blind” an die angegebene Absendeadresse verschickt.

AngreiferInnen können sich das zunutze machen, indem sie möglichst viele Anfragen an möglichst viele Geräte schicken, in denen sie als Absendeadresse jene ihres Opfers angeben. Wenn die Antworten dann protokollgemäß an diese gefälschte Adresse geschickt werden, kann das bei ausreichender Anzahl der Antworten zu einem DDoS-Angriff gegen das Opfer werden.

Um in solchen Szenarien einen möglichst großen Effekt bei möglichst geringem Aufwand zu erzielen, setzen AngreiferInnen auf Protokolle, bei denen die Anfragen im Verhältnis zur Antwort klein sind. Je größer die Antwort im Vergleich zur Anfrage, desto größer ist der sog. “Amplifikationsfaktor”.

In Abbildung 2.10 und Abbildung 2.11 sind jene Protokolle abgebildet, die in Österreich für solche Angriffe missbraucht werden können.

Während der temporäre starke Anstieg von offenen SSDP-Servern nach unseren Informationen tatsächlich stattgefunden hat, ist der einmalige Peak von NTP Mitte 2019 auf ein Problem eines unserer Datenfeeds zurückzuführen.

2.3.2 Probleme im Web

Das World Wide Web stellt zwar nur einen Teil des Internets dar, ist aber dennoch für viele der Inbegriff desselben bzw. ihr einziger bewusster Kontakt damit. Deshalb gliedert CERT.at Schwachstellen im Bereich des Web genauer auf, als in anderen Bereichen. Außerdem ist in diesem Bereich mehr Handarbeit notwendig als anderswo. Das hat vor allem 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 mit nicht immer gut funktioniert, ist, dass es in vielen Fällen um die Beurteilung der Legitimität von Inhalten geht. So ist der Schriftzug “defaced by” zwar eine Phrase, sie sehr häufig bei

[3] IPMI steht für “Intelligent Platform Management Interface” und ist nur der Name für eine standardisierte Schnittstelle die das Warten von Servern über das Netzwerk ermöglicht, selbst wenn diese abgeschalten sind. Bekannte Implementierungen davon sind HPEs iLO und Dells DRAC.

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.

In Abbildung 2.12 finden Sie einen Überblick zu den verschiedenen Angriffen auf Webseiten, von denen CERT.at Kenntnis hat.

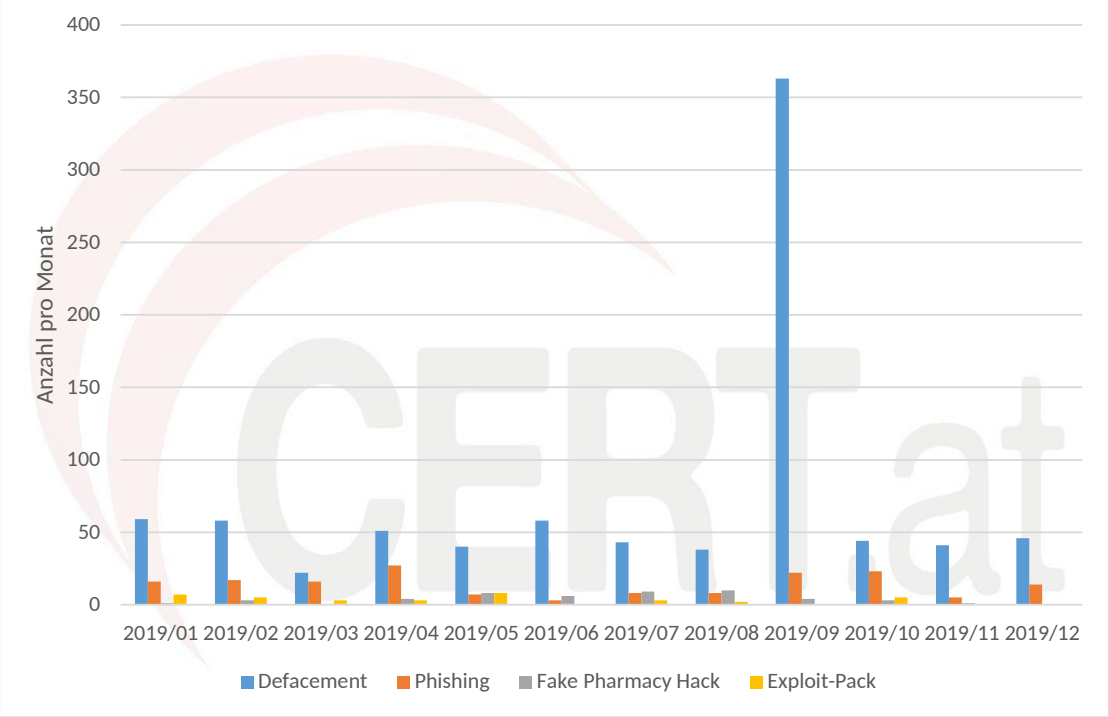


Abbildung 2.12: Gehackte Webseiten

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.

Der immense Anstieg von Defacements im September 2019 ist nicht auf eine tatsächliche Häufung zurückzuführen, sondern darauf, dass es AngreiferInnen bei einer einzelnen Webseite gelang, Subdomänen zu “defacen” bzw. sogar anzulegen. Jede Subdomäne wird von unseren Tools einzeln gezählt. Würde das also bei der Domain `example.com` passieren, so wären `www.example.com`, `unterseite1.example.com`, `unterseite2.example.com`, etc. defaced und würden jeweils einzeln gezählt.

Solche Subdomains einzeln zu behandeln ist insofern sinnvoll, als manche BesitzerInnen von Domains Subdomains weiterverkaufen und somit tatsächlich eine andere Person für die Subdomain zuständig ist, als für die Hauptdomain. Bekannte Beispiele dafür sind `wordpress.com` oder `blogger.com`.

Phishing

Während Defacements im allgemeinen eher harmlos sind und wenn überhaupt zu einem Reputationsschaden führen, sind Phishingseiten immer problematisch. Hier

versuchen AngreiferInnen Zugangsdaten von BesucherInnen zu stehlen, indem sie beispielsweise die Login-Seite einer Bank nachbauen.

Fake Pharmacy Hack

Mit diesem Begriff bezeichnet CERT.at eine Taktik, bei der AngreiferInnen durch diverse Techniken versuchen, Suchmaschinen wie Google dazu zu bringen, Personen, die auf ein Ergebnis in ihrer Suche klicken, auf eine andere Seite als die in den Ergebnissen angezeigte umzuleiten. In den meisten Fällen landen die Betroffenen dann auf einem betrügerischen Online-Shop, der vorgibt, billige Potenzmittel zu verkaufen.

