GovCERT Austria

CERT.at

Bericht Internet-Sicherheit Österreich 2020

Inhaltsverzeichnis

Impressum

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

Projektleitung: Dimitri Robl, BA, CERT.at

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

Illustrationen: Jana Wiese, BA

Herstellungsort: Wien, März 2021.

Vorwort: Ing. Clemens Möslinger, BA MSc (BKA)

Das vergangene Jahr war für uns alle durch die Pandemie geprägt. Über kein anderes Thema wurde so oft berichtet, nichts wurde so oft diskutiert und nichts hat unser aller Leben im vergangenen Jahr mehr beeinflusst, geprägt und bestimmt wie das Corona-Virus. Trotz dieses alles überdeckenden Themas sind die Bedrohungen und Risiken, vor allem auch im Cyberraum, nicht verschwunden. Vielmehr konnten sie im Schatten von Corona sogar wachsen und können durch die notwendig gewordene schnelle Digitalisierung noch mehr Schaden anrichten.

Ein Blick zurück auf das Jahr 2020 zeigt, dass die seit langem steigende Professionalisierung der Cyberangriffe einen Spitzenwert erreicht hat. Österreich ist seit den Angriffen auf das Außenministerium und auf Betreiber kritischer Infrastrukturen spürbar ins Zentrum der Aufmerksamkeit gewandert. Das Internet kennt keine Grenzen und verschont niemanden.

Der Anstieg an öffentlich bekannt gewordenen Fällen von Ransomware und die immer häufigeren Zuordnungen der Angriffe zu staatlichen oder staatlich unterstützten Gruppen zeigen, dass wir es mit gefährlichen GegnerInnen zu tun haben und Neutralität allein nicht schützt.

Umso wichtiger ist es, dass die Antwort auf diese Bedrohungen ebenso wirkungsvoll und professionell ist. Nachdem Ressourcen im Bereich der IT-Security immer schon knapp bemessen waren – vor allem, wenn man berücksichtigt, in wie viele Themen man gleichzeitig investieren muss – kann die Antwort nur aus einer Kooperation aller Kräfte – staatlich, privatwirtschaftlich und gesellschaftlich – bestehen. Operative Leistungsfähigkeit, gepaart mit strategischem Rahmenwerk erlauben uns, auch in diesen zwar unsicheren, aber chancenreichen Zeiten, bestens gerüstet und vorbereitet zu sein.

Von staatlicher Seite unterstützen wir diese Zusammenarbeit durch Beratung, durch die Cyber Sicherheit Plattform (CSP) und auch durch die Vorgabe von Regeln und Normen. Auch wenn diese nicht immer beliebt sind, sind sie immer noch das effektivste Mittel, um zumindest einen Mindeststandard in der Cybersicherheit garantieren zu können. Mit dem Netz- und Informationssystemsicherheitsgesetz ist es erstmals gelungen, eine zielgerichtete Diskussion zu Notwendigkeit und Ausmaß von rechtlichen Vorgaben im Cybersicherheitsbereich zu führen. Die aktuell in Verhandlung befindliche NIS-2-Richtlinie der EU versucht die Lektionen aus der ersten Version zu nutzen, um noch effektiver auf die Einhaltung der Mindestsicherheitsvorgaben zu achten.

Diese gesetzlichen Maßnahmen sind Grundvoraussetzung für die so wichtigen EU-weiten und nationalen Kooperationen, stellen sie diese doch auf rechtlich sichere Beine und erlauben die so wichtige enge Zusammenarbeit, insbesondere auf technisch-operativer Ebene national und EU-weit. Diese enge Kooperation in der Vorbeugung und Behandlung von Cybervorfällen, der Informationsaustausch, rechtzeitige Warnungen, das Sammeln von Erfahrungen und das Teilen von technischen Daten zu Angriffsmethoden und AngreiferInnenn – all das ist unerlässlich, wenn eine wirkungsvolle Antwort auf die Bedrohungen gegeben werden soll. Die CERTs und CSIRTs der EU sind dabei das Fundament, auf dem diese Kooperation aufgebaut ist und es soll mit der NIS-2-Richtlinie weiter verstärkt werden.

Der vorliegende Jahresbericht zeigt anhand von Zahlen und Fakten, dass das vergangene Jahr ein bisheriger Höhepunkt an Aktivitäten zum Schutz der digitalen Einrichtungen von Staat, Wirtschaft und Bevölkerung war. Die Pandemie hat uns unsere Abhängigkeit und die Kritikalität unserer digitalen Infrastruktur deutlich vor Augen geführt. Umso wichtiger ist ihr Schutz. Der Bericht zeigt, dass dies weitgehend gelungen ist, aber auch, wo Cyberkriminelle erfolgreich waren und wo trotz aller Bemühungen Angriffe nicht abgewehrt werden konnten. Er zeigt auch, welch hoher Einsatz aller Beteiligten, wie viel Arbeit und welche Ressourcen dafür notwendig waren.

Berücksichtigt man die Rahmenbedingungen, unter welchen im vergangenen Jahr gearbeitet werden musste, so kommt man nicht umhin festzustellen, dass es dennoch ein erfolgreiches Jahr für die österreichische Cybersicherheit war.

GovCERT Austria und CERT.at sind nicht alleine für diesen Erfolg verantwortlich, aber sie sind die zentralen Komponenten, ohne die alle anderen Anstrengungen weniger effektiv gewesen wären. Sie sind die Informationsdrehscheibe, ohne die eine Abwehr und ein Schutz nicht möglich wären. Zusammen mit vielen weiteren IT-Security-ExpertInnen in Österreich helfen sie, gleich einem Schild, Angriffe zu verhindern und deren Auswirkungen klein zu halten. Sie gemeinsam ermöglichen die sichere Digitalisierung unserer Infrastrukturen, unserer Wirtschaft und unseres Staates. Ihre Leistungen bleiben neben den Berichten zur Pandemie oft unbeachtet. Der Jahresbericht von GovCERT Austria und CERT.at soll das ändern.

Ich wünsche Ihnen viel Vergnügen bei der Lektüre.

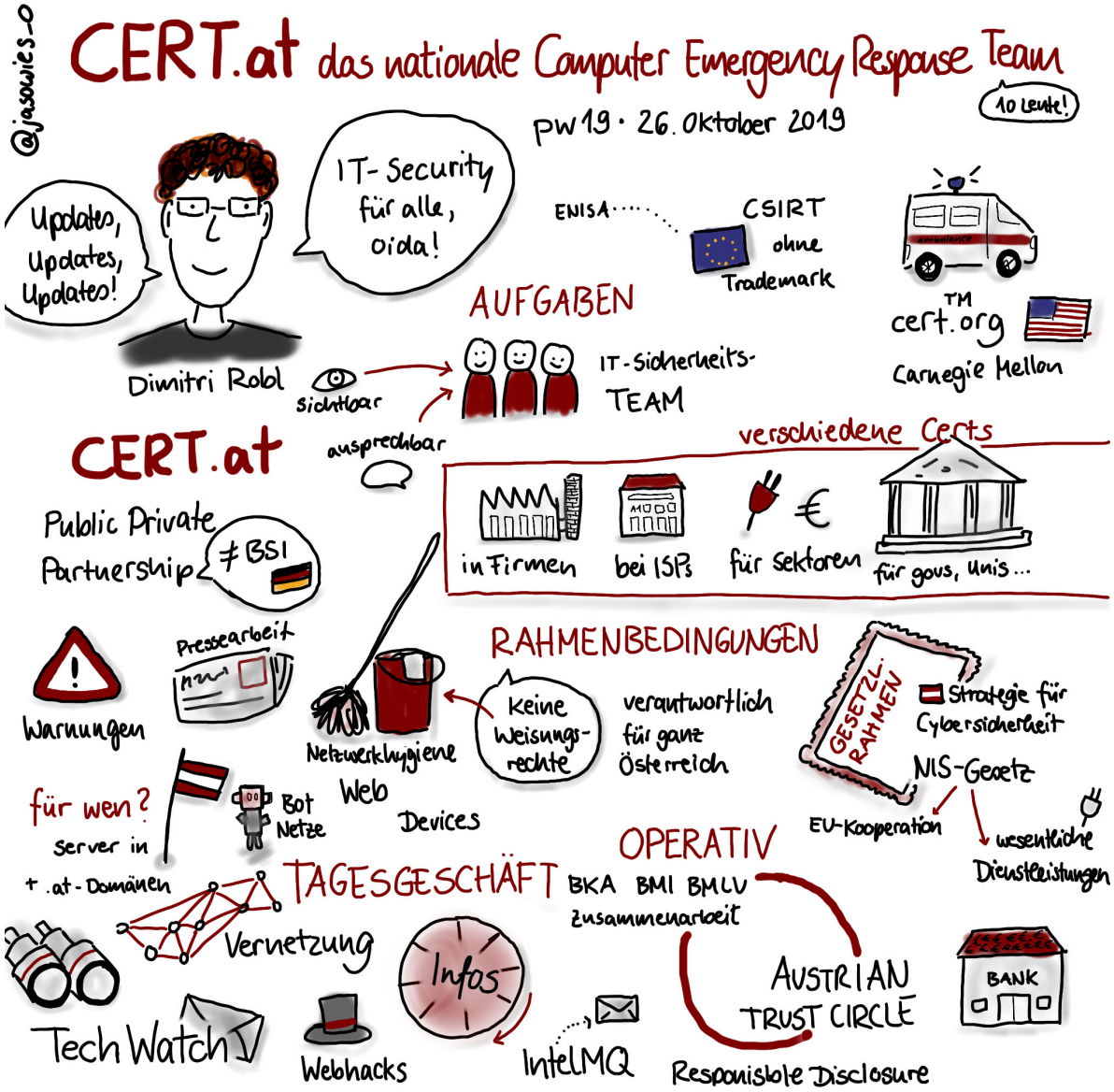


Abbildung 1: CERT.at bildlich dargestellt

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

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

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

Darüber hinaus ist CERT.at auch für vorbeugende Maßnahmen, wie Früherkennung, 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 14 Personen und wird von Robert Schischka als Geschäftsführer und Wolfgang Rosenkranz als Teamleiter geleitet. Eine wichtige Abgrenzung: CERT.at ist keine Ermittlungsbehörde und befasst sich da-

her 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 Themenvorschläge 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 NetzbetreiberInnen und zuständigen Security Teams in Kontakt tritt. Ein ExpertInnen-Team, das im Falle des Falles Hilfe zur Verfügung stellt und in enger Abstimmung mit anderen Beteiligten den österreichischen Teil des Internets von Problemen befreit – auf Basis eines freiwilligen Angebots.

Die Zusammenarbeit mit anderen Organisationen ist daher ein wichtiger Bestandteil der täglichen Arbeit von CERT.at: Diese reicht von der EU-Agentur für Cybersicherheit ENISA, internationalen Konzernen, über CERTs/CSIRTs in anderen Staaten, anderen Sicherheitsteams in Österreich, Universitäten, Fachhochschulen, Forschungseinrichtungen bis hin zu engagierten Privatpersonen. 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 dar, innerhalb dessen jedes Land Kapazitäten für die Cyber-Sicherheit aufbauen muss. Zudem formuliert sie Mindestsicherheitsanforderungen und Meldepflichten für kritische Infrastrukturen und für das Angebot bestimmter digitaler Dienste wie Cloud-Services oder Online-Marktplätze.

Österreich hatte bereits 2013 eine IT-Sicherheits-Strategie vorgestellt, die viele Punkte der Richtlinie vorwegnahm. Eines ist jedoch neu: Die Richtlinie verlangt von jedem Land, dass es ein offizielles Computer-Notfallteam einrichtet. Damit hat das BKA als zuständige NIS-Behörde im April 2019 CERT.at betraut und einen gesetzlichen Auftrag erteilt, ohne dessen 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 Vorstellung des neuen Teamleiters Wolfgang Rosenkranz

CERT.at ist seit seiner Gründung im Jahr 2008 stetig gewachsen. Neben der Rolle als Informationsdrehscheibe und als Unterstützung bei Incident Response Einsätzen hat CERT.at beispielsweise in den letzten Jahren eine wichtige Rolle in der Entwicklung neuer Werkzeuge zur Unterstützung internationaler Kooperationen im Bereich der Cybersicherheit übernommen. Die administrativen Aufgaben und die Personalkoordination, die mit dem Wachstum verbunden waren, haben es deshalb notwendig gemacht, personell aufzustocken. Im November 2020 war es dann so weit und ich durfte meinen Dienst als neuer Teamleiter von CERT.at antreten. Otmar Lendl, der bisherige Teamleiter und seit der Gründung von CERT.at mit an Bord, ist weiterhin unverändert in seinen vielen Rollen als Experte und Sprachrohr der Organisation tätig, hat aber die zusätzlich entstandenen Aufgaben an mich übergeben.

Ich sehe mich nach vielen Berufsjahren inzwischen als Veteran der Sicherheitsbranche. Nach der Ausbildung zum Milizoffizier und dem Berufseinstieg als Softwareentwickler und Systemadministrator für ein Sicherheitsunternehmen, wechselte ich 2003 zur Staatsdruckerei, wo ich für die Konzeption und die Einführung des Reisepasses mit Chip mitverantwortlich war. Im Jahr 2011 war wieder eine Veränderung angesagt, diesmal zur Repuco Unternehmensberatung, in der ich zuletzt als Geschäftsführer tätig war. Mein Hauptaufgabengebiet war dabei die Betreuung und Unterstützung des Kuratorium Sicheres Österreich (KSÖ), das mit seinen Cybersecurity Planspielen, dem Rechts- und Technologiedialog zum NIS-Gesetz und vielen weiteren Projekten maßgeblich dazu beigetragen hat, dem Thema Cybersicherheit auf der Ebene der Entscheidungsträgerinnen und Entscheidungsträger mehr Aufmerksamkeit zu verschaffen.

