GovCERT Austria

CERT.at

Bericht Internet-Sicherheit Österreich 2017

Inhaltsverzeichnis

Impressum

Medieninhaber und Verleger: nic.at GmbH, Computer Emergency Response Team Austria, Karlsplatz 1/3, 1010 Wien. Diese Publikation wurde in Kooperation mit dem Bundeskanzleramt erstellt. **Projektleitung:** Mag. Otmar Lendl, CERT.at **Konzeption und Redaktion**: pantarhei corporate advisors (Mag. Sigrid Moser-Sailer, MAS, Mag. Brita Eipeldauer, Thomas Kreidl, MSc), CERT.at (Mag. Otmar Lendl), Bundeskanzleramt (Dipl.-Ing. Mag. Andreas Reichard, M.Phil.)

Herstellungsort: Wien, Dezember 2018.

1 Vorwort

Erich Albrechtowitz

Leitung der Gruppe I/B
Bundeskanzleramt

Cybersicherheit, Voraussetzungen für die digitale Souveränität Österreichs und Europa

Österreichs Wirtschaft und Gesellschaft befinden sich aufgrund der digitalen Vernetzung im größten Transformationsprozess der letzten Jahrzehnte. Ein Leben ohne digitale Informationstechnologien ist heute kaum noch vorstellbar. Analysten von Gartner prognostizierten, dass im Jahr 2017 bereits 8,4 Milliarden Maschinen, Geräte oder Fahrzeuge mit dem Internet verbunden sind. Gerade das Internet der Dinge (IoT) trägt durch die rasante Zunahme mangelhaft geschützter Geräte im Internet dazu bei, eine Vielzahl neuer Angriffsszenarien zu ermöglichen. Laut einer Studie von KPMG waren 61 Prozent österreichischer Unternehmen in den letzten zwölf Monaten Opfer einer Cyberattacke.

Die Sicherheit der genutzten Daten, ihre Vertraulichkeit, Integrität und Verfügbarkeit, spielt dabei eine wesentliche Rolle. Es sind nämlich genau diese Faktoren, welche letztendlich die Akzeptanz digitaler Lösungen im privaten wie auch im öffentlichen Leben bestimmen. Erst durch eine strategisch gesteuerte Stärkung von Cyber Sicherheit kann somit das volle Potential der Digitalisierung ausgeschöpft werden, wodurch sich eine starke, digitale Wirtschaft in Österreich entwickeln kann. Aus diesem Grund ist die Zusammenarbeit von Wirtschaft, Politik und anderen Stakeholdern, etwa aus dem akademischen Bereich, im Rahmen von cybersicherheitspolitischen Initiativen von hoher Bedeutung. Dank ganzheitlicher Security-Ansätze soll es diesen Initiativen gelingen, geeignete Rahmenbedingungen zu schaffen, um die Übertragung, Speicherung und Nutzung von Daten ausreichend gegen Ausspähung, Manipulation oder Zerstörung zu schützen. Diese Stärkung der Cyber Sicherheit in Österreich kann nur durch die Zusammenarbeit, den Erfahrungsaustausch und durch Kooperationen auf nationaler und internationaler Ebene gelingen.

In der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) werden Angriffe aus dem Cyber Raum als unmittelbare Gefahr für unsere Sicherheit und für das Funktionieren von Staat,

Wirtschaft, Wissenschaft und Gesellschaft genannt. Es gehört somit zur obersten Priorität aller österreichischen Stakeholder auf nationaler und internationaler Ebene, gemeinsam an der Absicherung des Cyber Raums zu arbeiten. Um dies zu gewährleisten, sieht die ÖSCS vor, den neuesten Entwicklungen im Cyber Raum in der Praxis Rechnung zu tragen. Dies geschieht beispielsweise im Rahmen von Cyber Übungen, wo die Praxistauglichkeit der organisatorischen Strukturen, Notfallpläne und -dokumentationsprozesse der betroffenen Stakeholder geübt wird. Das Ziel dabei ist es, im Fall einer Cyberattacke die stressbedingte Fehleranfälligkeit bei den betroffenen Akteuren zu minimieren und die dahingehend bereits umgesetzten Maßnahmen in einem „sicheren" Übungsrahmen zu überprüfen. Im Jahr 2017 konnten sich die österreichischen Stakeholder, darunter auch CERT.at und das GovCERT, bei mehreren solchen Cyber Übungen bewähren.

Im vorliegenden Internet-Sicherheitsbericht zeigen wir die aktuellen Herausforderungen, mit denen unsere Gesellschaft konfrontiert ist auf, und geben einen Überblick über die 2017 gesetzten Aktivitäten und Maßnahmen von CERT.at und dem im Bundeskanzleramt angesiedelten GovCERTAustria. So wurden beispielsweise die bereits bestehenden CERT-Strukturen (CERT-Verbund, GovCERT) auf nationaler und auf Behördenebene weiter gefestigt, ausgebaut und operationalisiert. Das Bundeskanzleramt arbeitet weiters im Rahmen vom GovCERT gemeinsam mit seinen Partnern intensiv daran, das Thema der Cyber Sicherheit in Österreich strategisch zu verankern und gleichzeitig für die Betroffenen zugänglich zu machen, um so deren Wertschätzung für die Digitalisierung von Wirtschaft und Gesellschaft unter sicheren Rahmenbedingungen zu erhöhen.

Mag. Robert Schischka

Leiter des Computer Emergency Response Teams (CERT.at)

Produkte und Dienstleistungen sind von funktionierender IT-Unterstützung abhängig

Auch im Jahr 2017 ist das Thema IT-Security nicht aus den Schlagzeilen verschwunden, mit WannaCry und NotPetya gab es zwei Vorfälle, die auch in der breiten Öffentlichkeit wahrgenommen wurden. Zunehmend wird klar, wie sehr Produkte und Dienstleistungen in unserer modernen Gesellschaft von einer funktionierenden IT-Unterstützung abhängig sind. Eine Störung in der „virtuellen Welt der Daten" führt daher sehr schnell zu Ausfällen im „realen Leben". Diese mögen in vielen Fällen noch relativ harmlos sein, wie etwa die durch WannaCry gestörten Zugsanzeigen der Deutschen Bahn. In anderen Fällen kann dies aber schwerwiegende Konsequenzen haben - beispielsweise die durch NotPetya hervorgerufenen Ausfälle in der IT-Infrastruktur des weltweiten größten Containertransportunternehmens Maersk. Letztere führten zu Störungen in der Verladung und haben kurzfristig die globale Supply-Chain Infrastruktur ins Wanken gebracht und Schäden in dreistelligen Millionenbereich verursacht.

Die NIS-Direktive, die genau solche Szenarien adressiert, wurde auf EU-Ebene bereits 2017 verabschiedet, die volle Umsetzung in nationales Recht ist aber erst für 2018 vorgesehen. Trotzdem sind 2017 viele der Bausteine dieses Konstrukts aktiv geworden: Die Kooperationsgruppe hat sich konstituiert und arbeitet seitdem an der EU-weit harmonisierten Umsetzung der Direktive in Bezug auf die Identifikation der Betreiber wesentlicher Dienste und vorgeschriebener Sicherheitsmaßnahmen.