Exploit Packs

Bei diesem Angriff wird auf einer (zumeist) sonst legitimen Seite Schadsoftware eingebaut, die alle, die sie besuchen herunterladen.

2.3.3 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.

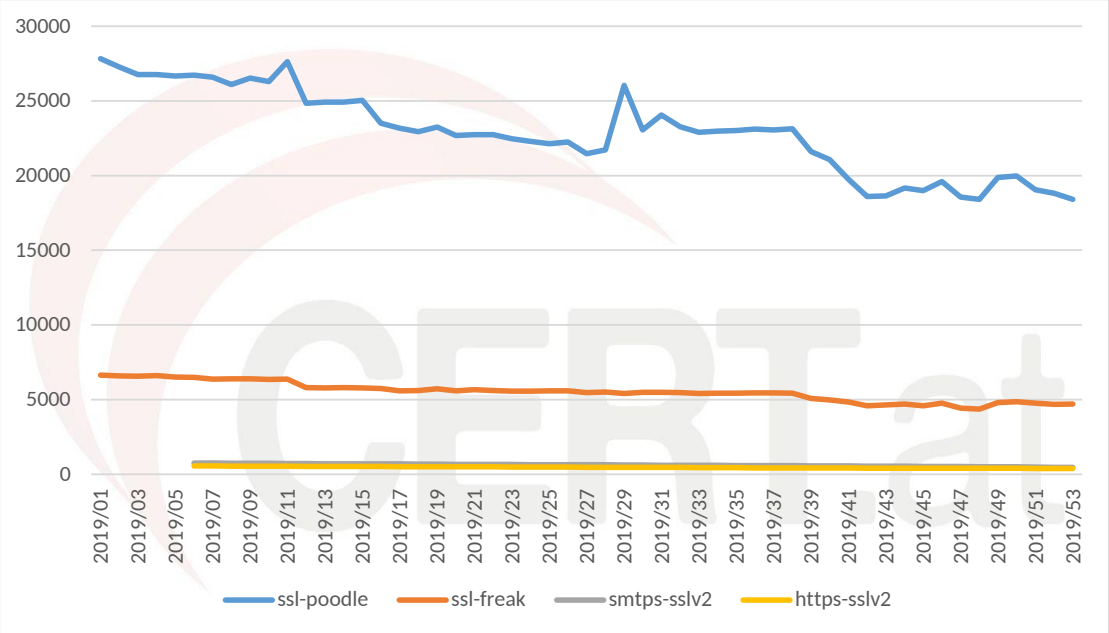


Abbildung 2.13: Web- und Mailserver mit veralteter Kryptographie

Das Positive an Abbildung 2.13 ist der Umstand, dass es in Österreich kaum noch Server gibt, die das völlig veraltete SSLv2 Protokoll aus dem Jahr 1995 im Einsatz haben.

Weniger gut sieht es hingegen bei Webseiten aus, die für POODLE aus dem Jahr 2014 und FREAK aus dem Jahr 2015 anfällig sind, aber auch hier zeichnet sich ein positiver Trend zu weniger betroffenen Servern ab.

2.3.4 Malware

In Abbildung 2.14 findet sich eine Aufstellung der mit Malware infizierten Clients, die CERT.at im Jahr 2019 gemeldet wurden.

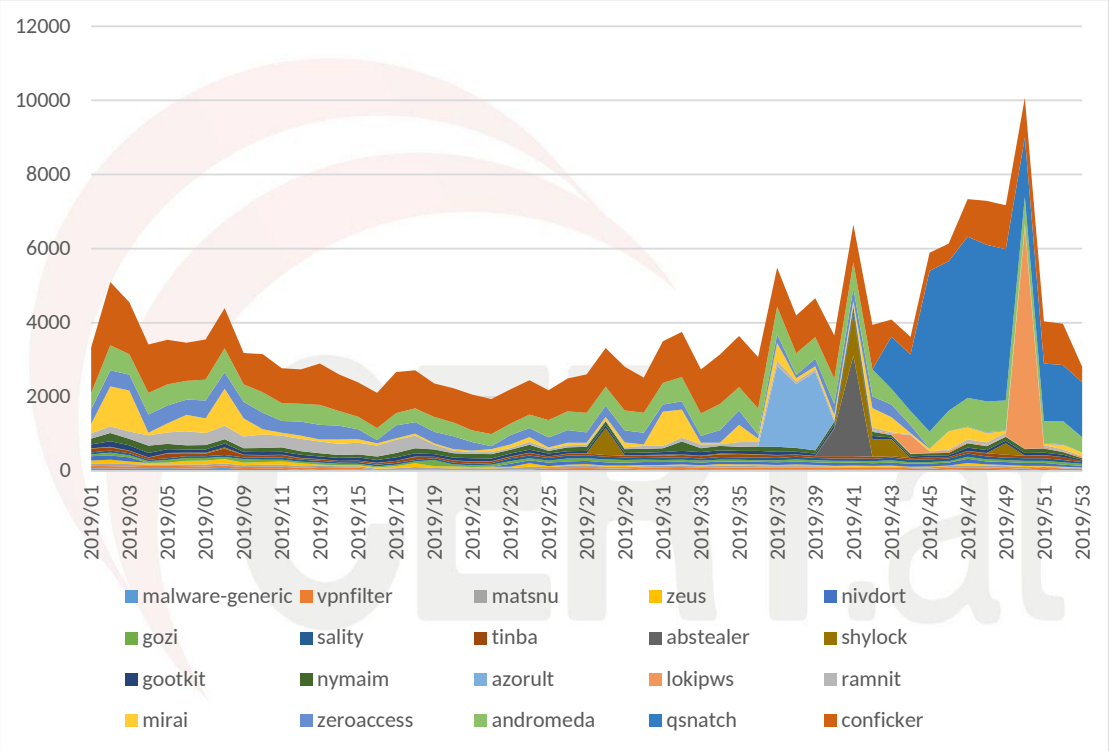


Abbildung 2.14: Mit Malware infizierte Clients

Unseren Quellen zufolge ist die Anzahl aktiver Command and Control (C2) Server, d.h. Server über die infizierte Computer Befehle erhalten, in Österreich im unteren einstelligen Bereich und daher haben wir dazu keine Statistiken erstellt.

2.4 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.

2.4.1 Eigene Erhebungen

Scanning Tools

Für die Suche nach ausgewählten verwundbaren Software-Installationen verwendet CERT.at `masscan` oder andere, z.T. 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-Domänen.