Das Thema "Sicherheit" hat mich also seit frühen Jahren begleitet und geprägt, weshalb ich den Wechsel zu CERT.at auch als Ergebnis einer langen Reise ansehe. Die primäre Aufgabe von CERT.at wird sich durch mich nicht verändern: wir informieren, wir unterstützen und wir beraten, wenn es um den Schutz des Internet vor Bedrohungen und Sicherheitsrisiken geht. Die Erweiterung des Teams ist aber ein deutliches Signal dafür, dass CERT.at erwachsen geworden ist. Die Erwartungshaltung an uns ist hoch und es ist klar, dass man uns braucht. Wir müssen uns deshalb laufend weiterentwickeln und ich freue mich darauf, bei dieser spannenden Aufgabe Teil des Teams zu sein.

Wolfgang Rosenkranz

1.2 GovCERT Austria – Expertise im Behördenbereich

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

Auf internationaler Ebene agiert GovCERT Austria als österreichische Kontaktstelle für Regierungen und internationale Organisationen bei Fragen der IKT-Sicherheit. Es tauscht Informationen und Warnungen mit diesen aus und leitet sie bei Bedarf an inländische 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 Bekanntmachungen über Risiken und Vorfälle heraus. Es reagiert auf Sicherheitsvorfälle, unterstützt bei Bedarf auch vor Ort und erweitert sein Wissen und Netzwerk durch die Koordination und Teilnahme an nationalen und internationalen Cyber-Übungen.

1.2.1 Public-Private-Partnership mit vielen Vorteilen

Da das GovCERT als Public-Private Partnership (PPP) des Bundeskanzleramtes mit nic.at eingerichtet wurde und auf das gleiche technische Team wie CERT.at zurückgreift, erhält der Staat Zugriff auf qualifizierte, technische Cybersicherheitsexpertise aus dem Privatsektor sowie auf das Kontaktnetzwerk von CERT.at, welches nationales und internationales Know-how und relevante Sicherheitsinformationen (z.B. klassifizierte Dokumente, White Papers usw.) bereithält. Hinzu kommt die Mitarbeit an und das Teilen von gesamtstaatlichen Cyberlagebildern im Rahmen von OpKoord[1] und IKDOK[2] und die Teilnahme an 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 Ransomware).

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

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

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 Austria neben selbst entwickelter Sensorik auf Quellen innerhalb der internationalen Gemeinschaft der IT-Sicherheitsbranche.[3] Ziel ist es, das Niveau der Netzwerksicherheit in Österreich durch die Übermittlung von Informationen über Sicherheitsprobleme an Betroffene laufend zu heben.

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

1.4 Zertifizierungen 2020

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.

nic.at wurde bereits im Jahr 2014 ISO 27001 zertifiziert. Gemeinsam beschloss man im Zuge des ersten großen Re-Audits von nic.at (nach drei Jahren) auch die Zertifizierung von CERT.at und GovCERT Austria anzustreben. Eine gemeinsame Zertifizierung von nic.at und CERT.at im

[3] Eine ausführliche Beschreibung der verwendeten Quellen findet sich in 2.5 Tooling.

Jahr 2014 wäre wegen der unterschiedlichen Anforderungen und getrennten Systemen zu aufwendig gewesen. Der notwendige Prozess und alle Maßnahmen zur ISO-Zertifizierung von CERT.at und GovCERT Austria wurden im Jahr 2017 erfolgreich abgeschlossen. 2020 wurden weitere Maßnahmen gesetzt, um das Sicherheitsniveau auch künftig zu erhalten.

1.4.2 TI Zertifizierung

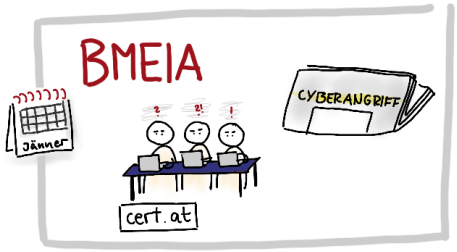
Das **Trusted Introducer (TI) Service** ist eine Einrichtung des europäischen Verbands der CSIRTs (TF-CSIRT), die die Vertrauenswürdigkeit und den Reifegrad von Teams im europäischen CERT-Netzwerk mithilfe der Stufen “listed”, “accredited” und “certified” dokumentiert. Wer in der TI-Datenbank aufscheint,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

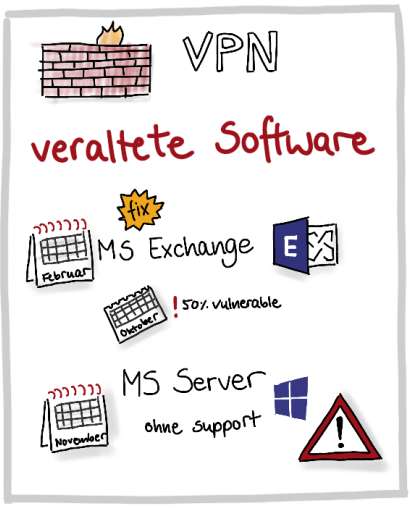
Im Jahr 2017 hat CERT.at den Schritt von der TI-Akkreditierung hin zur Zertifizierung gemacht. Dieser Prozess, der durch das TF-CSIRT-Netzwerk und damit die Branche selbst durchgeführt wird, überprüft die Organisation, die internen Sicherheitsmaßnahmen und Arbeitsprozesse des betroffenen CERTs anhand des international anerkannten SIM3 Reifegradmodells. CERT.at konnte diesen Prozess erfolgreich abschließen und ist (mit Stand 2020) eines von neun nationalen CERTs in Europa, das mit dem TI-Prädikat “Certified” ausgezeichnet wurde. Das ist die höchste Stufe des Trusted Introducer Zertifizierungsrasters. Das GovCERT wird als “listed” geführt.

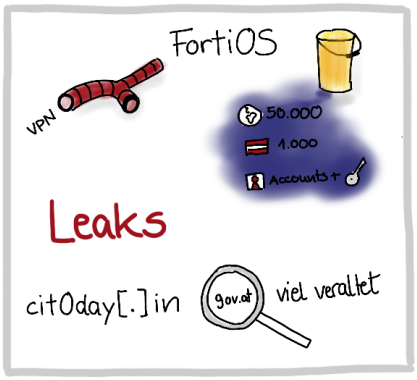
@jasowies_0

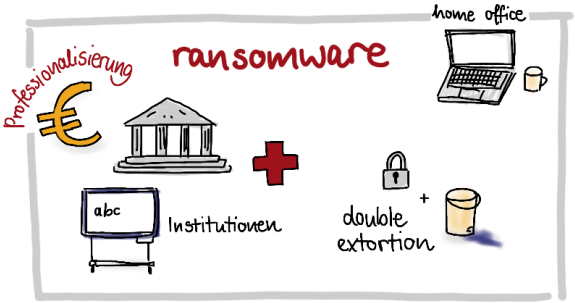
Das IT-Sicherheitsjahr 2020

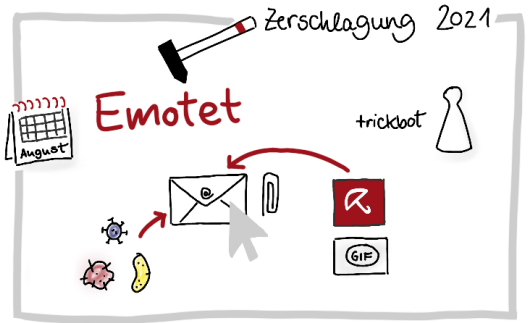
CERT.at











Kapitel 2

Das IT-Sicherheitsjahr 2020

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.

2.1 Incident Reports, Incidents und Investigations

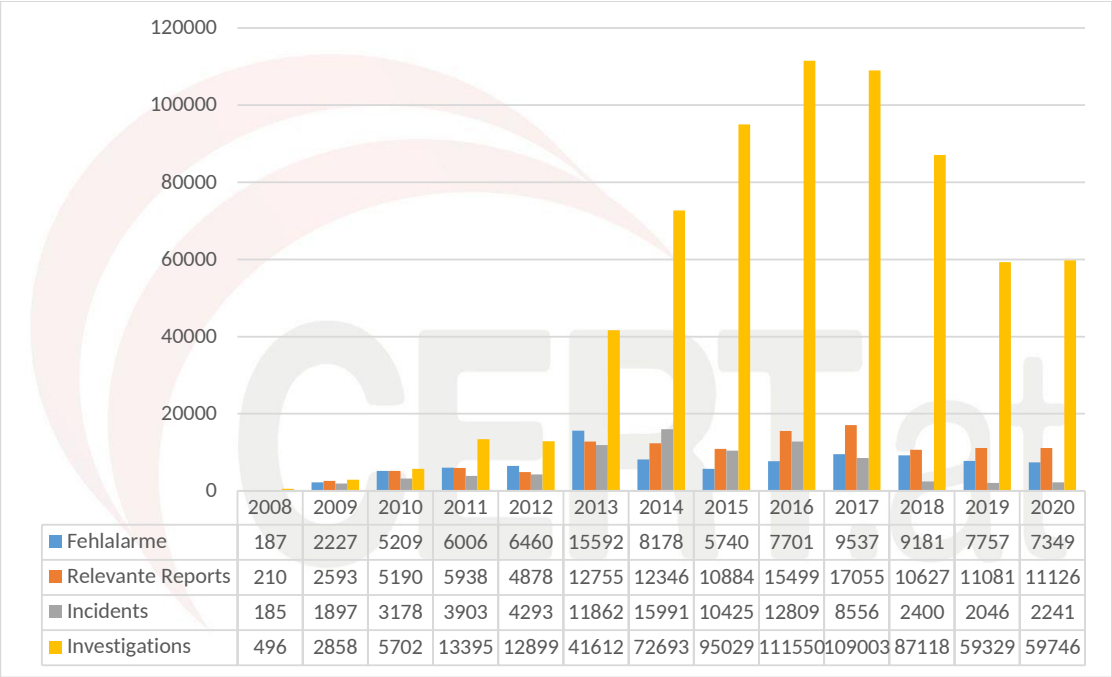
Eingehende und ausgehende Informationen werden bei CERT.at und GovCERT Austria über ein Ticketsystem (aktuell Request Tracker for Incident Response a.k.a. RTIR) abgehandelt. Dabei wird bei Vorfällen zwischen Incident Reports, Incidents und Investigations unterschieden:

Incident Reports sind Meldungen über Sicherheitsprobleme oder -vorfälle, die bei CERT.at eingehen. Diese werden anschließend als relevant, informativ oder als Fehlalarm kategorisiert. Als "informativ" sieht CERT.at Meldungen an, bei denen eine Weiterverarbeitung aufgrund verschiedener Faktoren nicht sinnvoll ist; beispielsweise Hinweise auf Opfer von bereits geschehenen DDoS Angriffen. Hier ist es nicht hilfreich, die Betroffenen über vergangene Attacken zu informieren, die sie aller Wahrscheinlichkeit nach ohnehin bemerkt haben.
Incident Reports können sowohl von automatisierten Datenfeeds (siehe 2.4 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	2020
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701	9537	9181	7757	7349
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055	10627	11081	11126
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556	2400	2046	2241
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003	87118	59329	59746

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 also in einem Monat ähnlich viele Incidents unter den Kategorien “vulnerable” und “malicious code” haben, sagt dies erst einmal nichts über die Anzahl der zugehörigen Incident Reports und Investigations aus.

Dadurch erklärt sich auch der Umstand, dass die Top 5 nicht identisch sind.

Ein Beispiel (mit erfundenen Zahlen): Wir erhalten an einem Tag aus acht verschiedenen Quellen Incident Reports zu offenen DNS Resolvern (Taxonomie “vulnerable”) und aus einer Quelle Incident Reports zu 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 2.4 Datenbasis näher eingegangen.