Auch das CSIRTs-Netzwerk – eine Austauschplattform der jeweiligen nationalen CSIRTs - hat 2017 seinen offiziellen Betrieb aufgenommen. Die österreichischen Vertreter dort sind CERT.at, das österreichische GovCERT und das Austrian Energy CERT (AEC).

Das Austrian Energy CERT ist eine Initiative der österreichischen Energiewirtschaft, die auf Grund einer ausführlichen Risikoanalyse zu dem Schluss gekommen ist, dass ein sektorales IT-Sicherheitsteam (wie im NIS-Gesetz vorgesehen) für die Resilienz der Branche ein wichtiger

Schritt ist. Im Mai 2017 hat das AEC seinen Testbetrieb aufgenommen, es arbeitet wie das GovCERT in enger personeller Kooperation mit CERT.at.

2017 war daher für die CERTs wieder ein spannendes Jahr, in dem neben der täglichen, technischen Arbeit für die IT-Sicherheit in Österreich auch sehr viel Kommunikation und Koordination auf allen Ebenen, global im CERT-Dachverband FIRST, über europäische Foren bis hin zu nationalen Initiativen, von der Mitgestaltung des NIS-Gesetzes, über nationale Lagebildprozesse bis zu gemeinsamen technischen Analysen auf der Agenda stand.

Der hier vorliegende Jahresbericht soll einen Einblick in die Arbeit von CERT.at und GovCERT geben und zeigt klar, dass diese Kooperation zwischen nic.at und Bundeskanzleramt eine wichtige Säule in der IT-Sicherheitsstrategie von Österreich ist und bleibt.

2 CERT.at – Österreichs Experte für Internet-Sicherheit seit 2008

CERT.at ist das österreichische, nationale Computer Emergency Response Team, das im Jahr 2008 gemeinsam mit dem GovCERT Austria vom Bundeskanzleramt (BKA) in Kooperation mit nic.at, der österreichischen Domain-Registrierungsstelle, als Projekt bei nic.at eingerichtet wurde. Als solches ist CERT.at der Ansprechpartner für IT-Sicherheit im nationalen Umfeld und ist für alle jene Fälle zuständig, die nicht durch ein spezifischeres CERT (etwa ein Sektor-CERT) abgedeckt werden.

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

Damit ist CERT.at in seinem Tätigkeitsfeld mit einer gesamt-österreichischen „Internet-Feuerwehr" gleichzusetzen, die laufendes Monitoring betreibt, Informationen weitergibt, sich effektiv national und international vernetzt und natürlich 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 neun Personen und wird von Robert Schischka geleitet.

Eine wichtige Abgrenzung: CERT.at ist keine Ermittlungsbehörde und befasst sich daher nicht mit dem Thema der Strafverfolgung im Internet. Es hat kein Durchgriffsrecht auf die Netzwerkinfrastruktur Österreichs und kann bei Sicherheitsvorfällen nur koordinierend und beratend aktiv werden.

Der CERT-Beirat: Strategische Leitplanken

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

Enger Verbund mit anderen Einrichtungen

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

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

2.1 GovCERT Austria: Die SpezialistInnen 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.

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

Das GovCERT leistet, neben der oben beschriebenen Rolle als Internetfeuerwehr und intensiver Netzwerker im öffentlichen Bereich, zentrale Aufgaben in der Koordination zwischen den einzelnen Stellen der öffentlichen Verwaltung in Angelegenheiten der Cybersicherheit. Dabei nimmt GovCERT schon heute die zukünftigen Aufgaben der sektoralen Meldestelle wahr, die unter der NIS-Richtlinie[1] zu implementieren ist.

Im Zentrum stehen für GovCERT dabei die Sammlung und Bewertung von Vorfällen aus dem operativen IKT-Betrieb der Bundes-, Landes-, Städte- und Gemeindeverwaltungen sowie der verfassungsmäßigen Einrichtungen des Bundes, das Setzen von Präventivmaßnahmen sowie die Bündelung sicherheitstechnischer und operativer Expertise für den Bereich der öffentlichen Verwaltung. Das GovCERT überwacht dabei Sicherheitsvorfälle auf nationaler Ebene und gibt Frühwarnungen und Alarmmeldungen sowie Bekanntmachung über Risiken und Vorfälle heraus. Es reagiert auf Sicherheitsvorfälle, unterstützt bei Bedarf auch vor Ort und erweitert

[1] Netzwerk-und Informationssicherheits-Richtlinie

sein Wissen und Netzwerk durch die Koordination und Teilnahme an nationalen und internationalen Cyber-Übungen.

Hoher Mehrwert durch zahlreiche Synergien in der PPP

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

2.2 CERT.at und GovCERT Austria – Unverzichtbar im Managen von Bedrohungen

Die Notwendigkeit der von CERT.at und GovCERT Austria wahrgenommenen Aufgaben wird durch die gestiegenen IT-Sicherheitsbedrohungen der letzten Jahre deutlich. So konnte festgestellt werden, dass Angreifer zunehmend professioneller, intelligenter und mehrdimensional agieren.

Die Aktivitäten von CERT.at - und damit auch das Ausmaß an Bedrohungen - sind in den letzten Jahren deutlich gestiegen - von 1897 Vorfällen im Jahr 2009 auf 8556 im Jahr 2017. 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 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 stützten sich CERT.at und GovCERT neben der eigens entwickelten Sensorik auf Quellen innerhalb der internationalen Gemeinschaft der IT-Sicherheitsbranche. Ziel ist es, das Niveau der Netzwerksicherheit in Österreich, durch die

[2] Operative Koordinierungsstrukturen im Cybersicherheitsfall
[3] IKDOK (Inneren Kreis der operativen Koordinierungsstrukturen) nimmt zentrale Aufgaben der operativen Koordinierungsstruktur wahr.

Übermittlung von Informationen über Sicherheitsprobleme an betroffene Betreiber, laufend zu heben.

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

2.3 CERT.at – Zertifizierungen im Jahr 2017

ISO 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 27 001/2017 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 27 001 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 27 001 zertifiziert. Gemeinsam beschloss man im Zuge des ersten großen Re-Audits von nic.at (nach drei Jahren) auch die Zertifizierung von CERT.at und GovCERT anzustreben. Eine gemeinsame Zertifizierung von nic.at und CERT.at im Jahr 2014 wäre wegen der unterschiedlichen Anforderungen und getrennten System zu aufwändig gewesen. Der notwendige Prozess und alle Maßnahmen zu ISO-Zertifizierung von CERT.at und GovCERT wurde im Jahr 2017 erfolgreich angeschlossen.

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 2018) eines von sechs nationalen CERTs in Europa, das mit dem TI-Prädikat „**Certified"** ausgezeichnet wurde. Das ist die höchste Stufe des Trusted Introducer Zertifizierungsrasters. Das GovCERT wird als „listed" geführt.