Der Ablauf eines Scans stellt sich gewöhnlich folgendermaßen dar:

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

2019 führte CERT.at folgende Scans durch:

SSLv2 ist ein 1995 veröffentlichtes Protokoll zur Verschlüsselung von z.B. Web- und E-Mail-Verkehr. Es weist gravierende Schwachstellen auf Protokoll-Ebene auf und sollte daher nicht mehr eingesetzt werden. CERT.at versucht dabei mit allen .at-Domänen 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.

In FortiOS, einem Produkt von Fortinet, wurden 2019 zwei gravierende Sicherheitslücken gefunden. Eine davon ermöglichte das Auslesen von Systemfiles (CVE-2018-13379), die andere das Verändern von Passwörtern (CVE-2018-13382). Beide Schwachstellen können über das Netzwerk und ohne jede Authentifikation ausgenutzt werden. Updates dazu wurden zwar rasch zur Verfügung gestellt, allerdings nicht immer eingespielt.

2.4.2 Externe Quellen

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

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

ResearcherInnen und NPOs

Es gibt einige Non-Profit Organisationen und Stiftungen, 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[5] 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 Spam-Blocklisten spezialisiert.

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

Andere CERTs/CSIRTs

Die IT-Sicherheitscommunity tauscht sich in unterschiedlichen Netzwerken und Plattformen aus. CERT.at ist unter anderem Mitglied des Trusted Introducer Netzwerkes, einer Akkreditierungs- und Zertifizierungsorganisations für CERTs/CSIRTs, und von FIRST, einem globalen Forum für CERTs/CSIRTs (vgl. dazu Kapitel 3: Kooperationen und Networking).

Durch diese Organisationen werden nicht nur gemeinsame Standards und Trainingsmöglichkeiten für die IT-Sicherheitscommunity erarbeitet, sondern auch Netzwerke für den Austausch von Informationen geschaffen.

Kommerzielle IT-Firmen

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

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

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

Geräte befinden sich meistens in mehreren Ländern und daher werden die so erfassten Daten – sofern es der rechtliche Rahmen erlaubt – oft an 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, SicherheitsforscherInnen oder CERTs/CSIRTs sogar, Zugang zu Servern der AngreiferInnen zu erlangen. Die dort vorgefundenen Daten geben oft Aufschluss über die Vorgehensweisen und eingesetzten Tools der Kriminellen.

2.5 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.

2.5.1 IntelMQ

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

[7] Zusammengesetzt aus "Threat INTELligence" und "Message Queueing".

Einmalige Aussendungen a.k.a. “Oneshots”

IntelMQ ermöglicht es außerdem, über ein Web-Interface sog. “Oneshots” 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 parsebares CSV-File umgewandelt werden, das dann bequem über das Web-Interface hochgeladen werden kann. Anschließend muss nur noch ein Erklärungstext zum vorliegenden Problem inklusive Links zu Workarounds/Updates verfasst werden und IntelMQ verschickt automatisch Mails an alle Betroffenen. Dies ermöglicht CERT.at nicht nur, schnell auf aktuelle, aber einmalige Umstände zu reagieren, sondern eignet sich auch, um neue Feeds auszutesten, um deren Qualität und/oder Nützlichkeit anhand des Feedbacks der Betroffenen zu evaluieren.

2019 wurde diese Funktion mehrmals genutzt, unter anderem in folgenden Fällen:

- Im Februar informierten wir BesitzerInnen von Web-Interfaces zu Kläranlagen, die ohne Authentifikation offen aus dem Internet zugänglich waren, über diesen Umstand.
- Im April warnten wir NetzwerkbetreiberInnen, die RDP-Server betrieben, die anfällig für die damals veröffentlichte BlueKeep Schwachstelle waren. Außerdem schickten wir im April Betroffenen von CVE-2019-0604, einer kritischen Schwachstelle von SharePoint, Informationen zu ebendieser, nachdem sich herausgestellt hatte, dass sie von Kriminellen aktiv ausgenutzt wird.
- Im August und September erhielten BetreiberInnen von Pulse Connect Secure und FortiOS Warnungen, wenn sie die Updates die vor CVE-2019-11510 für Pulse Connect Secure bzw. CVE-2018-13379 und CVE-2018-13382 für FortiOS, schützen, noch nicht eingespielt hatten.

2.5.2 MISP

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

CERT.at und GovCERT Austria betreiben gemeinsam eine MISP-Instanz zu der TeilnehmerInnen aus der Forschung, staatlichen Institutionen und der Wirtschaft Zugriff haben und Informationen abrufen sowie hochladen können.[9]

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

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

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

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

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

2.6 Bedrohungen 2019

Die meisten Probleme der IT-Sicherheit sind gut bekannt, nur selten werden von Grund auf neue Angriffe entwickelt. Dennoch gibt es in den meisten Jahren einzelne Vorgehensweisen oder Schadsoftware-Arten, die besonders intensiv eingesetzt werden.

2019 war dies aus der Sicht von CERT.at auf der Firmenseite die Malware-Trias Emotet, Trickbot und Ryuk, die Schlagzeilen mit der Verschlüsselung und Erpressung zahlreicher Unternehmen und in manchen Staaten auch öffentlicher Einrichtungen machte.

Privatpersonen hingegen wurden stärker als bisher von sog. “Sextortion-Scams” heimgesucht. Dabei wurden vorwiegend E-Mails verschickt, die behaupteten, das Opfer beim Besuchen von Pornoseiten über eine Webcam gefilmt zu haben und damit drohten, diese Aufnahme zu veröffentlichen.

2.6.1 Emotet, Trickbot und Ryuk

2019 war das Jahr der professionalisierten Erpressungsversuche. Obwohl “Ransomware”, also Schadsoftware, die Dateien auf infizierten Systemen verschlüsselt und für die Entschlüsselung Geld verlangt, als solches nichts Neues ist, kam es dieses Jahr vermehrt zu gezielten Angriffen gegen Firmen. Während sich die Kriminellen zuvor meist auf Privatpersonen konzentriert und (verhältnismäßig) kleine Summen zur Wiederherstellung der Dateien verlangt hatten, verbrachten sie jetzt einige Zeit in den internen Netzwerken von Firmen, um die wichtigsten Server und deren Backups zu identifizieren und die finanzielle Situation der Opfer einschätzen zu können. Sofern Backups vorhanden waren, vernichteten sie diese, bevor die eigentliche Verschlüsselungs-Malware zum Einsatz kam.

Es ist unklar, ob diese Angriffe von denselben oder ähnlichen Gruppen durchgeführt wurden, die davor jene auf Einzelpersonen zu verantworten hatten.

Die Kriminellen bedienten sich bei diesen Attacken vielfach der Malware-Trias Emotet, Trickbot und Ryuk.