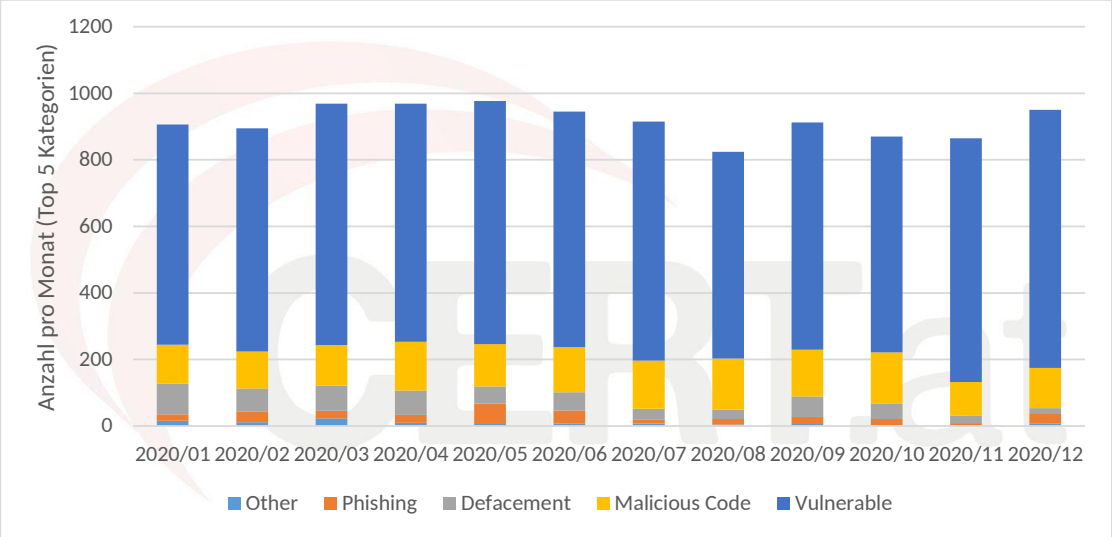


Abbildung 2.2: Top 5 Incident Reports Kategorien

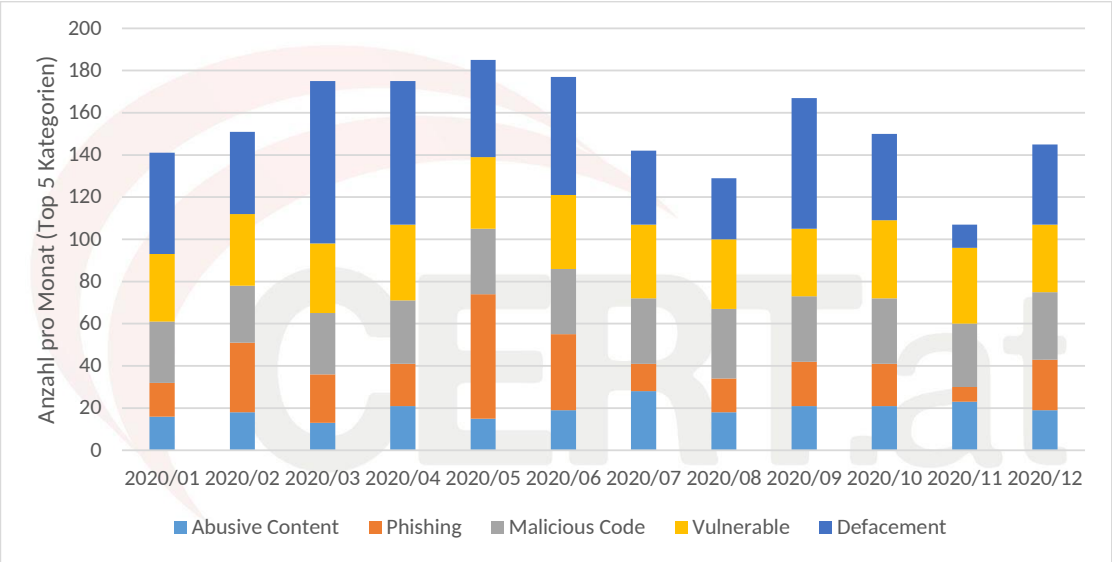


Abbildung 2.3: Top 5 Incident Kategorien

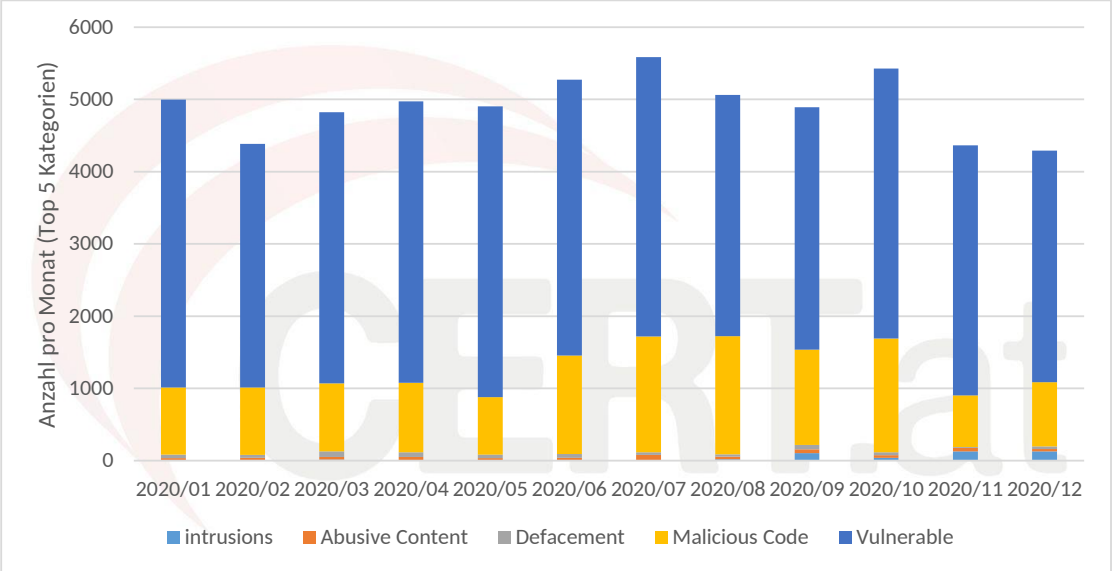


Abbildung 2.4: Top 5 Investigation Kategorien

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 dieser Taxonomie sind nicht exklusiv, d.h. mehrere Kategorien können auf einen Vorfall zutreffen.

In Bezug auf Probleme mit Webservern verwendet CERT.at eine noch genauere Aufspaltung der einzelnen Kategorien, siehe dazu 2.3.2 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 insgesamt einer Überarbeitung bedarf.

Test: Für Testfälle.

2.3 2020 im Detail

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

Im Verhältnis zu den Aussendungen ist zweierlei zu beachten:

1. CERT.at schickt Informationen zum gleichen Problem nur alle 30 Tage aus. Das heißt also, auch wenn wir jeden Tag die Information erhalten, dass auf IP Adresse X Port Y offen ist, obwohl er das wahrscheinlich nicht sein sollte, schicken wir das nicht täglich weiter, um die 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), leiten wir diese Informationen aggregiert an die Verantwortlichen weiter, d.h. hinter einer einzelnen Investigation können zahlreiche Datenbankeinträge a.k.a. “Events” stecken.

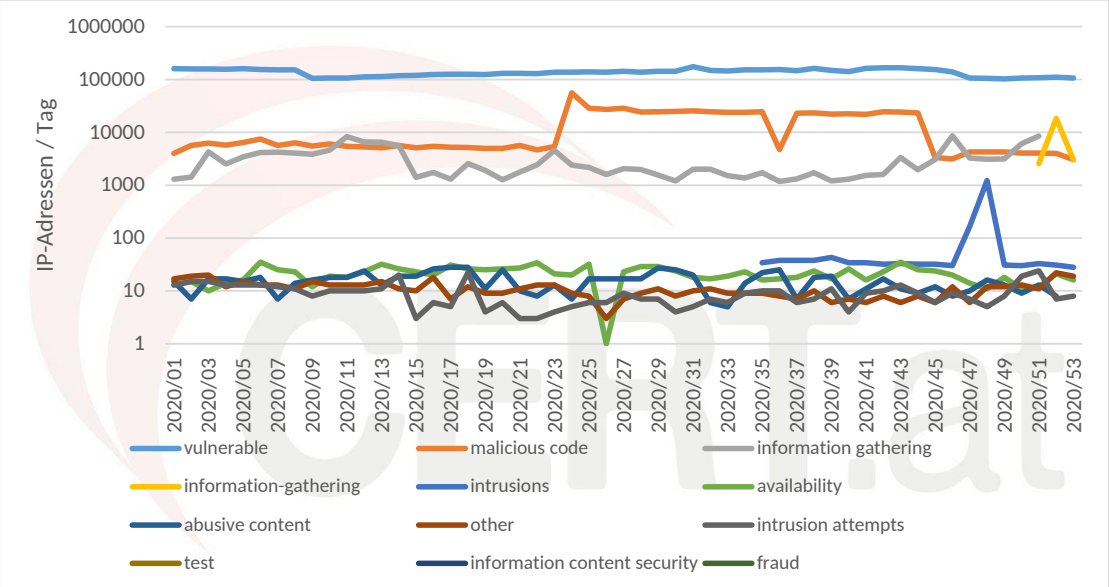


Abbildung 2.5: Events nach Taxonomie (logarithmische Skala)

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

[2] Für eine genauere Beschreibung siehe 2.4 Datenbasis.

Außerdem ist Abbildung 2.5 zu entnehmen, dass wir im letzten Jahresdrittel 2020 erstmals Feeds der Taxonomie “intrusions” in unsere regelmäßigen Benachrichtigungen aufnahmen, was bisher auf anlassbezogene Aussendungen beschränkt war.

2.3.1 Taxonomie “vulnerable”

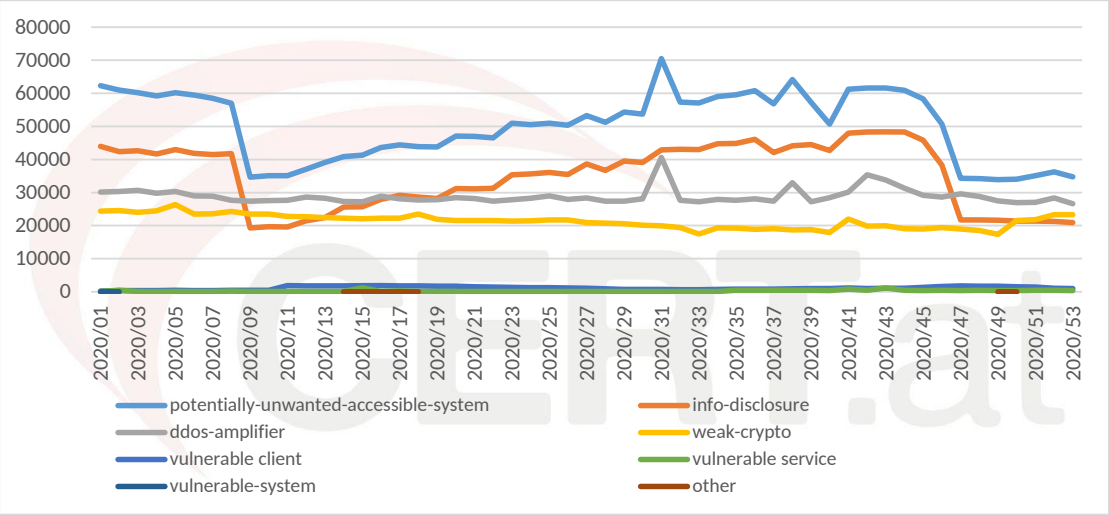


Abbildung 2.6: Alle Events der Taxonomie “vulnerable”