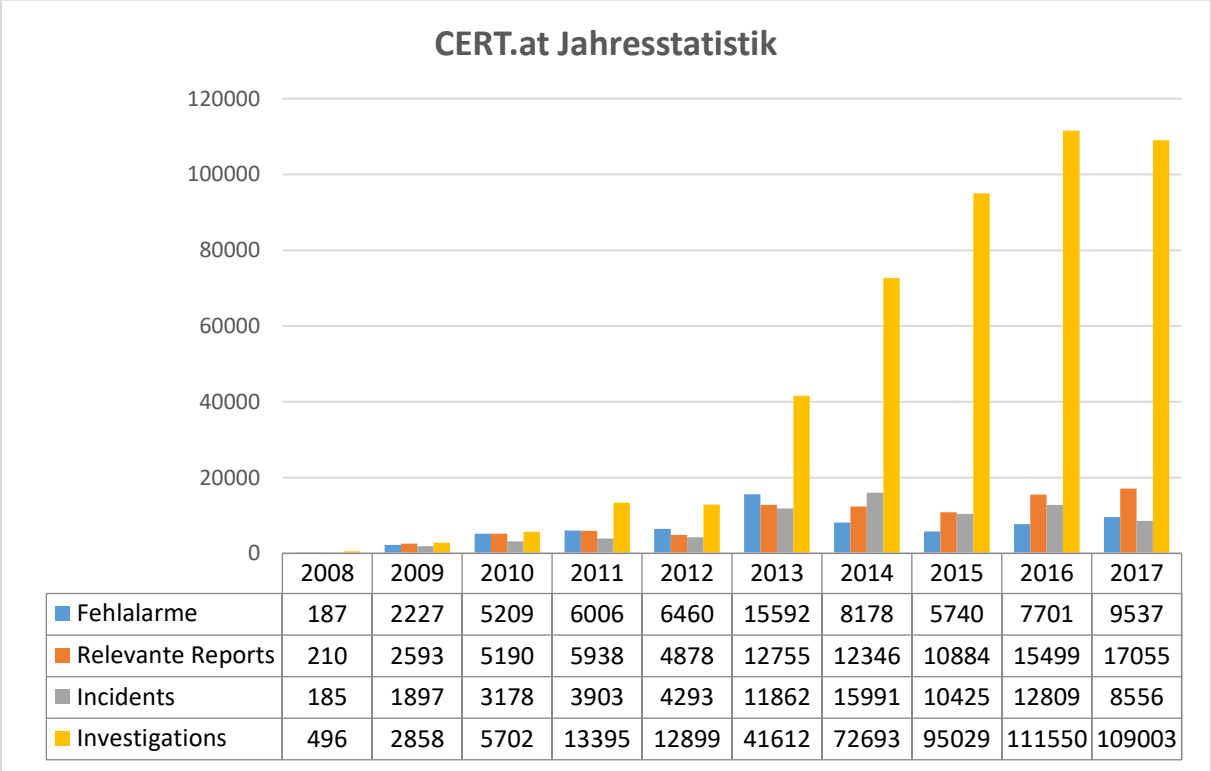
3 Das IT-Sicherheitsjahr 2017 aus Sicht von CERT.at und GovCERT

3.1 CERT.at Jahresstatistiken 2017

CERT.at und GovCERT Austria führen im Zuge ihrer Arbeit umfangreiche Statistiken, die einen Überblick über die aktuelle Internet-Sicherheitslage Österreichs und die wichtigsten Daten des vergangenen Jahres ermöglichen. Auf diese wird in Folge eingegangen.

Das Team von CERT.at führt seit dem Jahr 2008 Gesamt-Jahresstatistiken. Diese beinhalten die Zahl der relevanten **Reports, Incidents** und **Investigations** (nachfolgend eingehend erklärt) sowie auch **Fehlalarme**. Über den gesamten Zeitverlauf – von 2008 bis 2017 – zeigt Abbildung 1 die Intensivierung der Arbeit von CERT.at zur kontinuierlichen Verbesserung der Cyber Sicherheit in Österreich.

Da CERT.at im Jahr 2017 einige Veränderungen in der automatisierten Verarbeitung von Informationen zu Infektionen vorgenommen hat, sind die Zahlen von 2017 nicht direkt mit jenen von 2016 vergleichbar.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701	9537
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003

Abbildung 1: CERT.at Jahresstatistik mit Übersicht über Reports, Incidents und Investigations im Zeitverlauf, Quelle: CERT.at

Die wichtigsten einzelnen Kennzahlen: Reports, Incidents und Investigations

"Reports" bezeichnen eingehende Meldungen an CERT.at. Nicht alle davon beschreiben einen Sachverhalt, der von CERT.at als relevanter Vorfall (Incident) eingestuft wird und eine aktive Behandlung erfordert. Typische Gründe für eine Beurteilung als irrelevanter Vorfall (Fehlalarm) sind etwa:

- Meldungen zu Problemen, die bereits bereinigt wurden
- Falschmeldungen von einfachen Suchalgorithmen
- Mangelnde Zuständigkeit von CERT.at (z.B. die gemeldete IP-Adresse ist nicht in Österreich)
- Generische Anfragen (etwa Konferenzeinladungen, Frage zu den Mailinglisten etc.)
- E-Mail Irrläufer, Spam und automatische Antworten („Autoresponder")

Abbildung 2 zeigt die relevanten Reports, die im Jahr 2017 an CERT.at gesendet wurden. Die Anzahl der Reports wird pro Monat angegeben und ermöglicht dadurch einen guten Jahresvergleich in den 15 größten, durch CERT.at behandelten Bedrohungskategorien. Im Schnitt waren es rund 1300 Meldungen pro Monat. Die großen Schwankungen zwischen den Monaten sind auf Umstellungen in der Verarbeitung von automatisierten Berichten zurückzuführen (siehe weiter unten). Die hohen Defacement- und Exploit-Packzahlen im Februar und März 2017 sind im Abschnitt *Gehackte Webseiten in .at* näher erläutert.

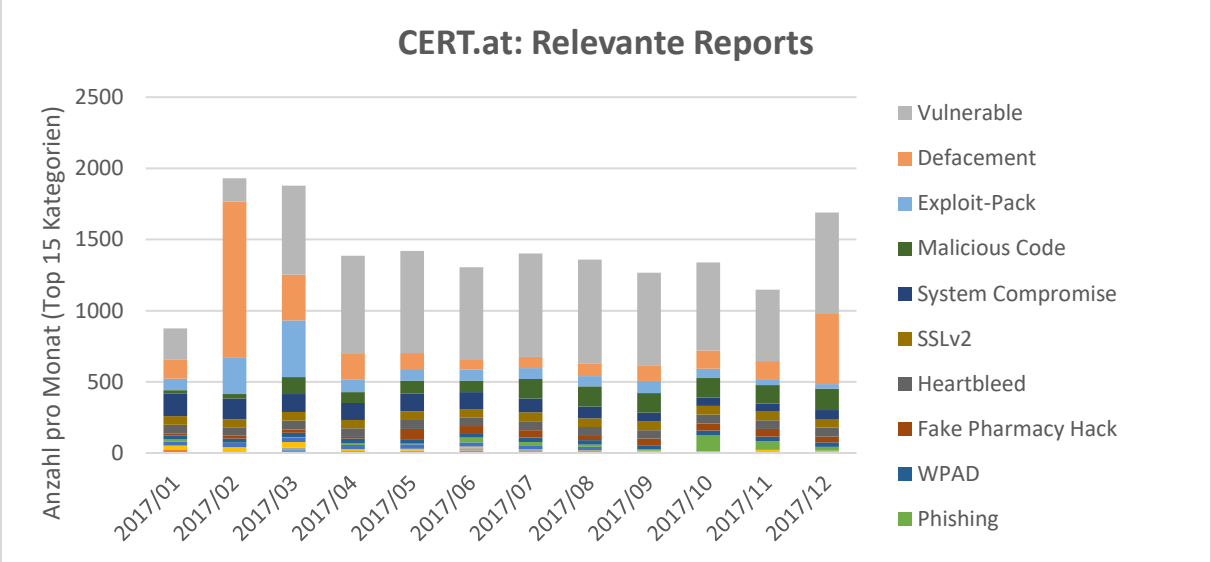


Abbildung 2: Klassifizierung der relevanten Reports nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Als "Incidents" werden jene Fälle eingestuft, die tatsächlich ein Sicherheitsrisiko darstellen. Bei diesen wird CERT.at aktiv und informiert beispielsweise betroffene Unternehmen, Organisationen oder PrivatanwenderInnen über IT-Sicherheitsbedrohungen und unterstützt in besonderen Fällen gegebenenfalls auch bei der Problemlösung.