Emotet, ursprünglich ein Banking-Trojaner, wird eingesetzt um initialen Zugang in ein Netzwerk zu erhalten. Das geschieht primär über das Verschicken von Spam E-Mails, die URLs zu Malware-Servern oder Attachments mit Schadsoftware enthalten. Die neueren Versionen (seit April 2019) haben außerdem noch ein Ass im Ärmel: Sobald ein Rechner infiziert wird, stiehlt die Schadsoftware das Adressbuch sowie einen Teil der E-Mails des Opfers und lädt sie auf einen Command-and-Control (C2) Server hoch. Mithilfe dieser Daten kann Emotet dann Malspam verschicken, der in eine legitime E-Mail-Konversation eingebettet wird, d.h. Personen bekommen Antworten auf E-Mails die sie tatsächlich verschickt haben und die auch vorgeben, von der ursprünglichen Zielperson zu stammen. Dieser Umstand erhöht die Wirksamkeit massiv, da auch vorsichtigere NutzerInnen hier leicht zum Opfer werden konnten.

Die gestohlenen E-Mails und Kontaktdaten auf den C2-Servern haben für die Kriminellen noch einen weiteren großen Vorteil: Selbst wenn die ursprünglich betroffene Firma/Person, ihr Netzwerk vollständig von Emotet bereinigt, schützt sie das nicht davor, dass weiterhin in ihrem Namen und in echten E-Mail-Verläufen Malspam verschickt wird. Aus diesem Grund können Reputationsschäden auch bei schneller Reaktion vielfach nicht verhindert werden.

Ist der initiale Zugriff auf das Opfernetzwerk gesichert, wird in vielen Fällen Trickbot nachgeladen. Dabei handelt es sich um einen wurmfähigen Trojaner, der diverse Daten stiehlt. Neben Zugangsdaten zu Bankkonten, Cryptowallets und E-Mails gehören auch Passwörter der NutzerInnen der infizierten Maschine dazu, die mithilfe des Tools Mimikatz ausgelesen werden. Auf diesem Weg können die Kriminellen in vielen

Fällen Zugriff auf Passwörter von AdministratorInnen bekommen und sich so im Netzwerk ausbreiten. Finales Ziel ist dabei die Erlangung des Passworts eines AD (Active Directory) Administrationsaccounts, mit dem das gesamte Netzwerk übernommen werden kann.

Ist auch dieser Schritt erfolgreich und konnten sich die Kriminellen ungestört einen Überblick über das Netzwerk und die Finanzen der betroffenen Firma machen, beginnen sie damit, die Backups zu löschen. Wenn das erledigt ist, wird gezielt Ransomware auf wichtigen Computern installiert. Dabei kommen oft Ryuk oder auch das durch den Angriff auf die norwegische Firma Norsk Hydro bekannt gewordene Lockergoga zum Einsatz.

Es ist nicht klar, ob all diese Schritte jeweils von einer Gruppe durchgeführt werden, oder ob eine erste Gruppe die initiale Infektion verursacht, die Zugänge dann an andere verkauft, die sich einen Überblick über das Netzwerk verschaffen und wichtige Accounts übernehmen, und diese dann wiederum weiterverkauft. Auch andere Aufteilungen sind denkbar.

Weiterführende Informationen finden Sie beispielsweise unter https://heise.de/-4573848 oder in den Artikeln des Virus Bulletin zu Emotet und Ryuk.

2.6.2 Sextortion Scams

Bei einem Sextortion-Scam verschicken Kriminelle E-Mails, in denen sie behaupten, den Computer der Opfer gehackt und dann mithilfe der Webcam Aufnahmen davon gemacht hätten, wie das Opfer Pornoseiten besucht habe. Diese Masche ist zwar keineswegs neu, das Ausmaß der Betrugsversuche erreichte 2019 allerdings ungeahnte Höhen. Auch wir haben zahlreiche dieser E-Mails erhalten, hier ein Beispiel, das an <reports@cert.at> ging:

```
ZUM: reports@cert.at

Ich schreibe Ihnen, weil Ich malware auf die Porno-Website
gesetzt habe, die Sie besucht haben.

Mein Virus hat all Ihre persönlichen Daten gesammelt,
und hat Ihre Kamera während Ihrer masturbation eingeschaltet.

Ich muss zugeben, Sie sind sehr pervers.....


Zudem hat die Software Ihre Kontakte kopiert.
Ich werde das Vide  löschen, wenn Sie mir 2.000 EUR in Bitcoin z hlen.
2.000 EUR = 0.2710196 BTC

Dies ist Adresse für die Zahlung :

3C9GAaz[redacted]


Wenn Sie die Zahlung nicht innerhalb von 48 Ştunden abschicken,
werde ich dieses VIdeo an alle Ihre Freunde und Bekannten schicken.
Ich weiß, wo Sie wohnen.

Ich gebe Ihnen 48 Ştunden für die Zahlung.

Es ist nicht notwendig, mir zu sagen,
```

```
dass Sie mir das Geld geschickt haben.

Diese Adresse ist mit Ihnen verknüpft, mein System wird alle Daten
nach der Übertragung automatisch löschen.


*********************************************
Se den Sie sofort 2.000 EUR = 0.2710196 BTC an diese Adresse:

0.2710196 BTC
an diese Adresse:

3C9GAaz[redacted]

(Kopieren & Einfügen)
*********************************************

1 BTC = 7.415 EUR also se den Sie 0.2710196 BTC
an die oben genannte Adresse..


Wenn Sie nicht wissen, wie man Bitcoin se det, googeln Sie es.


Sie können die Polizei einschalten, aber niemand wird Ihnen helfen können.
Wenn Sie versuchen, mich zu verarschen, werde ich das bemerken!

Ich lebe nicht in deinem Land. Also wird man mich auch
nach 9 Monaten nicht finden können.
Bis bald. Denken Sie an die Schande und dass Sie ruiniert werden können.


Anonymer Hacker


P.S. Wenn Sie mehr Zeit zum Kaufen und Se den von BTC benötigen,
 öffnen Sie Ihren Notizblock und schreiben Sie - 48H ++ -, und sparen Sie.
Auf diese Weise können Sie mich kontaktieren.
Ich werde mir überlegen, Íhnen noch 48 Ştunden zu geben,
 bevor ich das V deo an Ihre Kontakte schicke, aber nur,
wenn Sie sehen, dass Sie wirklich versuchen, Bitcoin zu kaufen.
```

Das “bemerkenswerte” an dieser Art von Scam ist, dass sie für die Kriminellen extrem billig ist: Sie müssen selbst keinerlei Infrastruktur betreiben, wie es z.B. bei gefälschten Web-Shops der Fall ist. Außerdem versuchen sie in den meisten Fällen nicht einmal, ihre Behauptungen zu belegen, wenn man vom Fälschen von “To”-Headern in den E-Mails absieht. In einigen Fällen waren auch angebliche Passwörter der Opfer enthalten, die jedoch mit größter Wahrscheinlichkeit einfach aus alten Leaks entnommen waren und in vielen Fällen dementsprechend nicht mehr stimmten. CERT.at ist bis heute kein Fall bekannt, in dem Kriminelle ihre Drohung der Veröffentlichung wahr machten bzw. wahr machen konnten. Wir haben dazu auch einen Blogpost auf Englisch veröffentlicht.