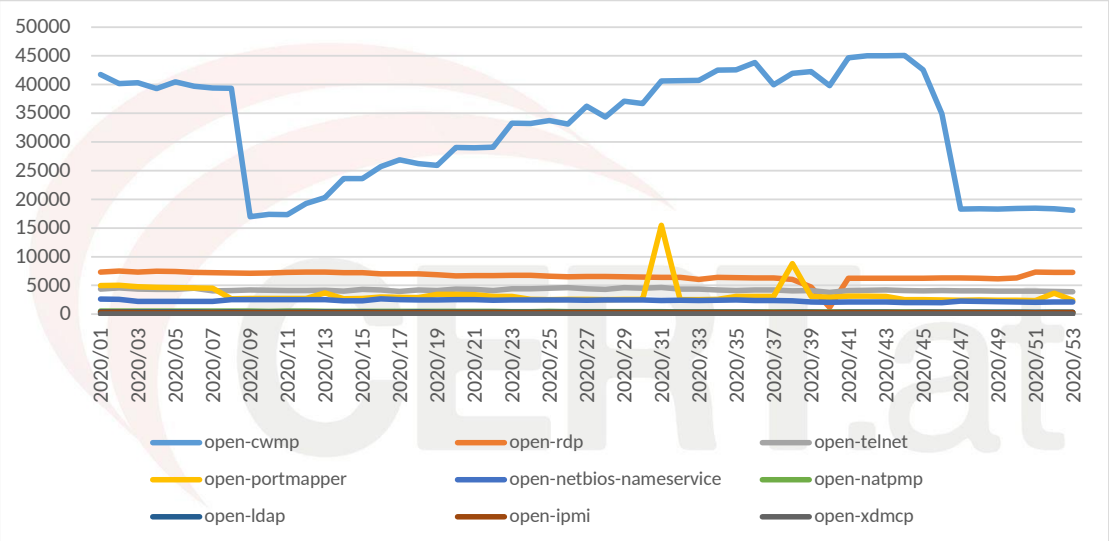


Abbildung 2.7: Ports, die nicht öffentlich erreichbar sein sollten

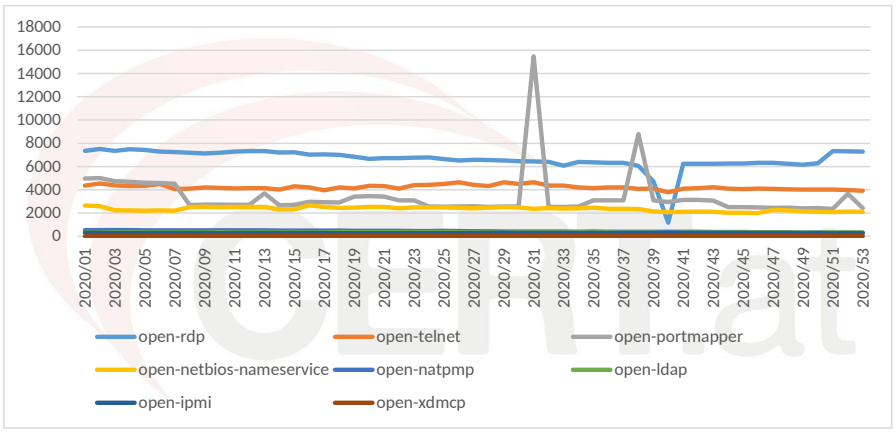


Abbildung 2.8: Wie Abbildung 2.7 aber ohne CWMP

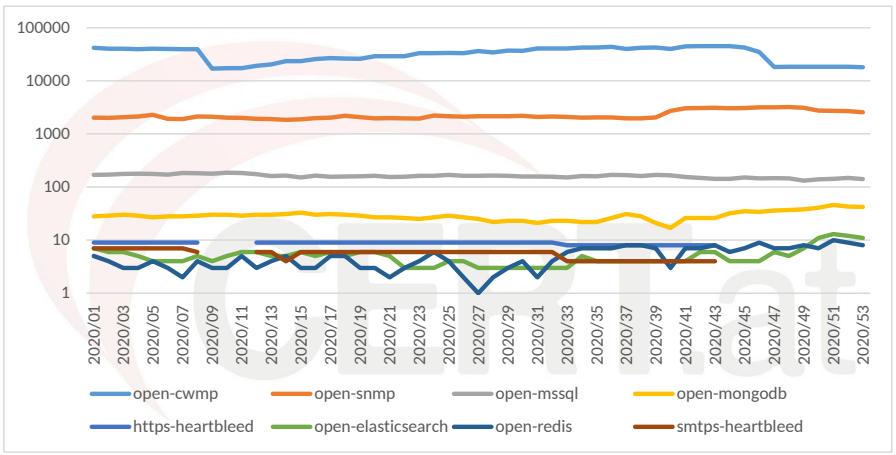


Abbildung 2.9: Services, über die sensible Informationen gewonnen werden können

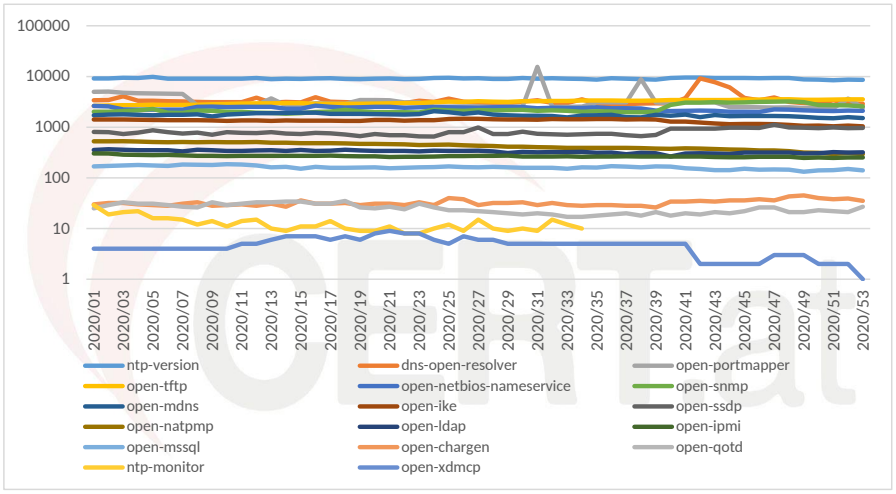


Abbildung 2.10: Geräte, die für UDP DDoS Amplifikation missbraucht werden können

Wie auch in den Jahren zuvor, fiel 2020 der größte Teil der von uns behandelten Meldungen in die Kategorie “vulnerable”, weshalb wir sie etwas näher vorstellen.

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

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

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

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

Wie Abbildung 2.6 zeigt, sind innerhalb der Taxonomie “vulnerable” wiederum wenige Unterkategorien für den Großteil der Events verantwortlich. Am Verlauf der Kurven lässt sich auch die in 2.3 2020 im Detail erwähnte doppelte Zählung bestimmter Events gut veranschaulichen: “`open-cwmp`”[3] fällt sowohl unter “potentially-unwanted-accessible-system” (vgl. Abbildung 2.7) als auch unter “info-disclosure” (vgl. Abbildung 2.9) und beeinflusst aufgrund seiner Häufigkeit beide Kurven sehr stark. Für die Spitze zwischen den Wochen 31 und 33 wiederum ist “`open-portmapper`”[4] verantwortlich, der ebenfalls in beide Kategorien fällt.

Shodan “Verified Vulnerabilities”

Im Jahr 2020 veröffentlichte die Suchmaschine Shodan ein neues Feature zur Schwachstellenanalyse. Diese “Verified Vulnerabilities” zeigen ihrem Namen entsprechend Schwachstellen an, die Shodan gefunden und verifiziert hat.[5] Diese Funktionalität ist nur für eine begrenzte Anzahl von IP Adressen anwendbar; im Falle von CERT.at sind das all jene, die in Österreich geolokalisiert sind.

Nach einigen Tests haben wir im September 2020 damit begonnen, einmal im Monat die aggregierten Daten aus dieser Quelle zu veröffentlichen und die Änderungen zu den Vormonaten zu besprechen. Der initiale Blogpost vom September findet sich hier, die nachfolgenden Entwicklungen für 2020 in den Posts zu Oktober, November und Dezember.

Bisher zeichnet sich ab, dass die Unterschiede zwischen den Monaten relativ gering sind und sich das Gesamtbild ingesamt bisher kaum verändert hat: Die zahlenmäßig größten Schwachstellen sind FREAK und Logjam, beides Schwachstellen in SSL/TLS Bibliotheken aus dem Jahr 2015, die potentiell das Entschlüsseln von HTTPS-Verbindungen ermöglichen, gefolgt von RCE

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

[4] Genauere Informationen dazu finden Sie unter https://cert.at/de/services/daten-feeds/vulnerable/#open-portmapper.

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

("Remote Code Execution") Schwachstellen in älteren Versionen von Microsoft Windows und RDP ("Remote Desktop Protocol").

Eine erfreuliche Erkenntnis aus diesen Daten ist, dass, obwohl die Anfang 2020 für einigen Aufruhr verantwortliche Lücke CVE-2019-19781 a.k.a. "Shitrix" zwar enthalten ist, die Anzahl der nach wie vor verwundbaren Server in Österreich sich aber im niedrigen einstelligen Bereich bewegt.

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 im Web nicht immer gut funktioniert, ist, dass es in vielen Fällen um die Beurteilung der Legitimität von Inhalten geht. So ist der Schriftzug "defaced by" zwar eine Phrase, sie sehr häufig bei Defacements (s.u.) auftritt, aber gleichzeitig oft auf Seiten von Museen oder Ausstellungen vorkommt, auf denen Kunstwerke beschrieben werden, die irgendwann "defaced", d.h. verunstaltet bzw. mutwillig beschädigt wurden. Hin und wieder treffen wir sogar auf Webseiten, bei denen sich im Nachhinein herausstellt, dass der augenscheinliche Hack eine Kunstinstallation ist, die ein Defacement imitiert oder eine angebliche Phishing-Seite in Wahrheit Teil eines gerade laufenden Pentests ist.

In Abbildung 2.11 finden Sie einen Überblick zu den verschiedenen Angriffen auf Webseiten, von denen CERT.at Kenntnis hat.

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.

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

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.

Dass die Anzahl der Phishings relativ stark schwankt, ist unter anderem mit dem Kampagnencharakter solcher Angriffe zu erklären: Kriminelle kompromittieren vor dem Aussenden

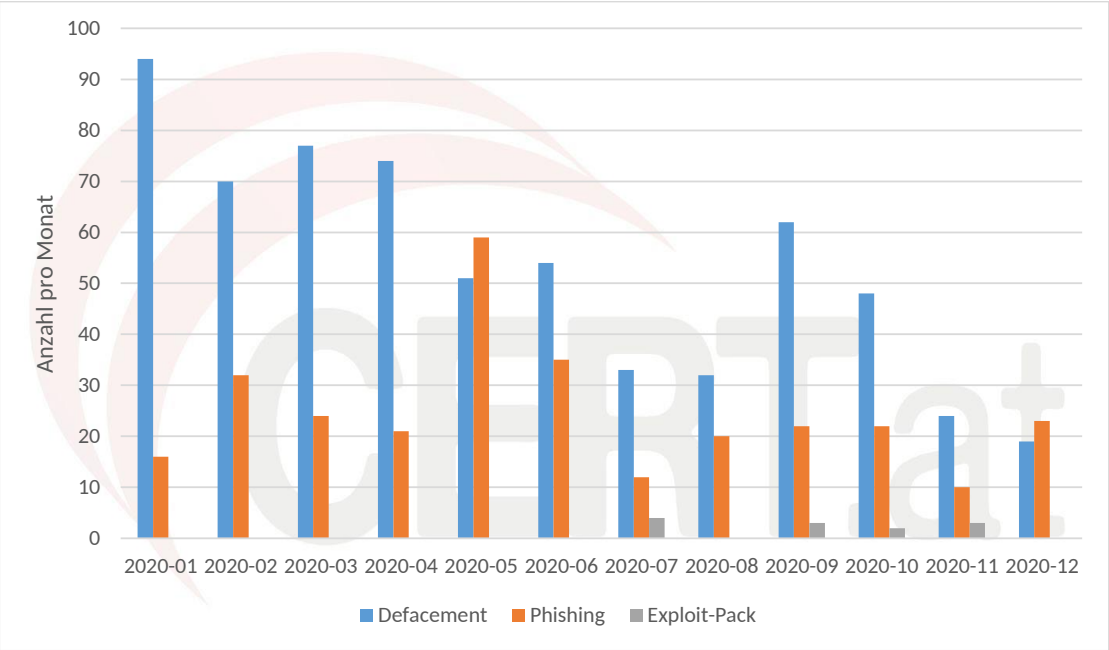


Abbildung 2.11: Gehackte Webseiten

der Phishing-Mails gleich eine größere Anzahl von Webseiten, damit das Bereinigen einzelner Phishingseiten nicht direkt den gesamten Angriff beendet. Nach dem Beginn einer solchen Kampagne gehen dann oft viele Meldungen zu Phishing-Seiten auf einmal ein.

Exploit Packs

Bei diesem Angriff 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.

Das Positive an Abbildung 2.12 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 primär ein positiver Trend zu weniger betroffenen Servern ab.

Dass veraltete TLS-Software einen großen Teil der öffentlich sichtbaren Schwachstellen ausmachen, konnten wir 2020 auch mithilfe der Shodan “Verified Vulnerabilities” bestätigen.

Die sehr kurzen Linien zu `2020-02-05-tlsversion` und `2020-02-24-deprecated-tls` beziehen sich auf zwei von uns durchgeführte Scans zu TLS Versionen, da die großen Browser-

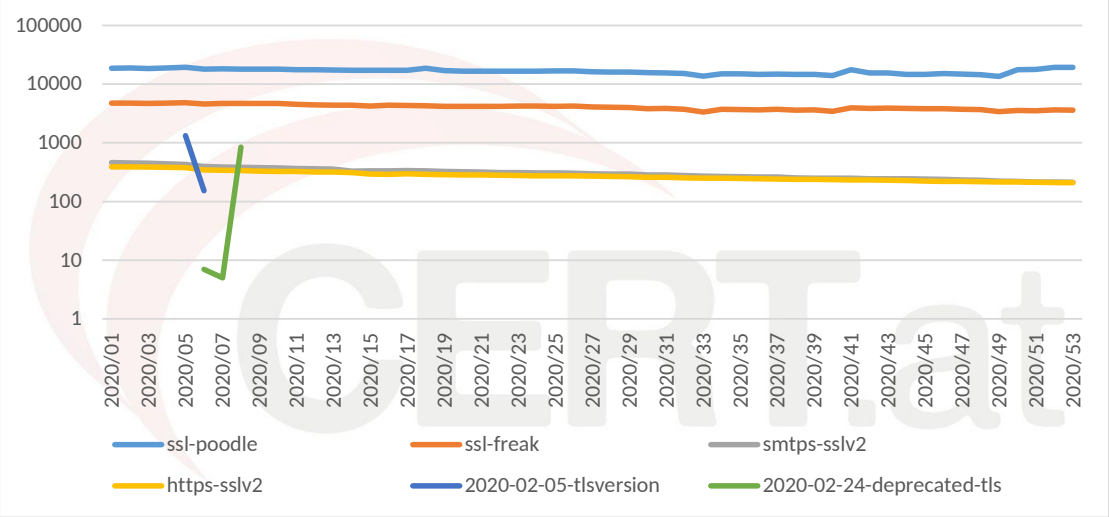


Abbildung 2.12: Web- und Mailserver mit veralteter Kryptographie

Firmen angekündigt hatten, die Unterstützung von TLS Versionen unter 1.2 im März 2020 einzustellen.[6] Das bedeutete, dass Webseiten, deren Server nicht mindestens TLS 1.2 unterstützten, ab diesem Zeitpunkt nicht mehr von NutzerInnen mit modernen Browsern hätten besucht werden können. Wir nahmen diesen Umstand zum Anlass, alle `.at` Domains auf ihre TLS-Version zu prüfen und informierten BetreiberInnen, deren Webseiten nach einer solchen Umstellung quasi nicht mehr erreichbar gewesen wären.

2.3.4 Malware

Malware war 2020, wie jedes Jahr, sehr aktiv. Über die aktivsten und gefährlichsten Varianten wird in 2.6 Bedrohungen 2020 genauer eingegangen.

Dabei ist zu betonen, dass diese in Abbildung 2.13 nicht enthalten sind, da es zu ihnen keine Feeds gibt, die Infektionen mit z.B. Emotet anzeigen. Der Grund hierfür ist, dass die meisten Feeds mit sog. “Sinkholes” arbeiten, d.h. Strafverfolgungsbehörden, ResearcherInnen oder Firmen betreiben einen Server auf IP-Adressen oder Domains, zu denen sich die Schadsoftware entsprechend ihrer Programmierung verbindet, um Befehle zu erhalten.

Das funktioniert aber natürlich nur, wenn die Infrastruktur der Kriminellen übernommen oder emuliert werden kann, was bei aktiver und regelmäßig weiterentwickelter Malware wie Emotet kaum der Fall ist.

Mit Beginn der COVID-19 Pandemie bot die Firma Bitsight einen ihrer sonst kostenpflichtigen Feeds für einige Monate kostenlos zu Evaluationszwecken an, was den großen Anstieg in der Grafik zwischen den Kalenderwochen 23 und 45 erklärt. Der Einbruch in KW 37 ist auf ein technisches Problem bei Bitsight zurückzuführen.

Nach Ablauf der kostenlosen Evaluationsphase haben wir uns dazu entschlossen, den Feed nicht käuflich zu erwerben, da er für unsere Zwecke zu viele False Positives enthielt. Für Firmen, die damit vor allem ihre eigenen Netze überwachen, dürfte die Anzahl zwar kaum ein Problem darstellen, bei unserer Arbeit kam es aber zu zahlreichen Rückfragen und verärgerten Netzbe-

[6] Siehe z.B. unseren Blogpost dazu.

treiberInnen.