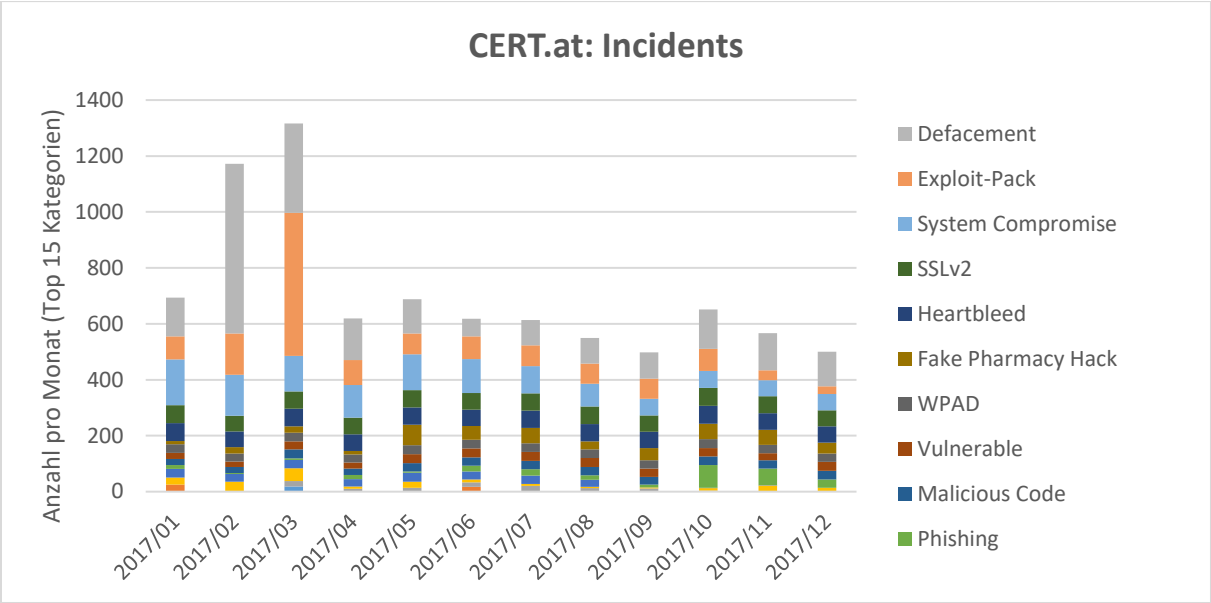


Abbildung 3: Klassifizierung von Incidents nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Die Kontaktaufnahme mit den betroffenen Unternehmen, Organisationen oder PrivatanwenderInnen wird im CERT.at Ticketsystem als "Investigation" bezeichnet.

Abbildung 4 zeigt die Zahl der Investigations im Jahr 2017. Eine Investigation ist üblicherweise eine E-Mail an den Netzbetreiber, Webhoster oder Domaininhaber. CERT.at verschickt an einem typischen Tag rund 300 E-Mails. Da in vielen Incidents Daten zu mehreren Netzbetreibern enthalten sind, kommen auf einen Incident im Schnitt rund 16 Investigations.

Im Jahr 2016 war dieses Verhältnis mit acht Investigations pro Incident deutlich niedriger. Diese Steigerung ist zum Großteil auf eine im nächsten Abschnitt näher beschriebene Umstellung bei der Verarbeitung von automatisierten Berichten zu Sicherheitsvorfällen zurückzuführen. Da das neue System Incidents nicht mehr pro Quelle, sondern pro Kategorie erstellt, sinkt die Anzahl pro Tag drastisch, was auch in der Grafik zu den Incidents gut erkennbar ist. 2016 lag die durchschnittliche Anzahl der Incidents bei 900 pro Monat, ab April 2017 lag diese bei nur mehr 500.

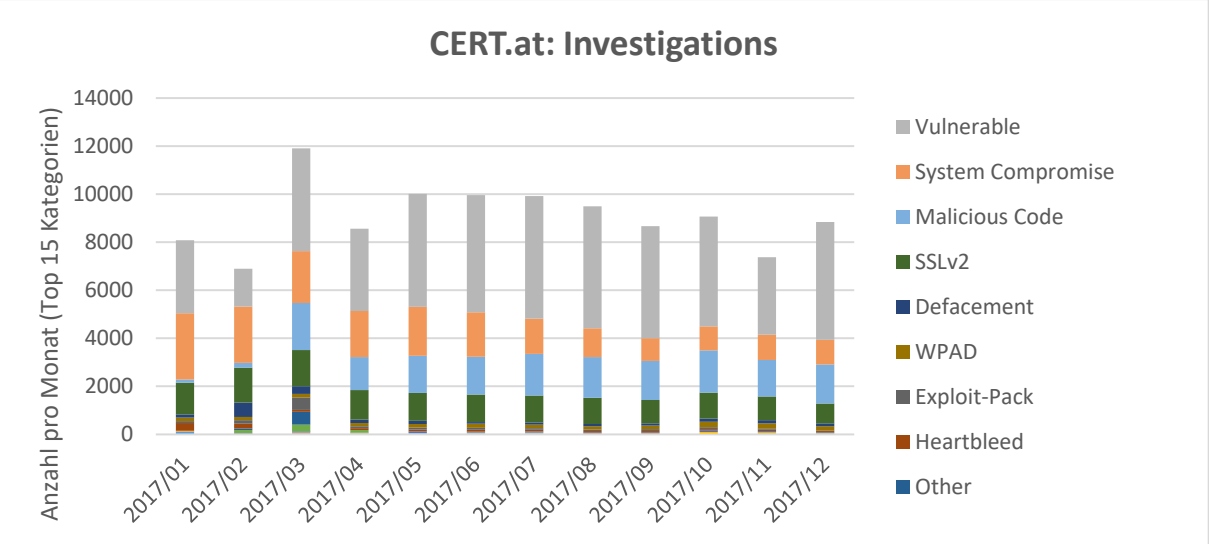


Abbildung 4: Klassifizierung der von CERT.at durchgeführten Investigations nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

3.2 Netzhygiene

CERT.at sammelt Informationen zu konkreten Sicherheitsproblemen im österreichischen Teil des Internets, wie etwa infizierte Computer, manipulierte Webseiten oder fehlkonfigurierte Server. Dazu stützten sich CERT.at und GovCERT neben der eigens entwickelten Sensorik auf Quellen innerhalb der internationalen Gemeinschaft der IT-Sicherheitsbranche. Ziel ist es, das Niveau der Netzwerksicherheit in Österreich durch Informationen über Sicherheitsprobleme an betroffene Betreiber von IKT laufend zu heben.