2.7 Hilfe bei Vorfällen

Auch wenn die Hauptaufgabe von CERT.at und GovCERT Austria darin besteht, koordinierend zu untertützen, gibt es Fälle, die dabei herausstechen und wesentlich mehr Zeit erfordern, als im normalen Tagesgeschäft.

2.7.1 Emotet

Im April 2019 gab es eine weltweite Welle von Emotet-Malspam. So weit, so alltäglich. Allerdings nutzte diese Welle neue "Features" von Emotet, die sie extrem erfolgreich machte: Erstens wurde die Domäne in den E-Mail Adressen der Betroffenen dazu verwendet, um glaubwürdige URLs in HTML E-Mails einzubetten. Ging eine solche E-Mail z.B. an reports@cert.at, dann enthielt sie eine URL die wie in Abbildung 2.15 aussah.

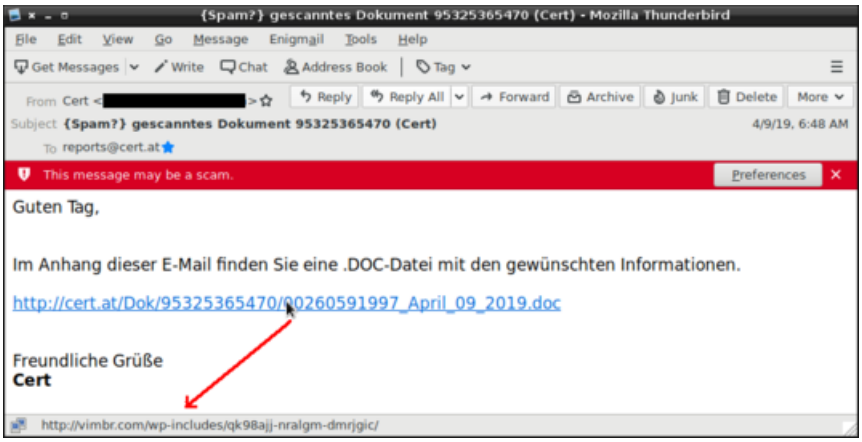


Abbildung 2.15: Emotet Malspam Beispiel

Zahlreiche Firmen dachten dementsprechend zuerst, dass es sich um geziehlte Phishing-Angriffe gegen ihre MitarbeiterInnen handelte, was viele an CERT.at meldeten.

Für mehr Informationen zu Emotet vgl. 2.6.1: Emotet, Trickbot und Ryuk.

CERT.at sammelte Informationen von Betroffenen und gab Hilfestellungen bei der Bereinigung. Außerdem informierten wir die Öffentlichkeit mit einem Blogpost, in dem auch kurzfristig IoCs (Indicators of Compromise) gesammelt wurden.

2.8 Übungen

Im Jahr 2019 nahm CERT.at an zwei größeren Übungen teil; der CyberCoin und der CyberSOPex der ENISA.

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 (offline durch Organisation und Teilnahmen an Konferenzen/Besuchen/Treffen, online durch Mailinglisten, Social Media und Instant Messaging) und kümmern sich um 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 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 Gebe, 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.

Ein Mitglied des ATC sind die Wiener Linien, deren IT-Sicherheitsbeauftragter den folgenden Gastbeitrag verfasst hat.

Gastbeitrag: Eine Lanze für den ATC (Autor: Anton Sepper)

Als ich, der Empfehlung eines Kollegen aus meinem erweiterten Arbeitsumfeld folgend, vor geraumer Zeit an einem Dezembervormittag im Wiener Café Schwarzenberg erstmals einem jungen Proponenten des ATC gegenüber saß, hatte ich noch keinen Begriff davon, von welchem Wert und von welcher Qualität die in diesem Gespräch angestoßenen Impulse für mich und damit für mein Arbeitsumfeld einmal sein würden.

Wir sprachen, weit ausholend, über Informationssicherheit generell und spezifisch über die Behandlung besonders schutzwürdiger Bereiche, über Kriterien zur Identifikation derselben und geeignete Maßnahmen zu deren besserem Schutz. Hier sei noch angemerkt, dass dieses Gespräch sehr lange vor dem Werden der nun geltenden, von der NIS-RL ausgelösten, gesetzlichen Regelungen stattfand. Wir stellten fest, dass in der Branche zu diesem Zeitpunkt bis auf einige freiwillig einzuhaltende Standards kein verbindliches Regelwerk zur Informationssicherheit existierte und es bereits ein guter Schritt wäre, wenn man sich allgemein auch ohne legistischen Druck wenigstens an klar definierten, standardisierten Mindestanforderungen orientieren und in diesem Zusammenhang “dieselbe Sprache sprechen” würde. Im Grunde ist das ja eine Sache des Hausverstands, wie wir aber wissen, wird diesem nicht zwangsläufig branchendeckend jener Platz eingeräumt, der ihm eigentlich zukäme.

Ich jedenfalls wollte gerne wissen, wie bestimmte Themen an anderen Stellen, in anderen Unternehmen behandelt würden, um daran allenfalls Maß für die eigenen Strukturen und Bemühungen nehmen zu können. Es war ein überaus konstruktives Gespräch, aus dem ich einige sehr brauchbare Gedanken mitnehmen konnte, deren Umsetzung ich auch bald danach in die Wege leitete. Am Ende des Treffens erhielt ich das Angebot, für mein Unternehmen dem ATC beizutreten.

Nach interner Klärung war es bald darauf so weit und ich durfte an der ersten Sitzung teilnehmen – als “Neuer” und doch von Anfang an vollkommen in die Gruppe

aufgenommen. Die Runde diskutierte über aktuelle Entwicklungen zur Informationssicherheit im gemeinsamen Sektor, anschließend wurde eine Präsentation gezeigt, danach über diese gesprochen. Es war immer eine Dynamik vorherrschend, man hatte einander etwas zu sagen.