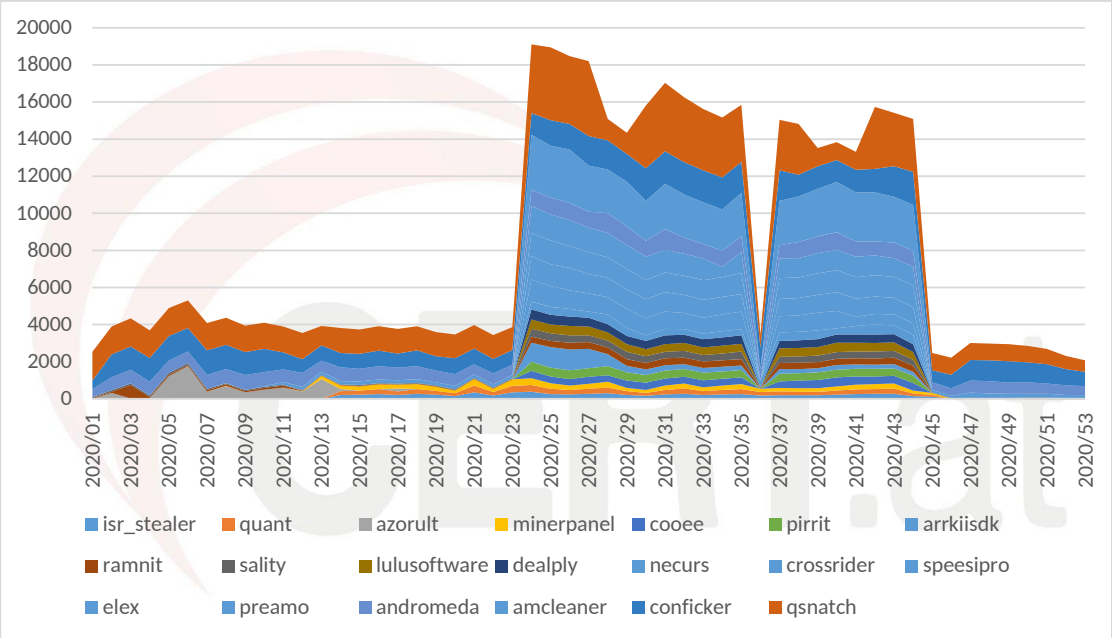


Abbildung 2.13: Malware in Österreich

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,[7] 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.

2020 führte CERT.at folgende Scans regelmäßig durch:

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

Dazu kamen einige einmalige bzw. unregelmäßige Scans. Diese sind auf der oben verlinkten Webseite genauer beschrieben. Hervorzuheben ist der Scan nach Microsoft Exchange Servern, die für CVE-2020-0688 anfällig sind, eine Lücke die es ermöglicht, beliebige Befehle mit Administrationsrechten über das Netzwerk auszuführen. Die einzige Voraussetzung dafür sind gültige Zugangsdaten zu einem beliebigen Mailbox-Account auf dem Server.

2.4.2 Externe Quellen

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

[7] 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[8] 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[9] 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

[8] 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.

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

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 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

Das Projekt

Gestartet wurde der Entwicklungsprozess von IntelMQ[10] 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.

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

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.

IntelMQ 2020

Anfang 2020 wurde ein Tutorial für IntelMQ auf GitHub veröffentlicht und in einem Workshop des TF-CSIRT auch gleich getestet. Über das Jahr hinweg wurde es kontinuierlich aktualisiert und verbessert; Feedback ist natürlich gern gesehen.

Außerdem wurde 2020 auch erstmals eine Schwachstelle im IntelMQ Manager, einer graphischen Managementoberfläche für IntelMQ, gefunden, die mit einer CVE-Nummer versehen wurde. CVE-2020-11016 ermöglicht(e) AngreiferInnen, beliebigen Code mit den Rechten des Web-Services auszuführen. Die Lücke wurde mit Version 2.1.1 von IntelMQ Manager behoben. IntelMQ Manager ist eigentlich nicht dazu gedacht, aus dem offenen Internet erreichbar zu sein, weshalb die Anzahl erreichbarer und verwundbarer Instanzen relativ klein war. Dennoch haben wir damals weltweit nach ebensolchen gescannt und die Betroffenen benachrichtigt.

Im Juli 2020 erschien dann mit Version 2.2.0 der erste größere Feature-Release in diesem Jahr, in dem die Unterstützung von Python 3.4 entfernt wurde. Außerdem waren zahlreiche Fehlerkorrekturen sowie neue Funktionen enthalten, darunter sechs komplett neue sowie sieben wesentlich überarbeitete Bots.

Im Dezember erschien mit Version 2.2.3 kurz vor Weihnachten der letzte Release 2020 und brachte neben einigen Bugfixes auch RPM-Pakete für CentOS 8 mit sich.

Eine Übersicht zu den Releases findet sich auf GitHub.

Eine weitere wichtige Veränderung des Projekts im Jahr 2020 war der im November erfolgte Umzug der Dokumentation auf https://intelmq.readthedocs.io/ und damit auf Sphinx.

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.

2020 wurde diese Funktion 51 Mal genutzt, unter anderem in folgenden Fällen:

- Um Betroffene von CVE-2019-19781 a.k.a. “Shitrix” zu informieren.
- Mehrfach, um Betroffene von Emotet zu warnen.
- Im Zuge des cit0day Leaks (vgl. 2.6.4 Leaks) konnten wir auf diesem Weg Betroffene schnell informieren.

2.5.2 MISP

MISP[11] 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.[12]

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

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

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

Die Hauptentwicklung von MISP liegt bei CIRCL, dem nationalen Computer-Notfallteam Luxemburgs. 2020 arbeiteten CERT.at und CIRCL verstärkt daran, die Schnittstellen zwischen MISP und IntelMQ zu verbessern, um den gemeinsamen Einsatz dieser Tools zu vereinfachen.

2.6 Bedrohungen 2020

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 bzw. neue, kritische Schwachstellen, die im großen Stil ausgenutzt werden.

2020 fielen darunter einerseits CVE-2019-19781 a.k.a. “Shitrix”, Lücken in diversen Firewall- und VPN-Lösungen auf der Seite der Schwachstellen, sowie Emotet und Ransomware auf der Seite der besonders aktiven Malware, die in diesem Jahr neben Unternehmen und Privatpersonen auch verstärkt Städte sowie Gesundheits- und Bildungseinrichtungen ins Visier nahmen.

Außerdem kam es Ende des Jahres zur Veröffentlichung einiger Leaks, die aber glücklicherweise zum Großteil nur sehr alte Daten enthielten.

Große Beachtung erhielt im Dezember der Supply-Chain-Angriff auf die Firma SolarWinds und ihr Produkt Orion. Obwohl diese Art von Attacken keineswegs unbekannt war, stellten Umfang und Professionalität bei der Durchführung ein Novum dar. Die unmittelbaren Auswirkungen auf Österreich waren allerdings gering, weshalb hier nur auf die regelmäßig aktualisierte Artikelsammlung des ThaiCERT, die hier zu finden ist, verwiesen werden soll.

2.6.1 Ransomware

Auch im Jahr 2020 blieb Ransomware eine der größten Bedrohungen für öffentliche Einrichungen, Firmen und Privatpersonen.

[11] 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.

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

Das durch die COVID-19 Krise vielerorts eingeführte Home-Office bietet zwar einerseits viele Vorteile, aber durch den häufigen Einsatz privater Geräte in diesen Gegebenheiten, wurde die ohnehin schon schwierige Aufgabe, Arbeitsgeräte effizient zu schützen, noch um einiges erschwert, was den Kriminellen hinter Ransomware in die Hände spielt(e).

Gerade große Institutionen wie Universitäten, Städte und Krankenhäuser wurden vermehrt ins Visier genommen. Bei einem Angriff auf die Uniklinik Düsseldorf kam es erstmals zu einem Todesfall, der mit einem Ransomwareangriff in Verbindung gebracht wurde – die Staatsanwaltschaft stellte die Ermittlungen wegen fahrlässiger Tötung jedoch bald darauf ein, da der Gesundheiszustand der Verstorbenen so schlecht war, dass ein Zusammenhang mit der Attacke nicht haltbar war.[13]

Aber auch Ransomware für Privatpersonen blieb 2020 nicht untätig und brachte z.T. relativ bizarre Blüten hervor, wie Schadsoftware, die einen Peniskäfig, also quasi ein Keuschheitsgürtel als Sexspielzeug, verschlüsselte, sodass Betroffene erst nach der Bezahlung von 0,02 Bitcoin ihre Genitalien wieder befreien konnten.[14]

Eine Taktik, die bereits 2019 aufgetaucht war, "etablierte" sich 2020 zusehends: Die Doppelerpressung. Dabei verschlüsseln die Kriminellen nicht, wie zuvor üblich, sofort alle ihnen relevant erscheinenden Teile des Netzwerks, sondern stehlen zuvor alle Daten, die ihnen besonders wichtig bzw. heikel erscheinen. Erst danach erfolgt die Verschlüsselung.

Oftmals unabhängig davon, ob das Lösegeld für die Entschlüsselung bezahlt wird oder nicht, stellen die Kriminellen etwas später eine weitere Forderung: Entweder das Opfer zahlt ein zusätzliches Lösegeld, oder die gestohlenen Daten werden im Internet veröffentlicht. Dies stellt auf viele Arten eine Gefahr dar:

- Die Daten enthalten oft intime Informationen über die Firma, die für (andere) Kriminelle in Folgeangriffen nützlich sein können. Beispielsweise kann Wissen über interne Abläufe oder Konflikte, die aus E-Mails ersichtlich sind, Social Engineering wesentlich erleichtern.

- Sind auch sensible Daten im Sinne der DSGVO abhanden gekommen, sind KundInnen sowie die Datenschutzbehörde zu informieren, was im Zuge eines ohnehin schon sehr belastenden Angriffs oft nicht bedacht wird, aber zu Folgestrafen führen kann. Dabei ist v.a. zu beachten, dass diese Meldung unabhängig davon zu erfolgen hat, ob es zu einer Veröffentlichung kommt, oder nicht – die Kriminellen selbst hätten diese Daten ja bereits nicht einsehen dürfen.

- Je nach Inhalt der Daten sind erneute Erpressungsversuche zu einem späteren Zeitpunkt nicht auszuschließen. Vielfach behaupten die Kriminellen zwar, die Daten nach erfolgter Zahlung zu löschen, kontrollieren können die Opfer das aber natürlich nicht. Bedenkt man dabei, wie oft es bei "normalen" Firmen zu Fehlern bei der Löschung von Daten kommt und diese irgendwann in diversen Leaks landen, ist also selbst bei "ehrlichen" Kriminellen das Risiko, dass die Daten ihren Weg in die Öffentlichkeit finden, nicht zu vernachlässigen.

2.6.2 Emotet

Emotet ist eines der anpassungsfähigsten Schadsofware-Netzwerke der letzten Jahre und dies zeigte sich auch 2020: CERT.at verarbeitete in diesem Jahr über 5000 Meldungen über mögliche Infektionen durch Emotet und informierte die Betroffenen.

[13] Siehe https://heise.de/-4908608 für einen frühen Bericht und https://heise.de/-4961183 zur Einstellung der Ermittlungen wegen fahrlässiger Tötung.

[14] Nachzulesen unter https://heise.de/-5025561.

Nach einem intensiven Jänner, legte Emotet im Februar eine fünfmonatige Pause ein, in der keine Spam-Nachrichten mit schadhaften Inhalten (Malspam) versendet wurden. Wie schon in früheren “Pausen”, blieben die Kriminellen aber keineswegs untätig, sondern nutzten die Zeit, um die Schadsoftware weiterzuentwickeln.

Bereits ab April konnten auf den Command & Control Servern neue Versionen von Emotet beobachtet werden, die bis-dato bekannte Detektions- und Präventionsmechanismen unbrauchbar machten. Diese wurden aber noch nicht aktiv eingesetzt.

Bevor der Versand von Malspam wieder startete, hatten die Kriminellen neue Funktionalität in die Schadsoftware integriert, die es ihnen bei erfolgreicher Infektion ermöglichte, nicht nur E-Mail-Konversationen, sondern auch Datei-Anhänge bis zu einer maximalen Größe von 131072 Bytes automatisiert zu stehlen. Diese Dokumente dienten dazu, den Spam noch glaubhafter zu gestalten, indem sie zusätzlich zu den schadhaften Anhängen in derselben E-Mail verschickt wurden.

Komplett Emotet-los war die Pause jedoch nicht; andere Schadsoftware (namentlich Trickbot) nutzte ihre Infrastruktur weiterhin, um Emotet zu verschicken. Im Juli startete Emotet selbst dann seine erste, eigene Malspam-Welle nach der Pause. Dieser neue Anlauf verlief allerdings etwas holprig, da es unbekannten AkteurInnen gelang, einige von Emotet benutzte Seiten zu kapern, so dass diese anstatt Schadsoftware animierte Bilddateien und später ”Avira Antivirus”-Installer auslieferten. Etwa Ende August konnten die Kriminellen dieses Problem aber vollständig beseitigen.

Im Oktober konnte erneut eine kurze Pause beobachtet werden. In diesem Monat wurde ein groß angelegter Takedown-Versuch gegen das Trickbot-Netzwerk unternommen, an dem unter anderem das US Cyber Command des Pentagon und Microsoft teilnahmen. Es ist unklar, ob diese Aktion mit Emotets Pause in Zusammenhang steht; teilweise wurde vermutet, dass sie der Grund für die Pause war, andere meinten allerdings, dass dadurch eine ohnehin geplante Pause vorzeitig abgebrochen wurde.