IntelMQ - Open Source Software zur Verarbeitung von Informationen über Infektionen und Fehlkonfigurationen

Seit 2016 wird die Verarbeitung von automatisierten Berichten zu Sicherheitsvorfällen bei CERT.at von einer halbautomatischen Verarbeitung durch eine vollautomatische Verarbeitung mit IntelMQ ersetzt. IntelMQ wird als gemeinsames Projekt von mehreren europäischen CERTs als Open Source Software entwickelt, und wird von CERT.at im Rahmen der Förderung der EU für CERTs (Connecting Europe Facility Telecom, Cyber Security Call 2+3) maßgeblich betreut und weiterentwickelt.

Im Zuge dieser Umstellung wurde auch die Zuordnung von Einzelereignissen zu Tickets geändert. Einzelereignisse sind eine Sicherheitslücke, Fehlkonfiguration oder Malwareinfektion eines einzelnen Geräts (PC, Server). Diese Umstellung ist in den Statistiken des Ticketsystems zu erkennen, da sie aber schrittweise erfolgte, ist kein klarer Umstellungszeitpunkt mit entsprechenden Änderungen in den Grafiken sichtbar.

Früher wurden alle Datenquellen (etwa Ergebnisse der Scans von ShadowServer, oder Daten von Microsofts Digital Crime Unit) unabhängig voneinander verarbeitet. Da diese typischerweise einmal pro Tag einen Datensatz liefern, ergab sich so pro Quelle ein Report, ein

Incident und dann pro vorkommendem Netzbetreiber eine Investigation. Nach der Umstellung gibt es zwar weiterhin tägliche Reports dieser Quellen, aber die Inhalte werden erst zusammengefasst und dann aufbereitet an die Netzbetreiber weitergesendet, anstatt umgekehrt, wie dies früher geschah. Weiters können nun auch Stream-basierte Datenquellen, bei denen ein ständiger Datenfluss besteht, anstatt eines täglichen Berichtes, direkt und einfacher verarbeitet werden. Das neue System basiert auf Einzelereignissen, genannt „Events", die jeweils eine einzelne Beobachtung bzw. Messung darstellen. Diese werden täglich pro Kategorie („Taxonomie") als ein Incident zusammengefasst und verarbeitet. Die dahinterstehende Taxonomie geht ebenfalls aus einer europäischen Zusammenarbeit hervor („eCSIRT II Taxonomy"). Damit soll erreicht werden, dass sowohl der Datenaustausch zwischen den CERTs, als auch ein länderübergreifender Vergleich der Statistiken, einfacher wird. Zu diesem Zweck nimmt CERT.at auch am europäischen Projekt „Reference Security Incident Taxonomy Task Force" zur Weiterentwicklung der Taxonomie für CSIRTs teil.

Der Effekt dieser Umstellung ist in den Graphen der Investigations gut erkennbar: So wurden die getrennten Investigations zu DDoS-Reflektoren per SNMP, NTP oder SSDP in E-Mails zu verwundbaren Systemen ("Vulnerable") zusammengefasst. Da es zwischen den Infektionsdaten-Quellen immer wieder Überschneidungen gibt, ermöglicht diese Vorgehensweise eine Vermeidung mehrfacher Einträge in Investigations und somit eine einfachere Verarbeitung durch die Netzbetreiber.

Da IntelMQ nicht mehr auf tägliche Reports per E-Mail angewiesen ist, ist es möglich die Infektionsdaten direkt ohne Verzögerung den Netzbetreibern weiterzuleiten. Es ist geplant, den Netzbetreibern ein Webportal zur Verfügung zu stellen, mit welchem diese die den Umfang, das Intervall sowie die Beschaffenheit der bezüglich ihres Bereiches gesendeten CERT-Meldungen selbst konfigurieren können.

Diese Umstellung beeinflusst die Vergleichbarkeit der Report/Incident/Investigation Zahlen mit den historischen Daten natürlich negativ. Dem ist jedoch entgegenzuhalten, dass die Zahl der E-Mails von CERT.at allein seit Beginn dieser Auswertungen nur bedingt etwas über den Sicherheitsstatus in Österreich ausgesagt hat. Grund dafür ist der Umstand, dass eine E-Mail, welche lediglich eine Infektion enthält, in dieser Betrachtungsweise einer E-Mail, welche tausende IP-Adressen enthält, rechnerisch gleichgestellt wurde. Aufgrund dieser Unschärfe ist die schlichte Anzahl gesendeter E-Mails zu Infektionen daher in ihrer Aussagekraft als Gradmesser für einen Status der Cybersicherheit in Österreich ungeeignet und sollte dafür nicht herangezogen werden.

Die Umstellung auf IntelMQ betrifft nicht die Meldungen über gehackte Webseiten und Phishings (in den Graphen sind dies die Kategorien Exploit Pack, Fake Pharmacy Hack, Phishing und Searcheengine Ranking Hack), diese wurden auch in der Vergangenheit schon als Einzelereignisse verarbeitet. Aussagekräftigere Lageinformationen bekommt man aus den Daten zu Events, die den folgenden Statistiken zugrunde liegen.

Botnetze in Österreich

Die vorhandene Datenbasis hinsichtlich der in Österreich verbreiteten Botnetze hängt sehr stark von der Möglichkeit ab, diese Daten auch erheben zu können. Bessere Daten sind daher vor allem für ältere Botnetze vorhanden, da diese bereits gut analysiert sind und entsprechende Sensoren ("Sinkholes") betrieben werden. Da verschiedene Quellen unterschiedliche Bezeichnungen für die gleiche Malware verwenden, harmonisiert CERT.at diese mit einer auch öffentlich verfügbaren Zuordnungstabelle. In der folgenden Grafik werden die Meldungen nach Malwarefamilie in Österreich dargestellt.