In der Folge besuchte ich weitere Treffen und allmählich erhielt ich ein konsistentes Bild von den Eckpunkten und Zusammenhängen im eigenen Sektor und weit darüber hinaus. Besonders hervorgehoben seien hier die überaus interessanten, aus ausgezeichneten Vorträgen und Arbeitsrunden zusammengestellten Jahrestreffen, die zudem eine stark fördernde Wirkung auf die Beziehungen innerhalb der Community haben und allen eine Vielzahl an Eindrücken aus der Branche bieten.

Ich kann aus heutiger Perspektive sagen, dass mir die Ereignisse von damals den Startimpuls gaben, Informationssicherheit nicht nur als interne Angelegenheit, sondern als im Grunde notwendig vernetzten und unbegrenzten Komplex zu verstehen, zu dem von allen Beteiligten auch entsprechend beizutragen ist. Deshalb schätze ich die Arbeit des ATC hoch und trage gerne dazu bei. Sich in dieser Community zu engagieren ist eine win-win-Angelegenheit für alle Beteiligten ohne jeden Nachteil. Wir treten damit aus unseren Partikularperspektiven heraus und gewinnen oft eine gemeinsame Sichtweise auf zahlreiche Themenbereiche.

Die Zusammenarbeit beschränkt sich selbstverständlich nicht nur auf die geplanten Veranstaltungen, für auftauchende Probleme oder für eine Frage findet sich auch sonst immer ein kompetenter Ansprechpartner, der einem auf kurzem Wege weiterhelfen kann. Es geht bei alledem um sehr alte, im Alltag manchmal scheinbar etwas in den Hintergrund tretende Tugenden wie Vertrauen, Aufrichtigkeit und Mut, die richtigen Dinge anzusprechen – das muss wachsen, das kann man nicht erzwingen.

Abschließend möchte ich den Organisatoren des ATC und den daran teilhabenden Kolleginnen und Kollegen meinen Dank für ihr Engagement und für die sich dadurch eröffnenden Möglichkeiten aussprechen und mit dem olympischen Gedanken enden: Dabei sein ist alles!

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 bestätigt.

Der CERT-Verbund wurde 2011 als Kooperation aller 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

Mit Stand Ende 2019 nehmen 14 Teams am österreichischen CERT-Verbund teil. Genauere Informationen finden Sie online.

3.2.3 IKDOK/OpKoord

Die »Struktur zur Koordination auf der operativen Ebene« (auch “Operative Koordinierungsstruktur” oder kurz “OpKoord” genannt) wurde gemäß der ÖSCS[1] im Jahr 2016 geschaffen. Sie erstellt periodische und anlassbezogene operative Lagebilder zur staatlichen Cybersicherheit. Weiters ist sie für die Erarbeitung von Maßnahmen im Anlassfall sowie für die Unterstützung und Koordinierung gesamtstaatlicher Notfallmaßnahmen im Rahmen des Cyber Krisenmanagements (CKM) zuständig. Auch der “Innere Kreis der operativen Koordinationsstruktur” (IKDOK) nahm im Jahr 2016 seinen Betrieb auf.

Der IKDOK umfasst das Cyber Security Center des Bundesministeriums für Inneres und das Cyber Verteidigungszentrum des Bundesministeriums für Landesverteidigung sowie weitere staatliche Akteure und Einrichtungen. Im Konkreten zählen hierzu das Cyber Crime Competence Center (BMI), das Heeres-Nachrichtenamt (HNaA/BMLV), das Kommando Führungsunterstützung und Cyber Defence mit seinem MilCERT (KdoFüU&CD/BMLV), das GovCERT (BKA) sowie das BMEIA. Sowohl der IKDOK als die OpKoord haben mit Inkrafttreten des NIS-Gesetzes Ende 2018 einen klaren rechtlichen Rahmen bekommen.

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 Energie Computer Emergency Response Team (AEC) aufgebaut hat. Mehr Informationen zu AEC finden Sie aus 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.

CERT.at ist ebenfalls Mitglied der Central European Cyber Security Platform (CECSP). Im Rahmen der CECSP werden regelmäßig gemeinsame Übungen absolviert.

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. Neben anderer Task-Forces zu Spezialthemen,

[1] Die “Österreichische Strategie für Cyber Sicherheit”, siehe https://www.bmi.gv.at/504/start.aspx.

hat sich eine auf CERTs konzentrierte Plattform entwickelt. Arbeitsgruppen im Rahmen des TF-CSIRT arbeiten zeitlich beschränkt und auf Projektbasis zusammen. Mit Trusted Introducer (TI) entstand aus dem Netzwerk weiters eine wichtige Datenbank, die über die Vertrauenswürdigkeit und Seriosität von AkteurInnen 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 hat das Potential, neue Dynamik in die europäische IKT-Sicherheitslandschaft zu bringen, steht aber noch in seinen Anfängen.

Im Vordergrund des CSIRTs Network stehen Vertrauensaufbau, Kommunikation und der Aufbau von Expertise durch Zusammenarbeit. 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[2] und eine gemeinsame Taxonomie (siehe 2.2: Taxonomie) gesetzt.

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 von zwischen Sicherheitsteams in Bezug auf aktuelle Vorfälle, Gefahrenpotentiale sowie Projekt 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 EntscheidungsträgerInnen und die interne Vertrauensbasis zwischen den Beteiligten garantieren einen effizienten Austausch zu Problemlagen und neuen Entwicklungen.

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.

[2] Konkret unter anderem MISP und IntelMQ.

Das Netzwerk trifft sich zum einen bei der jährlichen internationalen Konferenz und zum anderen bei zahlreichen themen- oder regionsspezifischen Treffen.

3.4 Weitere Kooperationen

3.4.1 Connecting Europe Facilities (CEF)

Abschlussbericht "Strengthening the CERT Capacity and IT security readiness in Austria" (2016-AT-IA-0089)

CERT.at (mit Mutterfirma nic.at GmbH) hat beim Connecting Europe Facilities (CEF) Rahmenprogramm in der Kategorie "Cyber Security" im Jahr 2016 eine Förderung eingereicht. Ziel des 2016-AT-IA-0089 Programmes war es, vor allem nationale CERTs/CSIRTs fit für die NIS Richtlinie zu machen bzw. auf die NIS Richtlinie vorzubereiten.
Es war somit möglich, Schwachstellen (unter Betrachtung der (damals) kommenden NIS Richtlinie) zu identifizieren und zu adressieren.