Anfang November bis kurz vor Weihnachten gönnte sich Emotet erneut eine Auszeit, die dafür genutzt wurde, den Infektionsweg, der aus den infizierten Dokumenten nachgeladenen Schadsoftware, von direkt ausführbaren Dateien mit Endung `.exe` auf `rundll32` beziehungsweise `regsvr32` ausgelöste “dynamic-link libraries” (`.dll`) Dateien umzubauen.

Diese Taktik wurde bis zum Ende des Emotet-Netzwerks (s.u.) weiterverfolgt.

2020 benutzte Emotet folgende Methoden, um ein System initial zu infizieren:

- Sich verändernde Word-Vorlagen, die nach der teilweise zweistufigen Aktivierung von Makros den Schädling installieren. Kurz vor Weihnachten kam nach der Aktivierung der Makros noch die Anzeige eines Microsoft Windows Nachrichtenfensters dazu, um glaubhafter zu wirken und eine Detektion weiter zu erschweren.

- Links in den Spam-Mails, die auf Seiten verwiesen, von denen der Schadcode heruntergeladen wurde.

- Passwortgeschützte ZIP-Dateien im Anhang. Dabei war das Passwort selbst in der E-Mail enthalten. Grund für diese Vorgehensweise ist der Umstand, dass solche ZIP-Dateien nicht von Anti-Virus-Software am Mailserver erkannt werden, da diese ja nicht sehen kann, dass das zugehörige Passwort in der E-Mail enthalten ist und so höchstens warnen kann, dass der Inhalt der ZIP-Datei nicht geprüft werden konnte.

Emotet wird zumeist als ”Loader” genutzt, d.h. sein Hauptzweck ist es, nach erfolgreicher Infektion weitere Schadsoftware nachzuladen. Zu diesen zählten 2020 neben Trickbot auch Qak-

bot, ZLoader und IceID/Bokbot. Praktisch muss man sich das so vorstellen, dass die Kriminellen hinter Emotet mit diesem Nachladen die Zugänge zu den infizierten Systemen an andere kriminelle Gruppen weitergeben. Das ist höchstwahrscheinlich nicht gratis, sondern es ist davon auszugehen, dass diese Gruppen Geld bezahlen, damit Emotet ihre Schadsoftare nachlädt und sie die Kontrolle über den infizierten Computer erhalten.

Diese Geschäftsbeziehungen zwischen den einzelnen kriminellen Gruppen sind zwar sehr wahrscheinlich vorhanden, aber natürlich kaum faktisch nachweisbar (bzw. erst, wenn die jeweilige Gruppe von Strafverfolgungsbehörden ausgehoben wird).

Allerdings war 2020 mit etwas Glück das letzte Jahr, in dem Emotet sein Unwesen trieb: In einer bemerkenswerten internationalen Aktion unter der Koordination durch Europol und Eurojust, ist es Ende Jänner 2021 gelungen, das Emotet-Netzwerk zu zerschlagen.[15]

Dies war ein wichtiger Schritt im Kampf gegen die organisierte Cyber-Kriminalität, dessen Folgen aktuell noch nicht absehbar sind. Selbst wenn Emotet selbst sich davon nicht erholen sollte, bleibt zu befürchten, dass das entstandene Vakuum früher oder später durch andere Kriminelle gefüllt wird. Außerdem richtete sich die Aktion vor allem gegen Emotets Infrastruktur; es konnten zwar auch einige der beteiligten Personen festgenommen werden, aber leider nicht alle.

2.6.3 Vergessene Updates

Das Einspielen von Updates ist in der IT seit jeher ein Problem – vielfach werden Patches nicht installiert, da um die Stabilität des Systems gefürchtet wird. Diese Furcht ist leider nicht unbegründet, wie Updates diverser großer Softwarefirmen immer wieder eindrucksvoll unter Beweis stellen.

Hinzu kommen potentiell noch Probleme mit ausgelaufenen Lizenzen, die Updates blockieren und fertig ist eine Situation, in der die Wartung von (sicherheitskritischen) Systemen vernachlässigt wird.

2020 waren es vor allem Instanzen von Microsoft Exchange Servern und diverse VPN- bzw. Firewallprodukte, die wegen mangelnder Patch-Disziplin bei gleichzeitiger Verfügbarkeit von öffentlichen Exploits vielversprechende Angriffsziele darstellten.

CVE-2020-0688: RCE in Microsoft Exchange Servern

Im Februar 2020 veröffentlichte Microsoft einen Patch für CVE-2020-0688, einer Remote Code Execution (RCE) Schwachstelle, bei der AngreiferInnen lediglich über ein gültiges Login[16] verfügen müssen, um Befehle als `NT Authority\SYSTEM` ausführen zu können. Letzteres ergibt sich daraus, dass es im Zuge des Ausnützens der Lücke auch zu einer Privilegieneskalation kommt.

Da Mailserver einerseits oft von außen erreichbar sind und andererseits gewöhnlich hochsensible und wichtige Daten enthalten, sind sie ein lohnendes Ziel für viele AngreiferInnen – von einem einfachen Stören des Betriebsablaufs durch Änderung der Konfiguration, über Diebstahl sensibler Daten wie Firmengeheimnissen, bis hin zur Verschlüsselung des Servers, gibt es verschiedenste Möglichkeiten für Kriminelle, aus dieser Schwachstelle Kapital zu schlagen.

Bei einer so kritischen Schwachstelle mit potentiell so weitreichenden Folgen, könnte man nun davon ausgehen, dass sie mit hoher Priorität behoben wird. Dem ist allerdings nicht so: Nachdem bereits zeitnah Exploits auf GitHub verfügbar waren und andere nationale CERTs/CSIRTs

[15] Eine genauere Beschreibung davon finden Sie auf der Webseite von Europol.
[16] D.h. beliebige, gültige Zugangsdaten zu irgendeinem Mail-Account auf dem Server

in Europa davon berichteten, dass sie zahlreiche ungepatchte Instanzen in ihren Ländern gefunden hatten, machten wir uns im April mithilfe von Shodan und einem Script von CERT.LV[17] auf die Suche nach verwundbaren Systemen in Österreich – und wurden fündig: Knapp ein Viertel der identifizierten Exchange-Server hatte den Patch noch nicht eingespielt. Details können in unserem Blogpost dazu nachgelesen werden. Wir informierten die Betroffenen und hofften darauf, dass die fehlenden Patches nun bald eingespielt würden.

Diese Hoffnung blieb allerdings ebenfalls unerfüllt, wie sich im Oktober 2020 herausstellte, als wir den Scan wiederholten und die Ergebnisse mit jenen vom April verglichen: Im Zuge dieses zweiten Scans verbesserten wir unsere Erkennungsmethoden und kamen zu folgendem Ergebnis:

Version	Anzahl	Verwundbar	Verwundbar (%)
Exchange Server 2013	1583	863	54.52%
Exchange Server 2016	3868	1993	51.53%
Exchange Server 2019	1025	252	24.59%
Gesamt	6476	3108	47.99%

Obwohl dieses Ergebnis sogar schlechter aussieht, als jenes vom April, gehen wir davon aus, dass das mit der verbesserten Verifikation zu tun hat und faktisch kaum eine Veränderung stattgefunden hat. Details zum zweiten Scan finden Sie wiederum in einem Post auf unserer Webseite.

Es zeigt sich also insgesamt, dass auch bei so hochgefährlichen Schwachstellen auf wahrscheinlich kritischen Systemen[18] Updates vielfach auch acht Monate nach ihrer Veröffentlichung noch nicht eingespielt wurden und dementsprechend ein Umdenken stattfinden muss, um Kriminellen das Leben zumindest etwas schwerer zu machen.

Veraltete Windows Server

Im Oktober 2020 veröffentlichte Rapid7 einen Blogpost zu Microsoft Servern, die aus dem öffentlichen Internet erreichbar waren, aber auf einer nicht mehr unterstützten Version von Microsofts Server Betriebssystem liefen.[19]

Das Ergebnis war zwar nicht sehr überraschend, aber trotzdem erschreckend: Mehr als 50% aller Microsoft Server, die Rapid7 identifizieren konnte, setzten auf Windows Server 2008 R2, dessen Support im Jänner 2020 eingestellt worden war.

CERT.at nahm das zum Anlass, um einen Blick auf die Situation in Österreich zu werfen. Dazu haben wir in der Shodan-Datenbank nach Servern gesucht, die sich in ihrem Banner als Microsoft Internet Information Service (IIS) 7.0 bzw. 7.5 zu erkennen geben, einer Standardsoftware auf Windows Server 2008 bzw. Windows Server 2008 R2. Zusätzlich haben wir auch nach IIS Version 6.0 gesucht, die in Windows Server 2003 zum Einsatz kam kommt, dessen regulärer Support Mitte 2010 ausgelaufen ist. Das Ergebnis: Insgesamt gab es 31661 Geräte, die sich als ”Microsoft IIS” identifizierten, und bei unserer Suche stießen wir auf Versionen, die so alt waren, dass wir gar nicht mit ihnen gerechnet hatten. In der folgenden Tabelle sind jene Versionen die zum Zeitpunkt des Scans nicht mehr unterstützt waren, rot hinterlegt.

[17] Zu finden auf GitHub unter https://github.com/cert-lv/CVE-2020-0688.
[18] Kaum ein Unternehmen wird den eigenen Mailserver als irrelevant abtun.
[19] https://blog.rapid7.com/2020/10/19/are-you-still-running-end-of-life-windows-servers/

Version	Anzahl	Anteil
IIS 4.0 (Windows NT 4.0)	9	0.03%
IIS 5.0 (Windows 2000)	64	0.2%
IIS 5.1 (Windows XP Professional)	38	0.12%
IIS 6.0 (Server 2003)	607	1.92%
IIS 7.0 (Server 2008)	903	2.85%
IIS 7.5 (Server 2008 R2)	7477	23.63%
IIS 8.0 (Server 2012)	1133	3.58%
IIS 8.5 (Server 2012 R2)	8304	26.23%
IIS 10.0 (Server 2016/2019)	13125	41.45%
Unklassifiziert	1	0.00%

In Summe stellen die nicht mehr unterstützten Versionen etwas mehr als 28% dar. Das ist zwar erfreulich weit weg von den über 50%, die Rapid7 dem gesamten Internet attestierte, aber leider immer noch näher daran, als an den 0%, die wir uns wünschen.

Wir haben daraufhin sämtliche BetreiberInnen der betroffenen Server informiert, ein erneuter Scan 2021 ist noch ausständig

(Alte) Lücken in Firewalls und VPN-Produkten

Firewall- und VPN-Lösungen sind meist extrem wichtige Geräte im Netzwerk und Zugriff auf sie bedeutet oft auch Zugriff auf interne Daten und Services. Dementsprechend sind sie, ähnlich wie die oben besprochenen Mailserver, ein häufiges Angriffsziel und kritische Schwachstellen in ihnen dementsprechend gefährlich.

2020 gab es einerseits eine Reihe neuer Schwachstellen, z.B. CVE-2020-12271, einer RCE in Sophos XG Firewalls, die schon beim Bekanntwerden aktiv im Zuge einer Kampagne namens "Asnarök" ausgenutzt wurde,[20] oder CVE-2020-2021, einer Schwachstelle in Palo Alto Networks PAN-OS, die bei bestimmten Konfigurationen dazu führte, dass die Verifikation von Signaturen bei der Authentisierung via SAML nicht korrekt funktionierte und so Unbefugte Zugriff auf interne Ressourcen erhalten konnten.[21]

Andererseits zeigte sich aber auch, dass alte Schwachstellen nichts an ihrer Gefährlichkeit eingebüßt hatten: In vielen Fällen gibt es keine (öffentlichen) Follow-Up Scans von ResearcherInnen oder Firmen, die zeigen, ob und wie zeitnah Patches eingespielt wurden.[22] 2020 stellte dazu aber CVE-2018-13379 eine Ausnahme dar, eine Schwachstelle in FortiOS SSL VPN-Lösungen, für deren Behebung seit Mai 2019 Updates zur Verfügung stehen und für die seit August 2019 öffentliche Exploits auf GitHub zu finden sind. Ende 2020 wurden jedoch Scan-Ergebnisse auf Twitter veröffentlicht, die angaben, dass es weltweit fast 50 000 nach wie vor verwundbare Instanzen gab, die auch exploitet wurden. Im Zuge dieser Angriffe wurden Accountnamen und Passwörter gestohlen.[23]

[20] Details finden sich z.B. unter https://news.sophos.com/en-us/2020/04/26/asnarok/.
[21] Siehe https://security.paloaltonetworks.com/CVE-2020-2021.
[22] Dies gilt natürlich nicht nur für Firewall- und VPN-Software.
[23] Vgl. z.B. https://heise.de/-4968392.

CERT.at wurden alle Daten aus diesem Leak zugespielt, die sich auf Geräte in Österreich bezogen (etwa 1000 IP-Adressen), wodurch wir alle Betroffnen zeitnah informieren konnten.

Wir suchen seitdem automatisiert via Shodan nach potentiell verwundbaren FortiOS-Instanzen und schicken entsprechende Warnungen aus. Siehe dazu auch 2.4.1 Eigene Erhebungen.