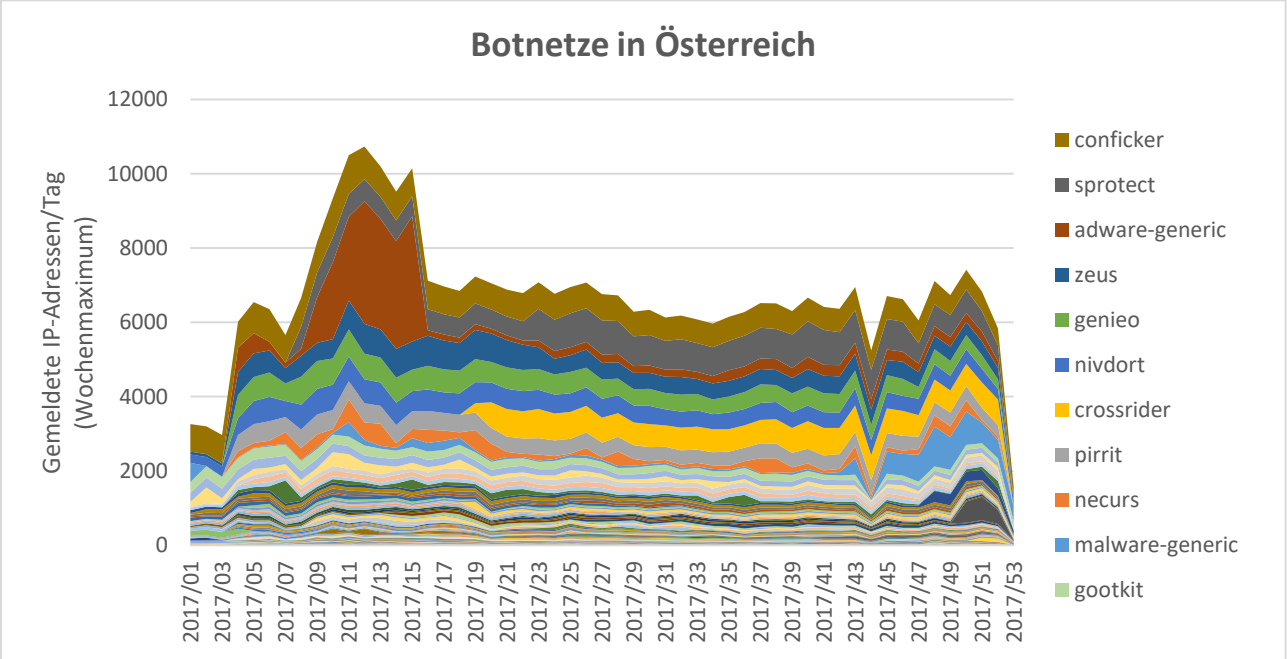


Abbildung 5: Klassifizierung der Meldungen nach Botnetzen im Zeitverlauf (Wochen) des Jahres 2017 bis Ende 2017, Quelle: CERT.at

Denial of Service-Attacken – DoS und DDoS

DoS (Denial of Service) und DDoS (Distributed Denial of Service) Attacken zählen derzeit zu den häufigsten und wirksamsten Cyber Attacken. Vor allem in der Industrie und dem Finanzwesen werden diese Angriffe eingesetzt, um Unternehmen unter Druck zu setzen und hohe Summen an Schutzgeld einzufordern.

DDoS-Attacken legen Webserver oder ganze Netzwerke lahm. Im Gegensatz zu einer einfachen DoS-Attacke haben DDoS-Angriffe eine wesentlich höhere Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund (beispielsweise über ein Botnetz) eine Webseite oder eine ganze Netzinfrastruktur an. Das angegriffene System wird mit (teils sinnlosen) Anfragen überflutet, die mit den dort zur Verfügung stehenden Ressourcen nicht mehr schnell genug abgearbeitet werden können. Typische DDoS-Angriffe zielen dabei regelmäßig auf die Überlastung der Internetanbindung, der Ressourcen der Netzwerkkomponenten sowie der Web- und Datenbankserver ab.

DDoS-Angriffe lassen sich im Wesentlichen in **drei Gruppen** kategorisieren:

- **Quantitative Angriffe:** Diese versuchen, das Zielsystem durch den Angriff zu überlasten. Dabei kommen in der Regel keine hochspezialisierten Angriffsvektoren zum Einsatz, sondern der gewünschte Effekt wird allein durch die Menge des Datenverkehrs erzielt.
- **Qualitative Angriffe:** Diese versuchen primär, Schwachstellen in Systemen gezielt auszunutzen, um so die Erbringung dieses Dienstes für die dafür vorgesehenen BenutzerInnen einzuschränken oder gänzlich zu unterbinden. Solche Angriffe setzen zumeist ein höheres technisches Niveau der Angreifer voraus.
- **Eine Kombination daraus:** Durch Verschränkung von quantitativen und qualitativen Angriffen können Systeme noch effizienter gestört werden.

DDoS-as-a-Service

Gegenwärtig ist in immer stärkerem Ausmaß die Entwicklung zu beobachten, dass DDoS-Angriffe im Internet unkompliziert als „Dienstleistung" „eingekauft" werden können. So bieten im „Darknet" zahlreiche Anbieter gegen vergleichsweise geringes Entgelt die Möglichkeit, Angriffe nach Dauer und Volumen preislich gestaffelt zu ordern. In den letzten Jahren konnten einige dieser Anbieter enttarnt und verhaftet werden.

So funktioniert ein DoS/DDoS-Angriff im Detail

Bei DoS-Angriffen werden häufig Schwächen in Anwendungen, Betriebssystemen oder Webprotokollen ausgenutzt. Die Attacken können in verschiedenen Varianten durchgeführt werden:

- Syn Flooding
  Soll eine TCP-Verbindung - etwa zum Abruf einer Webseite - aufgebaut werden, so führt dies zu einem Austausch von SYN- und ACK-Datenpaketen zwischen Client und Server (dies wird auch „TCP-Handshake" genannt). Im Falle eines Syn Flooding-Angriffs werden von den Angreifern viele SYN-Pakete losgeschickt, die jeweils eine gefälschte Absender-IP-Adresse enthalten. Das Zielsystem antwortet auf diese Pakete, so wie dies gemäß TCP-Handshake vorgesehen ist, mit entsprechenden SYN-ACK-Paketen, schickt diese aber an die gefälschten IP-Adressen zurück und erwartet von dort (gemäß eines regulären TCP-Handshakes) Antworten in Form eines ACK-Pakets. Für diese Abhandlung und insbesondere das Warten auf eine Antwort wird vom Zielsystem jeweils etwas Rechenleistung und für eine gewisse Zeit Speicherkapazität in Anspruch genommen. Wenn diese ACK-Pakete jedoch ausbleiben (was bei einer Syn Flooding Attacke der Fall ist), so werden umso mehr Ressourcen gebunden je höher die Rate der empfangenen SYN-Pakete ist. Sind die vorhandenen Verbindungskapazitäten (TCP State Table) des Zielsystems ausgeschöpft, dann kann dieses keine weiteren Verbindungen mehr annehmen und ist damit auch für legitime Anfragen nicht mehr

erreichbar – das Ziel einer DDOS Attacke wurde damit erreicht. Für effektive SYN Flooding Angriffe reichen oft schon Bandbreiten im Bereich von wenigen Mbit/s. Mittels SYN Cookies, welche die Bindung von Ressourcen auf einen späteren Zeitpunkt im Handshake verschieben, lassen sich diese Angriffe allerdings gut abwehren.

- Reflected-DoS-Angriff
  Diese Angriffsvariante zielt auf die Überlastung von Leitungskapazitäten und nutzt legitime, aber schlecht konfigurierte UDP-basierte Server im Internet als Reflektoren/Verstärker von Paketen. Der Angreifer schickt dabei viele (kleine) Anfragen an diese Server, wobei er aber die IP-Adresse des Opfers als Absenderadresse einträgt (IP-Spoofing). Die Server halten diese Anfragen für legitim und beantworten sie mit großen oder mehreren Antwortpaketen. Diese werden aufgrund des IP-Spoofing jedoch an das Opfer anstelle des eigentlichen Senders zugestellt.

Dadurch hat der Angreifer folgende Vorteile:

- Seine Angriffsbandbreite wird durch die Reflektoren verstärkt.
- Nutzt er viele verschiedene Server als Reflektoren, so sieht das Opfer breit verteilte Angreifer, die sich nicht einfach über eine Filterliste ausblenden lassen.
- Der Standort des Angreifers, bzw. die Quelle der gefälschten Pakete ist schwer auszuforschen.