Eine der größten Herausforderungen, die CERTs/CSIRTs (bzw. die gesamte IT Security Industrie) betrifft, ist das Fehlen qualifizierten Personals. Das "Handling" von Security Incidents für den gesamten "Österreich" Bezug im Internet (zur Definition siehe 2: Das IT-Sicherheitsjahr 2019) bedarf eigentlich immer mehr Personal, als vorhanden ist.
Demnach war einer der Schwerpunkte die Automatisierung des Incident Handlings. Hierbei werden alle möglichen Data Feeds von Vorfällen (fast immer Open Source Intelligence, manchmal werden die Feeds nur mit nationalen CERTs geteilt) gesammelt, geholt, vorverarbeitet, gefiltert und mit weiteren Informationen angereichert. Die so gewonnenen angereicherten und bereinigten Data Feeds werden anschließend nach Netzwerkbetreiber gruppiert und täglich an diese ausgeschickt. Weitere Informationen dazu finden sich auf unserer Webseite sowie in 2.4: Datenbasis.

Diese Automatisierung wurde im Rahmen des CEF Projekts im Zeitraum September 2017 bis September 2019 erfolgreich abgeschlossen. Alle Arbeiten wurden als Open Source auf der Plattform GitHub unter https://github.com/certtools/intelmq veröffentlicht und stehen damit allen CERTs/CSIRTs und anderen Interessierten zur Verfügung, vgl. dazu auch 2.5.1: IntelMQ. Dem nicht genug, unsere Arbeit wurde von vielen verwendet und es gibt derzeit weltweit etwa 200 Installationen von IntelMQ von denen wir wissen.

Weitere Aspekte des CEF-2016-3 Projektes waren mehr Mitarbeiter für CERT.at (zeitlich befristet), die Erstellung eines NIS Meldeportals, Server-Hardware, Reisen zur Vernetzung mit anderen CERTs/CSIRTs und Trainings für CERT.at Mitarbeiter.

CyberExchange (2017-EU-IA-0118)

Das von der europäischen Kommission unterstützte CyberExchange Projekt ist quasi das Erasmus-Äquivalent für nationale CERTs/CSIRTs der EU. MitarbeiterInnen 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 hat 2019 sowohl als sendende als auch empfangende Stelle an diesem Projekt mitgewirkt.

CERT.at entsandte im Oktober Sebastian Wagner im Rahmen eines "Technical Assistance Visits" für eine Woche an CERT.pl, das nationale CERT Polens. Beide Teams sind maßgeblich an der Entwicklung von Softwaretools zur automatisierten Verarbeitung von "IoCs" ("Indicators for Compromise", Verwundbarkeits- und Vorfallsdaten) beteiligt bzw. leiten sie. Während CERT.at die langjährige Open-Source Software IntelMQ betreut, hat CERT.pl deren Entwicklung "n6" (n6.readthedocs.io) 2018 als Open-Source freigegeben. Ziel des Besuches war es daher, sich gegenseitig über die Stärken und Schwächen, die unterschiedlichen Ausrichtungen und mögliche Synergien sowie Schnittstellen der beiden Projekte auszutauschen.

Der Besuch hat die Möglichkeiten zur Interoperabilität der Softwareprojekte und verwandter Programme gezeigt, was eine wertvolle Basis für die weitere Zusammenarbeit darstellt. Erste Früchte hat die Kooperation bereits getragen, da Anpassungen durchgeführt werden konnten, die den Weg für eine gemeinsame Nutzung einer Komponente frei gemacht haben.

Im November 2019 wurde Dimitri Robl von CERT.at für zwei Wochen zu CERT.hr, dem nationalen CERT Kroatiens, geschickt. Dort lernte er einerseits die Abläufe von Penetration-Tests kennen, da CERT.hr diese Service für gewisse Teile der kroatischen Contituency anbietet und andererseits bekam er einen Einblick in Planung, Ablauf und Ergebnisse der erfolgreichen Awarenesskampagne "Veliki Hrvatsi Naivci" ("Die großen kroatischen Naiven"). Zusätzlich tauschte er sich mit dem Incident Response Team von CERT.hr über Best-Practices und allgemeine Abläufe aus. Insgesamt hat der Aufenthalt das Vertrauen zwischen den beteiligten CERTs stark erhöht und das Ziel des Wissensaustauschs wurde voll erfüllt.

Außerdem kamen im November 2019 Jarosław Jedynak von CERT.pl und Raphaël Vinot von CIRCL[3] zu CERT.at. Beide sind ihrem Fokus nach Programmierer und es ging bei ihren Besuchen primär darum, wie die von CERT.at, CERT.pl und CIRCL entwickelte Software reibungslos zusammenarbeiten kann, damit alle CERTs die Tools der anderen einsetzen können.

Beim Besuch von CERT.pl ging es verstärkt um das gegenseitige Kennenlernen der Tools der jeweils anderen, um mögliche Synergien ausfindig und dadurch nutzbar zu machen.

Mit CIRCL konzentrierte sich die Arbeit auf die Interoperabilität von IntelMQ und MISP, da beide Projekte bereits von vielen CERTs/CSIRTs in Europa (und außerhalb) eingesetzt werden, d.h. wohldefinierte Schnittstellen zwischen den beiden sind nicht nur für CERT.at und CIRCL nützlich.

Kickoff "Enhancing Cybersecurity in Austria" (2018-AT-IA-0111)

CERT.at reichte im Jahr 2018 als Anschlussprojekt an "Strengthening the CERT Capacity and IT security readiness in Austria" (CEF 2016-AT-IA-0089) ein weiteres EU Projekt "Enhancing Cybersecurity in Austria" (2018-AT-IA-0111) im Rahmen des Connecting Europe Facilities (CEF) Program ein, das ebenfalls wieder in vollem Umfang genehmigt wurde und eine 75%-ige Förderung der Kosten durch die Europäische Union beinhaltet. Die geplante Laufzeit ist von September 2019 bis August 2021.

Ausgebaut werden unter anderem sowohl die personellen Ressourcen, Trainings, Code-Weiterentwicklungen sowie auch der Ausbau der Server- und Sicherheitsarchitektur von CERT.at.

[3] CIRCL ist das national CERT Luxemburgs.

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

Ein besonderer Fokus liegt auch in der Forschung (Data Science) und der Automatisierung von vorhandenen Daten und dem Ausbau der eigenen Datenquellen für das Incident Management unter Beteiligung des Research & Development Teams (“R&D”) der nic.at.

Zu guter Letzt wird auch die Weiterentwicklung von IntelMQ im internationalen Kontext und insbesondere auch in Kooperation mit CERT.pl’s “n6” Werkzeug gefördert.

3.4.2 Mitarbeit an Forschungsprojekten

InduSec

CERT.at nimmt am 2019 gestarteten Project InduSec der SBA Research teil. Dabei geht es vor allem darum, IT und OT in bezug auf Security auf einen gemeinsamen Level zu bringen. Mehr Informationen finden Sie auf der Webseite von SBA Research.