2.6.4 Leaks

Leaks sind mittlerweile ein Dauerbrenner – es vergeht kaum ein Monat, in dem es nicht zu einer gröberen Datenpanne kommt. In dieser Hinsicht war 2020 keine Ausnahme: Neben den zunehmenden Leaks durch Ransomware-Gangs (vgl. 2.6.1 Ransomware) und der Veröffentlichung der Daten aus Angriffen auf FortiOS-Geräte (vgl. 2.6.3 Vergessene Updates), schlug im November der "cit0day" Leak hohe Wellen:

Die Plattform `cit0day[.]in`, auf der (vornehmlich) Kriminelle andere Leaks kaufen konnten wurde im September 2020 vom Netz genommen. Ab diesem Zeitpunkt wurde ein Banner angezeigt, das behauptete, die Seite sei von der amerikanischen Exekutive beschlagnahmt worden. Dazu gab es aber keine offizielle Bestätigung und es kam auch zu keinen öffentlich bekannten Festnahmen in diesem Zusammenhang. Aus diesem Grund liegt die Vermutung nahe, dass der Takedown von den Verantwortlichen hinter der Plattform selbst inszeniert war.[24]

Unabhängig davon, was hinter dem "Takedown" steckte, wurde Anfang November 2020 das Leak-Archiv von `cit0day[.]in` zuerst auf der File-Sharing-Plattform MEGA und wenig später an anderer Stelle und in anderem Format veröffentlicht.

CERT.at durchsuchte die Daten auf betroffene `gv.at` Adressen und informierte die jeweiligen MX-BetreiberInnen. Aus den Rückmeldungen wurde klar, dass die gestohlenen Daten zum Großteil ziemlich alt (z.T. mehr als zehn Jahre) waren, und daher kaum eine unmittelbare und große Gefahr darstellten.

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 Cyberangriff auf das BMEIA

GovCERT Austria gibt immer wieder Hinweise über Bedrohungen an die öffentliche Verwaltung weiter. Diese reichen von sehr generischen Informationen zu Schwachstellen in verbreiteter Software, über Beschreibungen von Angriffsmustern (Indicators of Compromise "IoCs") bis hin zu sehr konkreten Hinweisen; etwa, dass gewisse E-Mail Adressen das Ziel von Spear-Phishing waren.

So auch rund um das Neujahr 2020: Im Außenministerium (BMEIA) wurde auf Grundlage von übermittelten Indikatoren durch die TechnikerInnen des BMEIA sowie MitarbeiterInnen des GovCERTs und des früh eingebundenen Cyber Security Centers (CSC) im BVT entsprechende Nachforschungen durchgeführt.

Auf Basis der Erkenntnisse dieser Nachforschungen und darauf aufbauender weitergehenden Analysen des CSC im BVT wurde am Samstag, den 4. Jänner eine Sitzung des IKDOK ein-

[24] Einen Artikel von ZDNet dazu finden Sie hier.

berufen, bei dem das darauffolgende Treffen des Koordinationsausschusses laut §25 NISG vorbereitet worden ist. Von diesem wurde nach entsprechenden Beratungen das Vorliegen einer Cyberkrise durch den Bundesminister für Inneres festgestellt und der Vorfall proaktiv kommuniziert.

In der folgenden Woche wurde ein Einsatzteam bestehend aus Personal des BMEIA, Bundeskanzleramts, GovCERTs, Innenministeriums (CSC und Bundeskriminalamt/C4) und Bundesheers (MilCERT, Abwehramt und Nachrichtenamt) etabliert, um diesen Vorfall mit allen verfügbaren Kräften abzuarbeiten. Zusätzlich wurde durch das BMEIA ein österreichischer Dienstleister hinzugezogen, der vor allem bei der Vorbereitung der Remediation unterstützte. So konnte kurz nach den ersten Erkenntnissen an einem Wochenende das Netz des BMEIA auf einen Schlag bereinigt werden.

Das Einsatzteam bestand aus mehrern AnalystInnen und gliederte sich u.a. in die Bereiche “Analyse”, “Verbesserung der Sichtbarkeit”, “Remediation”, “Stab” und “Infrastruktur. Da dies der erste Einsatz in dieser Konstellation war, wurden Infrastruktur und Prozesse aufgebaut und laufend verbessert.

Die Zusammenarbeit in dieser sehr diversen Gruppe hat nicht nur auf menschlicher Ebene gut funktioniert, sondern war auch technisch erfolgreich und Grundlage für die schlussendlich erfolgreiche Bereinigung des kompromittierten Systems.

Eine der Aufgaben des GovCERTs war, als Informationsdrehscheibe auf technischer Ebene zwischen dem Team vor Ort und externen Teams zu fungieren – sowohl in Österreich (CERT Verbund, andere Ministerien) als auch auf europäischer Ebene (CSIRTs Network und European Government CERTs Group). Wir wollen uns hier noch einmal bei allen bedanken, die uns bei der Bewältigung des Vorfalls mit ihrem Know-How geholfen haben.

Nicht zu unterschätzen war neben der Arbeit auf technischer Ebene die Kommunikation in Richtung des Koordinationsausschusses und der Politik sowie die außenpolitische Kommunikation mit Partnern. Es wurde sich stets bemüht, die gewonnen Erkenntnisse und deren Implikationen so zusammenzufassen und zu präsentieren, dass diese auch für Nicht-TechnikerInnen verständlich und nutzbar sind.

Rückblickend war der Vorfall im BMEIA ein erster großer und insgesamt erfolgreicher Test für die Strukturen, die mit dem NIS Gesetz geschaffen wurden. Gleichzeitig konnten aber auch Optimierungsmöglichkeiten für diese Strukturen identifiziert werden, die es umzusetzen gilt.

2.7.2 CVE-2019-19781 a.k.a. “Shitrix”

Bereits am 17. Dezember 2019 hatte Citrix in einem Advisory bekanntgegeben, dass es über eine kritische Lücke (CVE-2019-19781, späterer Spitzname “Shitrix”) in einigen seiner Produkte Bescheid wusste und Workarounds zur Verfügung gestellt. Diese wurden allerdings (vermutlich unter anderem aufgrund der weltweit verbreiteten Feiertage zum Jahreswechsel) in vielen Fällen nicht zeitgerecht eingespielt und richtige Updates wurden erst in der zweiten Jännerhälfte zu Verfügung gestellt.

Am 10. Jänner wurde der erste Exploit auf GitHub veröffentlicht, und spätestens da zeigte sich, wie einfach die Lücke auszunutzen war: Mit wenigen HTTP-Requests mit einem bestimmten Pfad konnten AngreiferInnen über das Netzwerk beliebige Befehle auf den Geräten ausführen ohne irgendwelche Zugangsdaten zu benötigen.

In diesem Fall hatten wir ein wenig Glück im Unglück: CERT.at hatte mithilfe befreundeter CERTs/CSIRTs schon etwas früher mit dem Scan nach verwundbaren Geräten beginnen können und unsere Warnungen an die Betroffenen konnten dadurch am 10. Jänner, kurz bevor die ers-

ten größeren Medienberichte zu den Exploits die Runde machten, bereits verschickt werden.

Dennoch waren die nächsten Wochen von vielen Anrufen und Nachfragen zu “Shitrix” geprägt.

Ganz aus den Schlagzeilen verschwand die Lücke während des gesamten Jahres nicht, aber zumindest die Anzahl der Betroffenen in Österreich war unseren späteren Scans zufolge gering.

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 Austria ist dabei der staatliche österreichische Ansprechpartner für vergleichbare Stellen im Ausland sowie für internationale Organisationen zu Fragen der IKT-Sicherheit.

3.2 Vernetzung auf nationaler Ebene

3.2.1 Austrian Trust Circle (ATC)

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

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

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

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

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 2020 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.

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

Der IKDOK umfasst das Cyber Security Center des BMI und das Cyber Verteidigungszentrum des BMLV 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 Energy Computer Emergency Response Team (AEC) aufgebaut hat. Mehr Informationen über das AEC finden Sie auf deren Webseite unter https://www.energy-cert.at/.

3.3 Vernetzung auf internationaler Ebene

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

3.3.1 Bilaterale Vernetzung

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

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, 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 zwischen Sicherheitsteams in Bezug auf aktuelle Vorfälle, Gefahrenpotentiale sowie Projekte und Werkzeuge der Teilnehmenden. Neben den regelmäßigen Treffen von VertreterInnen der GovCERTs gibt es auch eine laufende niederschwellige Kommunikation zwischen den Teams. Die Unabhängigkeit von politischen 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.

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

[2] Konkret unter anderem MISP und IntelMQ.

3.4 Weitere Kooperationen

3.4.1 Connecting Europe Facilities (CEF)

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

CERT.at reichte im Jahr 2018 ein weiteres EU Projekt "Enhancing Cybersecurity in Austria" (2018-AT-IA-0111) im Rahmen des Connecting Europe Facilities (CEF) Programm ein, das in vollem Umfang genehmigt wurde und eine 75%-ige Förderung der Projektkosten durch die Europäische Union ab September 2019 beinhaltet. Das geplante Projektende ist August 2021.

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

Research and Development Ein besonderer Fokus liegt dabei auf der Forschung und dem Ausbau der Automatisierung unter maßgeblicher Beteiligung des Research & Development Teams ("R&D") der nic.at:

- Mittels eines neu entwickelten internen RDAP[3]-Dienstes steht CERT.at nun der whois-Nachfolger zur Verfügung, was den weiteren Ausbau des automatisierten Incident Handlings mit IntelMQ ermöglicht.
- Im Juli stellten wir erstmals das Projekt tag2domain in einem Blogpost vor. Dabei handelt es sich um ein erweiterbares System, das Webseiten anhand von deren Eigenschaften in verschiedene Taxonomien in Form von Tags klassifiziert. Darauf basierend können Benachrichtigungen, Auswertungen und Statistiken erstellt werden – beispielsweise welche Webseiten in welchen Wirtschaftszweig fallen oder veraltete bzw. verwundbare Software einsetzen. Den Quelltext dazu finden Sie auf https://github.com/certtools/tag2domain/
- Zur Analyse der Webseiten unter .at entwickelten wir unseren bestehenden "Crawler" wesentlich weiter, der nun die gesamte .at-Zone in einer Woche abdecken kann (statt ursprünglich in 3 Monaten). Auch der Code zu diesem Programm ist öffentlich verfügbar: https://github.com/nic-at/nic-crawler-analysis
- In weiterer Folge werden die Webseiten analysiert und z.B. auf verwendete Sprache oder eingesetzte Technologien (CMS-Software, Webserver) hin analysiert. Weitere Einblicke in die Daten wurden mit Hilfe von Data-Science und Machine-Learning möglich.
- Das OpenINTEL-Projekt ist eine Kooperation der Universität Twente, SURFnet, SIDN Labs und NLnet Labs mit dem Ziel den Status großer Teile des globalen Domain Name Systems auf täglicher Basis zu erfassen. Für die Analyse von Vorfällen ist es für CERT.at von wesentlicher Bedeutung, den zeitlichen Verlauf von Einträgen im DNS-System nachvollziehen zu können. Hierfür entwickelten wir Such- und Analysefunktionen, um die großen Datensätze in der täglichen Arbeit von CERT.at nutzbar zu machen. Die entstandene Software steht auf GitHub bereit: https://github.com/nic-at/openintel-lookup

[3] Registration Data Access Protokoll

IntelMQ Mithilfe von IntelMQ verarbeitet CERT.at rund um die Uhr vollautomatisiert Informationen zu Malwareinfektionen und Verwundbarkeiten in österreichischen Computernetzwerken. Täglich werden die NetzbetreiberInnen über Probleme in deren Netzen informiert (siehe 2.3 2020 im Detail). Im Rahmen des CEF-Projekts entwickeln wir die von uns betreute Open-Source Software gemeinsam mit anderen Partnern weiter. Im Jänner 2020 veröffentlichten wir erstmals ein eigenes Tutorial zu dessen Nutzung. Beim TF-CSIRT Treffen im Jänner wurde dieses auch gleich im Zuge eines Workshops erprobt. Außerdem zog IntelMQs Dokumentation im November auf intelmq.readthedocs.io (und damit auf Sphinx) um, und erhielt dadurch eine neue Struktur und Navigation.

Im Laufe des Jahres 2020 erschienen mehrere neue Versionen der Software mit zahlreichen Neuerungen. Details zu den Versionen 2.1.3, 2.2.0, 2.2.1, 2.2.2, 2.2.3 finden sich in unserem Blog und in IntelMQs Changelog.

Außerdem wurde die Entwicklung von IntelMQ 3.0 fortgesetzt. Dazu gab es einen auf NutzerInnenfeedback basierenden, ersten großen Änderungsvorschlag bei der Konfiguration.

Das Jahr 2020 brachte uns auch unsere erste CVE-Nummer für eine IntelMQ Komponente: CVE-2020-11016. Bernhard Herzog von Intevation fand im IntelMQ-Manager, dem Web-Frontend zu IntelMQ eine Command-Injection Schwachstelle, die im schlimmsten Fall zu einer Remote Code Execution ohne jegliche Authentifizierung führen konnte. Die Lücke wurde mit dem Release von IntelMQ-Manager 2.1.1 behoben.

Constituency-Portal Im Sommer konnte mit der Intevation GmbH aus Osnabrück ein neuer Partner für die Weiterentwicklung der nächsten Version des “Constituency-Portals”, unseres Tools zur Verwaltung von Kontaktadressen, gewonnen werden. Es wurde beschlossen, eine komplett neue Version des Constituency-Portals zu entwickeln, weil sich im Verlauf des Projekts herausstellte, dass die Struktur der aktuellen Version den Anforderungen nicht entspricht. Diese befindet sich daher nur noch im Maintenance Mode, sie wird nicht mehr weiterentwickelt.

Die Fertigstellung des Constituency-Portals als freie Software ist bis Sommer 2021 geplant und wird ebenfalls zu großen Teilen aus CEF finanziert. Intevation hat im Rahmen anderer Projekte bereits IntelMQ maßgeblich weiterentwickelt. Die offene Entwicklungsweise unterstreicht unser Engagement für Freie Software und die internationale IT-Security-Gemeinschaft und das Werkzeug wird damit auch anderen CERTs/CSIRTs zur Verfügung stehen. Das Code-Repository ist auf gitlab zu finden.