Für eine solche DoS-Reflection lassen sich mehrere **Protokolle** zweckentfremden: Primär betroffen sind UDP-basierte Protokolle, da hier nicht auf Transportebene mittels eines Handshakes die IP-Adresse des Clients validiert wird. Aktuell sind DNS (Domain Name Service), NTP (Network Time Protocol), SSDP (Simple Service Discovery Protocol) die am häufigsten missbraucht werden. Es wurden aber auch schon Angriffe, welche SNMP (Simple Network Management Protocol), portmapper, chargen und sogar LDAP (Active Directory Pings über UDP) verwendeten, beobachtet.

CERT.at informiert die heimischen Netzbetreiber laufend über Server in deren Netzen, die sich für solche Angriffe ausnutzen lassen. Wie Abbildung 6 zeigt, ist es ein langwieriger Prozess, das Netz bezüglich dieser Gefahr zu säubern. Um Reflected-DoS zu unterbinden, ist eine globale Anstrengung nötig, denn das Problem ist mit dem Umweltschutz oder der globalen Erwärmung vergleichbar: Nur wenn alle an einem Strang ziehen, kann sich die Lage nachhaltig verbessern.

- Angriffe auf den Applikationslayer
  Sowohl gegen Webserver, als auch gegen Nameserver wurden in der letzten Zeit spezifische Angriffsmuster beobachtet. Ähnlich wie bei Reflection-Attacks funktionieren etwa Angriffe auf Basis der Pingback Funktion der weit verbreiteten Blogsoftware „Wordpress“. Das grundliegende Prinzip dabei ist der Umstand, dass solche Blogs auf Artikel anderer Blogger verweisen, was gerne mit einem Retour-Link („Folgende Blogs zitieren diesen Artikel“) beantwortet wird. Im Hintergrund notifiziert der zitierende Blog die Quelle eines Verweises, das dortige Wordpress verifiziert das und setzt erst dann den Pingback Link. Dieses Verifizieren ist jedoch ein Problem: Wenn ein Angreifer

tausenden Wordpress-Installationen mitteilt, dass die Webseite eines Opfers gerade einen Link gesetzt hat, dann versuchen die, dies auf die beschriebene Weise zu verifizieren und lösen so eine Überlast beim Opfer aus.
Angriffe auf das Domain Name System werden ebenfalls regelmäßig registriert. Aktuell beobachtet man „Random Subdomain Requests“ als größte Bedrohung: Hierbei werden aus einem Botnet heraus sehr viele Anfragen zu zufällig gewählten Subdomains des Opfers an beliebige Nameserver gestellt. Diese Randomisierung hebt den Effekt von Caches auf, wodurch eine Flut von Anfragen die Nameserver des Opfers erreicht und diese potentiell überlastet.

CERT.at informiert die Netzbetreiber in Österreich laufend darüber, welche IP-Adressen in den jeweiligen Netzen für eine DDoS-Angriffsverstärkung verwendet werden können. Die Entwicklung dafür verwendeter Systeme in Österreich wird in Abbildung 6 dargestellt.

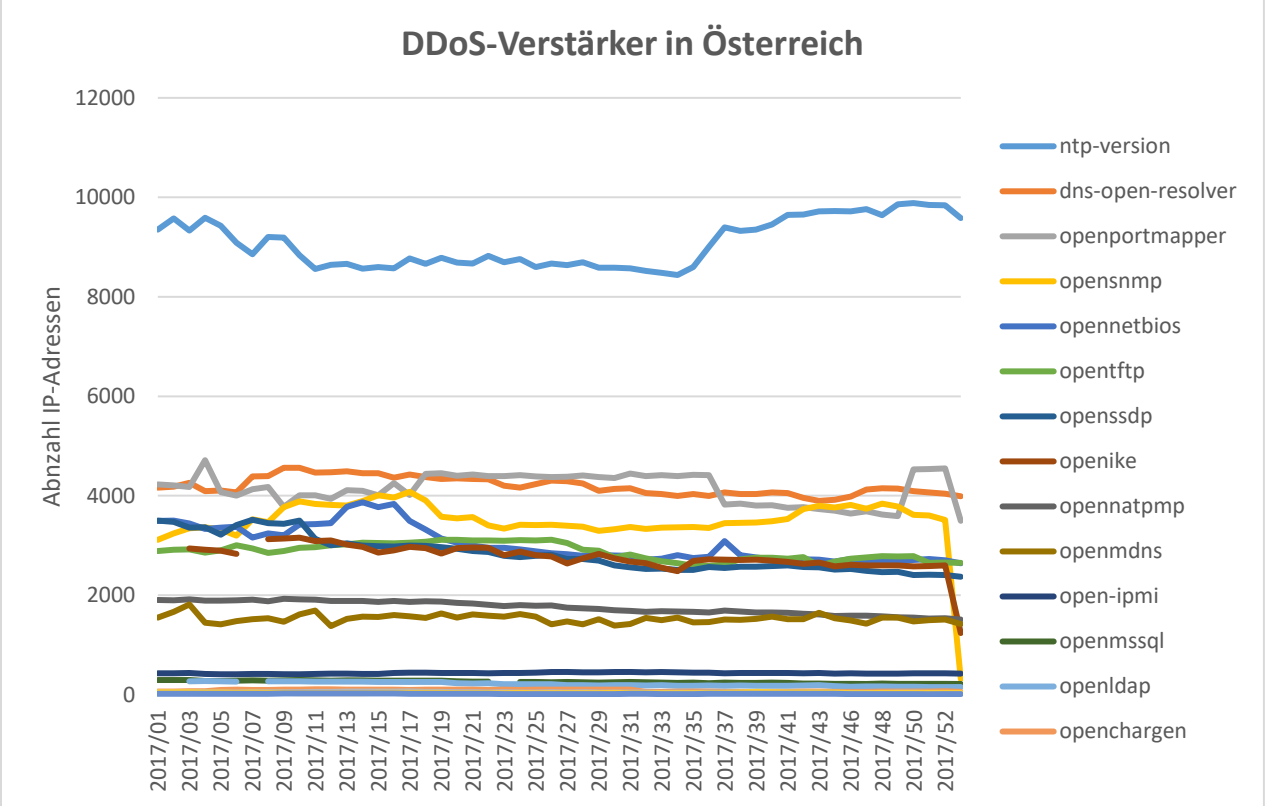


Abbildung 6: Entwicklung der DDoS Reflektoren in Österreich, Quelle: CERT.at 2018

Die Quellen der Daten zu Botnetzen

Die den Statistiken zu Botnetzen zugrundeliegenden Daten stammen aus unterschiedlichen Quellen. Durch die diversen Mess- und Erhebungsmöglichkeiten dieser Daten, die von Aktionen von Strafverfolgungsbehörden bis zu Spuren, die Täter selbst hinterlassen, reichen, wird ein umfassender Blick auf die IT-Sicherheitslage in Österreich ermöglicht. Zu diesen Quellen gehören:

Aktionen von Strafverfolgungsbehörden: Diese Daten stammen aus der Beschlagnahmung von Domains oder Servern von Botnetzen. Dabei werden die ursprünglich von den Angreifern eingesetzten Steuerserver der Botnetze (sog. "Command and Control Server") durch Sensoren (diese werden "Sinkholes" genannt) ersetzt, die für die Strafverfolgungsbehörden mitprotokollieren, von welchen IP-Adressen infizierte Geräte neue Befehle abholen wollen.