ACCSA (KIRAS)

CERT.at beteiligt sich an den **A**ustrian **C**yber **C**risis **S**upport **A**ctivities (ACCSA), die darauf abzielen, AkteurInnen im staatlichen Cyber-Krisenmanagement (CKM) auf Cyber-Krisen mit umfangreichen Schulungs-, Übungs- und Auswertekonzepten vorzubereiten und dadurch Reaktionszeiten und Fehlerraten im Falle einer echten Cyber-Krise zu verringern. Genaueres finden Sie auf der Webseite von KIRAS.

Kapitel 4

Rechtsgrundlage

4.1 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, BGBl. I Nr. 111/2018). Das NIS-Gesetz überträgt dabei Aufgaben, die sich aus der NIS-Richtlinie ergeben, auf bestehende Strukturen und regelt Zuständigkeiten für die mit der Umsetzung betrauten Behörden sowie deren Befugnisse. In diesem Zusammenhang nimmt der Bundeskanzler die strategischen und der Bundesminister für Inneres die operativen Aufgaben wahr. Im Anwendungsbereich des Gesetzes befinden sich Einrichtungen mit einer hohen Bedeutung für das Funktionieren des Gemeinwesens, weshalb ihre Netz- und Informationssysteme besonders schutzbedürftig sind. Dies betrifft zum einen Einrichtungen in den sieben Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur, zum anderen Einrichtungen, die bestimmte digitale Dienste zur Verfügung stellen sowie Einrichtungen der öffentlichen Verwaltung.

Auf Grundlage des NIS-Gesetzes nahm das Büro für strategische Netz- und Informationssystemsicherheit (“strategisches NIS-Büro”), welches im Bundeskanzleramt als Teil der Abteilung I/8 angesiedelt und für bestimmte Angelegenheiten im Zusammenhang mit der Umsetzung der gesetzlichen Verpflichtung aus der NIS-Richtlinie zuständig ist, seine Arbeit auf.

Als ein erster Meilenstein kann diesbezüglich die im April 2019 auf Antrag erfolgte bescheidmäßige Feststellung der Eignung und Ermächtigung von CERT.at als nationales Computer-Notfallteam im Sinne des NIS-Gesetzes genannt werden.

Ein weiterer Meilenstein erfolgte, als die auf Basis des NIS-Gesetzes erlassene “NIS-Verordnung” (Netz- und Informationssystemsicherheitsverordnung, kurz: NISV, BGBl. II Nr. 215/2019) am 18. Juli 2019 in Kraft trat. In dieser Verordnung legte der zuständige Kanzleramtsminister im Bundeskanzleramt im Einvernehmen mit dem Bundesminister für Inneres verschiedene essentielle Sachverhalte aus dem NIS-Gesetz näher fest. Dazu gehören nähere Regelungen zu den Sektoren, wobei insbesondere die wesentlichen Dienste und die Kriterien für die Parameter zu Sicherheitsvorfällen (“Meldeschwellenwerte”) definiert wurden. Ferner wurden in der NIS-Verordnung Kategorien und Maßnahmen hinsichtlich der Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste festgelegt.

Auf Grundlage der NIS-Verordnung nahm das strategische NIS-Büro im August 2019 die Ermittlung der Betreiber wesentlicher Dienste in den sieben Sektoren auf. Dabei werden die Betreiber zunächst in einem Vorverfahren mit einem sogenannten "Informationsschreiben" darüber informiert, dass sie aufgrund von Daten, die dem strategischen NIS-Büro beispielsweise infolge von durchgeführten Amtshilfeverfahren vorliegen, als Betreiber wesentlicher Dienste in Frage kommen. Die Unternehmen werden dadurch einerseits über die Aufnahme der Ermittlungen informiert, sollen andererseits aber auch die Gelegenheit erhalten, sich dazu zu äußern. Darüber hinaus werden über das Informationsschreiben mögliche grenzüberschreitende Bezüge erfragt, die in einem weiteren Ermittlungsschritt als Grundlage für die Aufnahme von Konsultationen mit anderen Mitgliedstaaten der EU verwendet werden, falls ein Betreiber wesentlicher Dienste seinen Dienst noch in einem anderen Mitgliedstaat bereitstellt. Ferner wird versucht, über die Informationsschreiben gewisse inter-sektorale Abhängigkeiten zu eruieren. In einem abschließenden Schritt wird auf Basis der im Vor- und Konsultationsverfahren erlangten Informationen der Bescheid erlassen, mit dem eine öffentliche oder private Einrichtung als Betreiber wesentlicher Dienste ermittelt wird.

Dem strategischen NIS-Büro kommt gesetzlich weiters die Vertretung von Österreich in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind, zu. So nimmt das strategische NIS-Büro unter anderem aktiv an den Arbeiten der NIS-Kooperationsgruppe teil und leitet dort beispielsweise Work Stream 8 über Cybersicherheit im Energiesektor. Hierbei kann als Erfolg die Annahme des umfangreichen Referenzdokuments über die Umsetzung der NIS-Richtlinie im Sektor Energie (CG Publication 03/2019 (PDF)) durch die NIS-Kooperationsgruppe im September 2019 hervorgehoben werden.

Neben diesen gesetzlichen Aufgabenbereichen lagen weitere Tätigkeiten, die das strategische NIS-Büros im Jahr 2019 verfolgte, insbesondere im Bereich der Informationstätigkeit. So wurde gemeinsam mit dem BMI eine NIS-Website (zu finden unter https://www.nis.gv.at) ins Leben gerufen, die als Anlaufstelle im Hinblick auf die NIS-Richtlinie und das NIS-Gesetz fungiert und die bei der Beantwortung häufiger Fragen helfen soll.

Des Weiteren wurden die Adressaten des NIS-Gesetzes bei der Umsetzung der gesetzlichen Vorgaben unterstützt, indem vier sogenannte NIS Fact Sheets im Jahr 2019 erstellt und auf der NIS-Website zur Verfügung gestellt wurden. Der NIS Fact Sheet 1/2019 (PDF) vom Jänner erläutert die Erwartungshaltung der Behörden im Hinblick auf die Kontaktstellen von Betreibern wesentlicher Dienste. Der NIS Fact Sheet 7/2019 (PDF) vom Juli bietet den qualifizierte Stellen eine Hilfestellung insbesondere im Antragsverfahren. Der NIS Fact Sheet 8/2019 (PDF) vom August erörtert die Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste näher und der NIS Fact Sheet 9/2019 (PDF) vom September dient als Umsetzungsleitfaden für Einrichtungen des Bundes bei der Festlegung der wichtigen Dienste sowie der Meldekriterien.