Human Resources Es konnten im Rahmen des Projektes im Jahr 2020 drei neue Mitarbeiter begrüßt werden – das CERT Incident-Handler Team, CERT Operations sowie R&D freuten sich über personellen Zuwachs.

Seit Anfang des Jahres erhält das Handlerteam durch Thomas Pribitzer und das Operations Team durch Rhonda D’Vine Unterstützung.

Seit Juli wird CERT.at von Clemens Moritz als Research Engineer aus der R&D Abteilung der nic.at gemeinsam mit den anderen Kollegen von R&D bei der Umsetzung unserer Threat Intel Projekte wie tag2domain, webcrawling and site-analytics sowie OpenIntel unterstützt – unserem dritten CEF Projektmitarbeiter.

Reisen und Konferenzen Februar und März beschäftigten uns die Auswirkungen des ersten “Lockdowns” und sämtliche geplanten Reisen und Konferenzen wurden storniert oder verschoben, alle wechselten komplett ins Homeoffice und die ersten Meetings und Konferenzen wur-

den online geplant. Auch die für März und April bei uns im Haus geplanten Hackathons u.a. zum Thema RTIR ("Request Tracker Incident Response", einem Helpdesk-System) konnten nicht mehr vor Ort stattfinden und mussten vorerst abgesagt werden.

Auf Grund der anhaltenden Restriktionen wegen COVID-19 musste das für April in Pörtschach am Wörthersee geplante jährliche ATC (Austrian Trust Circle) Treffen zuerst auf Oktober 2020 verschoben und schlussendlich leider für 2020 ganz abgesagt werden.

Dank des Wechsels auf Online-Formate konnten wir den Austausch mit unseren internationalen Partnern aufrecht erhalten und an diversen Konferenzen, darunter TF-CSIRT, CSIRTs Network, European GovCERT Group, FIRST teilnehmen.

Im Juni fand ein virtuelles Treffen der CENTR[4] "Registry Data Nerd" Group mit zwei Beiträgen von uns statt – Philipp Adam sprach über low content Klassifizierungen und L. Aaron Kaplan über Tag2domain, die Folien sind auf GitHub verfügbar.

Verbesserung der internen Sicherheit Im Februar 2020 konnten wir erfolgreich unser Rezertifikationsaudit im Rahmen von ISO 27001 abschließen.

Ein anderes Projekt, das im Juli abgeschlossen werden konnte, war SIRF, das Security Incident Response Framework, dessen Setup und Hardwarebeschaffung im Rahmen von CEF durchgeführt wurde. Hier konnte u.a. ein mobiler Einsatzkoffer für Incident Response Einsätze vor Ort angeschafft werden.

Im Dezember 2020 konnten wir mit einem gezielten Pentest die Sicherheit unseres neuen SIEM[5] Tools bzw. unserer Linux Server Infrastruktur in einem nachfolgenden Workshop testen und verbessern. Unser SIEM ist seit Herbst 2020 in Betrieb.

Außerdem haben wir Verbesserungen im Bereich der physischen Sicherheit umgesetzt und damit den ISM[6] Teil unseres CEF Projektes fertiggestellt.

Die "Trusted Introducer" (TI) Zertifizierung des TF-CSIRT ist ein wesentlicher Maßstab, um die Leistungen der internationalen CERTs vergleichbar zu machen und um einen Mindeststandards sicherzustellen. CERT.at hat im Jahr 2020 seine Prozesse weiter optimiert, um die Erfüllung des Standards weiterhin zu garantieren.[7] Das wurde nicht nur erfolgreich erreicht, sondern wir haben in einigen Bereichen die Anforderungen auch übererfüllt. Für CERT.at ist das für die Zertifizierung genutzte SIM 3 Modell eine willkommene Möglichkeit, um die Erwartungen an uns besser zu verstehen und um allfällige Verbesserungsmöglichkeiten zu identifizieren.

Ausblick 2020 war – trotz oder wegen Corona – ein sehr starkes Jahr für das CEF Projekt und es konnte – abgesehen von der Reiseproblematik – sehr viel umgesetzt werden.

Für 2021 erwarten wir die Fertigstellung des Constituency Portals, die Releases von IntelMQ 3.0, Tag2Domain und OpenINTEL. Außerdem hoffen wir, endlich unsere Hackathons nachholen und das diesjährige ATC Treffen abhalten zu können.

3.4.2 "MeliCERTes" (SMART-2018-2014)

Die NIS Direktive von 2016 hat das CSIRTs Network (CWN) eingerichtet. In diesem Verband soll CERT-EU mit allen CSIRTs zusammenarbeiten, die ihre Aufgaben aus den jeweiligen NIS Umsetzungen bekommen.

[4] Council of European National Top-Level Domain Registries
[5] Security Information and Event Management
[6] Information Security Management
[7] Vgl. 1.4.2 TI Zertifizierung.

Die EU-Kommission hat neben den Vorgaben für die Mitgliedsstaaten auch Hilfen bei der Umsetzung geplant: im Rahmen der Connecting Europe Facility (CEF) gibt es Fördergelder (siehe 3.4.1 Connecting Europe Facilities (CEF)), die unter anderem beim Aufbau der geforderten nationalen Infrastrukturen helfen.

Für das CSIRTs Network und die darin vertretenen CERTs hat die Kommission ein Projekt gestartet, das die nötige Software bereitstellen soll. Diese Software, deren offizieller Name etwas sperrig "Connecting Europe Facility (CEF) Core Service Platform for Cooperation Mechanisms for Computer Emergency and Response Teams in the European Union" lautet, wurde später schlicht "MeliCERTes 1" getauft. Der Anforderungsprozess für dieses Projekt (Teil von SMART 2014/1079) fand im Sommer 2015 statt, also vor der Entstehung des CNW. Dieser Vorausgriff führte zu einem spekulativen Prozess, da noch nicht abzusehen war, wie das CNW wirklich arbeiten würde.

Die zugrundeliegende Software für MeliCERTes 1 wurde im Rahmen des Projektes SMART 2015/1089 entwickelt und erst im Sommer 2019 fertiggestellt. Bis dahin hatten aber die ENISA (als Sekretariat) und einzelne Teams bereits eine Reihe von Tools zur Unterstützung des CNW bereitgestellt, die aber nicht in MeliCERTes 1 integriert waren. Darüber hinaus erwies sich das ursprüngliche Design von MeliCERTes 1 insgesamt als ungenügend, um die unterschiedlichen Anforderungen der CSIRTs und ihrer Zusammenarbeit zu erfüllen. Das lag primär daran, dass es zwischen den Fragen "Was brauchen die Teams für ihre eigentliche Arbeit?" und "Was braucht das CNW, damit die Teams zusammenarbeiten können?" oszillierte, ohne eine konsistente Antwort bieten zu können. Entsprechend muss leider festgehalten werden, dass MeliCERTes 1 keine operative Bedeutung im CNW erlangt hat.

Nach Ende des Projektes SMART 2015/1089 mit Anfang 2020 hat die EU-Kommission einen weiteren Projektauftrag (SMART 2018-1024) zu MeliCERTes vergeben: diesmal an ein Konsortium aus fünf nationalen CSIRTs (PL, EE, SK, LU, AT) und Deloitte. Der Wechsel des Auftragnehmers für die Wartung und Entwicklung von MeliCERTes 2 (MC2) bot die Gelegenheit, die Anforderung an MeliCERTes zu überdenken und alle Annahmen von MeliCERTes 1 zu überprüfen. Das Ergebnis soll ein Satz an Software sein, der dem CNW und seinen Teams wirklich bei der Erfüllung ihrer Aufgaben helfen kann.

Dazu sollen vor allem folgende Aspekte beitragen:

- Scope: In Zukunft sollen drei Säulen die Grundlage von MeliCERTes sein:
  1. Die zentrale Infrastruktur des CNW, also z.B. ein Kooperationsportal, Directory Services, Instant Messaging, etc.
  2. Tools, die den CNW-Mitgliedern vom Konsortium bereitgestellt werden
  3. Das Teilen von Werkzeugen: Es soll für die Teams leichter werden, ihre lokalen Tools auch für Partner zu verfügbar zu machen.
- Enge Zusammenarbeit mit ENISA, dem Sekretariat des Netzwerkes
- Anpassungen der Auslieferung der Software auf die Bedürfnisse des Netzwerkes

Im Jahr 2020 bestand die Hauptaufgabe des Konsortiums in der Überarbeitung der Anforderungen an MeliCERTes. Diese wurde in vier Kleingruppen von Mitgliedern der CNW Tooling WG in einer Serie von Telefonkonferenzen im Sommer 2020 bearbeitet und die Ergebnisse im Herbst von der EU-Kommission und vom CSIRTs Network offiziell angenommen.

CIRCL, Luxemburgs nationales CERT, arbeitet außerdem bereits intensiv an Cerebrate, einem Tool, das als Team Directory und Orchestration für die Zusammenschaltung von anderen

Werkzeugen dienen wird. Der Source Code des Projekts ist unter https://github.com/cerebrate-project abrufbar.

Für CERT.at ist insbesondere interessant, dass wir über diesen Auftrag auch einen Finanzierungsbeitrag für die Weiterentwicklung von IntelMQ erhalten.

Neben IntelMQ wird uns 2021 das Thema Identity and Access Management (IAM) im CSIRTs Network besonders beschäftigen.

3.4.3 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). Während das Bundeskanzleramt nach dem NIS-Gesetz strategische Aufgaben wahrnimmt, nimmt das Bundesministerium für Inneres operative Aufgaben wahr. Im Anwendungsbereich des Gesetzes befinden sich Einrichtungen mit einer hohen Bedeutung für das Funktionieren des Gemeinwesens, weshalb ihre Netz- und Informationssysteme besonders schützenswert sind. Dies betrifft zum einen Einrichtungen in den sieben Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur ("Betreiber wesentlicher Dienste"), zum anderen Einrichtungen, die bestimmte digitale Dienste zur Verfügung stellen ("Anbieter digitaler Dienste") sowie "Einrichtungen der öffentlichen Verwaltung".

4.1.1 Strategisches NIS-Büro

Das im Bundeskanzleramt angesiedelte Büro für strategische Netz- und Informationssystemsicherheit ("strategisches NIS-Büro") führte seine Arbeit im Jahr 2020 – trotz der schwierigen Umstände angesichts der COVID-19 Pandemie – erfolgreich fort. So wurde beispielsweise mit der bescheidmäßigen Feststellung der Eignung und Ermächtigung des Austrian Energy CERT (AEC) als erstes sektoren-spezifisches Computer-Notfallteam im Sinne des NIS-Gesetzes ein wichtiger Schritt gesetzt. Auch konnten bei den Ermittlungen der Betreiber wesentlicher Dienste auf Grundlage der NIS-Verordnung substantielle Fortschritte erzielt werden. Im Hinblick auf die Vertretung Österreichs in der NIS-Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind, wurden umfangreiche Aktivitäten gesetzt. Das NIS-Büro arbeitete u.a. mit den betroffenen Behörden und Regulatoren am Thema der Cybersicherheit von 5G-Netzen. Die NIS-Kooperationsgruppe nahm in diesem Zusammenhang im Jahr 2020 zwei Referenzdokumente, nämlich die CG Publication 01/2020 - Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures sowie die CG Publication 02/2020 - Report on Member Sta-

tes' progress in implementing the EU Toolbox on 5G Cybersecurity, an. Des Weiteren konnten im Jahr 2020 im Bereich der Informationstätigkeit weitere Aktivitäten gesetzt werden. Hervorzuheben sind hier die englischen Übersetzungen des NIS-Gesetzes und der NIS-Verordnung, die auf der NIS-Website (nis.gv.at) abgerufen werden können. Gemeinsam mit dem BMI wurden auf der NIS-Website darüber hinaus der NIS Fact Sheet 8/2018 ("Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices") bereits in der 3. Version sowie der NIS Fact Sheet 7/2019 ("Qualifizierte Stellen") in der 2. Version veröffentlicht.

4.1.2 EU-Cybersicherheitsstrategie 2020 und NIS-2-Richtlinie

Die Europäische Kommission hat am 16. Dezember 2020 eine neue Cybersicherheitsstrategie veröffentlicht, die die Cybersicherheitsstrategie 2013 mit einem neuen strategischen Referenzrahmen für Cybersicherheit auf EU-Ebene ablösen soll. Die neue Cybersicherheitsstrategie zielt darauf ab, das digitale Leben der Menschen in Europa sicher zu gestalten sowie sichere und vertrauenswürdige digitale Instrumente für Wirtschaft, Demokratie und Gesellschaft zu schaffen. Dies soll durch die Steigerung der Resilienz von kritischer Infrastruktur und vernetzten Dingen, den Aus- und Aufbau von operativen Kapazitäten zur Vorbeugung, Abschreckung und Reaktion auf Cyberangriffe sowie die Zusammenarbeit mit internationalen Partnern für einen globalen, offenen, stabilen und sicheren Cyberraum, in welchem Völkerrecht, Menschenrechte, Grundfreiheiten und demokratische Werte gelten, erreicht werden.

Zu den unter der neuen Cybersicherheitsstrategie verfolgten Initiativen gehört auch die Überarbeitung der NIS-Richtlinie. In diesem Sinne legte die Europäische Kommission am 16. Dezember 2020 eine neue NIS-Richtlinie ("NIS-2-Richtlinie") vor, die das Ziel hat, ein hohes gemeinsames Niveau von Cybersicherheit in der EU zu erreichen. Zu diesem Zweck verpflichtet sie die Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige Cybersicherheitsbehörden, zentrale Anlaufstellen und Computer-Notfallteams zu benennen. Ferner sollen bestimmte wesentliche und wichtige Einrichtungen zu einem Cybersicherheitsrisikomanagement und zur Meldepflicht von IT-Sicherheitsvorfällen verpflichtet sowie der Austausch von Cybersicherheitsinformationen weiter forciert werden.