Analyse von Malware und Registrierung der verwendeten Domains: 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 kann man durch eine Teilnahme am P2P Protokoll die Mitglieder des P2P-Netzes bestimmen.

In manchen Fällen gelingt es der Polizei, SicherheitsforscherInnen oder CERTs Zugang zu Servern der Angreifer zu erlangen. Die dort vorgefundenen Daten können sehr aufschlussreich sein.

Aktive Suche nach Sicherheitsproblemen: Manche Sicherheitsprobleme können "von außen" überprüft werden. Beispielsweise, ob eine IP-Adresse auf gewisse Protokoll-Anfragen antwortet und sich daher als DDoS-Verstärker missbrauchen lässt.

Operation Avalanche

Am 30. November 2016 wurden durch eine breit angelegte Kooperation von Polizei (Europol, Eurojust, FBI...), Staatsanwälten und IT-Sicherheitsorganisationen (BSI, Shadowserver, CERTs) die Server und Domains der Avalanche Botnetzinfrastruktur übernommen. Ausschlaggebender Grund dafür war Avalanches Beteiligung an mehreren großen Botnetzen. Dies war ein wichtiger Schritt in Richtung eines sichereren Cyber Raumes durch internationale Zusammenarbeit.

Am 1. Dezember 2017 wurden im Rahmen einer Nachfolgeoperation auch die Kontrollserver der Schadsoftwarefamilie Andromeda (auch bekannt unter den Namen Gamarue) übernommen. Im Graphen zur Operation Avalanche ist dieser „Takedown" sehr gut durch einen Anstieg der infizierten Geräte am Ende des Jahres 2017 in den Berichten zu erkennen.

Dies war ein gutes Beispiel für "Aktionen von Strafverfolgungsbehörden", denn statt der echten Command and Control Server nehmen die infizierten PCs mit Sensoren ("Sinkholes") Kontakt auf, die von Sicherheitsforschern im Auftrag der Polizei betrieben werden. Die so erhaltenen Daten werden an CERT.at übermittelt, welches sie wiederum an die Netzbetreiber weiterreicht. Anfänglich wurden mehr als tausend Infektionen in Österreich gemessen:

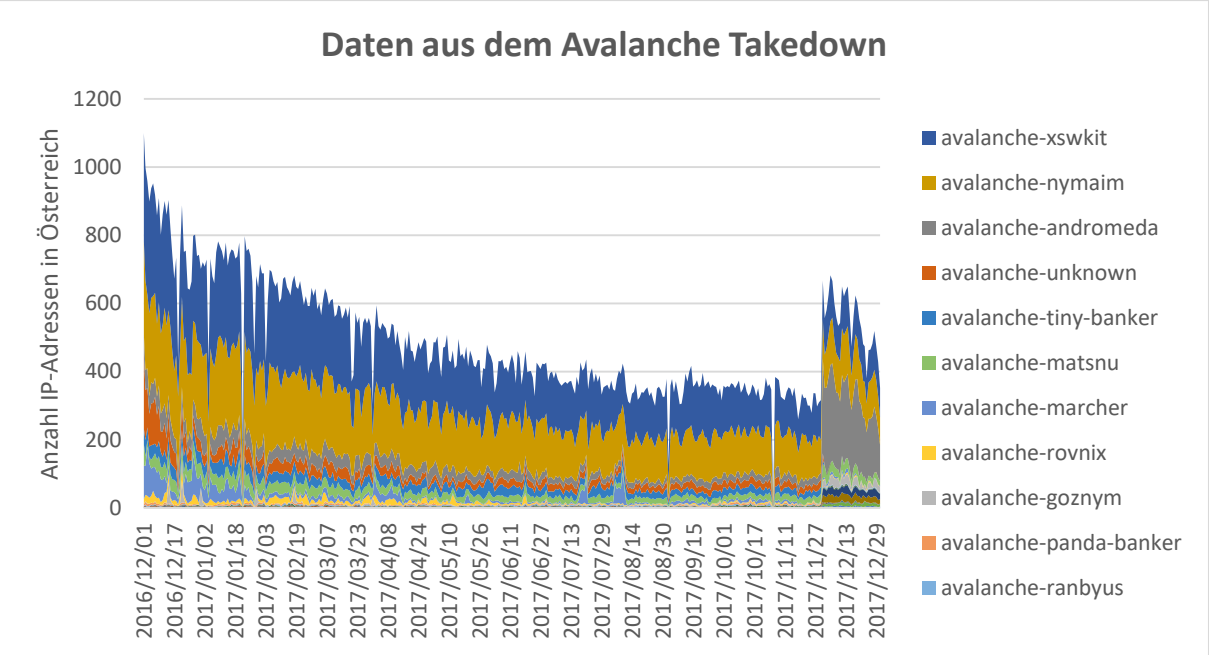


Abbildung 7: Daten aus dem Avalanche Takedown in Österreich, 2016 bis Ende 2017, Quelle: CERT.at

TLS Probleme in .at

Die Verschlüsselungsprotokollfamilie SSL/TLS wird verwendet um HTTP- (Web) und SMTP- (Mail) Datenverkehr zu verschlüsseln. In der Vergangenheit wurden bereits mehrmals protokollarische Schwächen bzw. Sicherheitslücken gefunden, die durch Aktualisierungen der verwendeten Software bzw. durch neuere Versionen von SSL/TLS behoben wurden. CERT.at überprüft täglich alle unter .at-Domains erreichbaren Webseiten und Mailserver auf zwei besonders schwerwiegende Sicherheitslücken, „Heartbleed" und „DROWN".

Die Sicherheitslücke Heartbleed – bekannt geworden im April 2014 – bestand in bestimmten Versionen der Softwarebibliothek openssl, welche von sehr vielen Serverdiensten genutzt wird Entsprechend groß war auch ihre Auswirkung. Durch die Lücke ist es möglich, den geheimen Schlüssel von einem betroffenen Server auszulesen, womit ein Angreifer die Möglichkeit bekommt, den eigentlich verschlüsselten Datenverkehr zu entschlüsseln. Es kann davon ausgegangen werden, dass alle mit Ende 2017 immer noch verwundbaren Systeme nicht aktualisiert und damit nicht betreut werden.

Unter DROWN wird eine Schwäche in der SSL-Version 2.0 verstanden. Diese wurde im März 2016 bekannt. Betroffen sind alle Serverdienste welche diese SSL-Version anbieten bzw. nicht

explizit verbieten. Die Folge ist auch hier wieder, dass ein Angreifer verschlüsselten Datenverkehr entschlüsseln kann. Es ist dringend zu empfehlen die SSL-Version 2.0 sowie auch das Nachfolgeprotokoll SSL 3.0 zu deaktivieren. Empfehlungen zur sicheren Konfiguration von kryptografischer Software finden sich zum Beispiel im Dokument *Applied Crypto Hardening* auf bettercrypto.org.

Die folgenden Abbildungen zeigen einen Überblick über von beiden Sicherheitslücken betroffene Server in Österreich. Die kleinen Sprünge in den Zahlen sind auf Änderungen an den Suchprogrammen und in der zugrundeliegenden Datenbasis zurückzuführen.

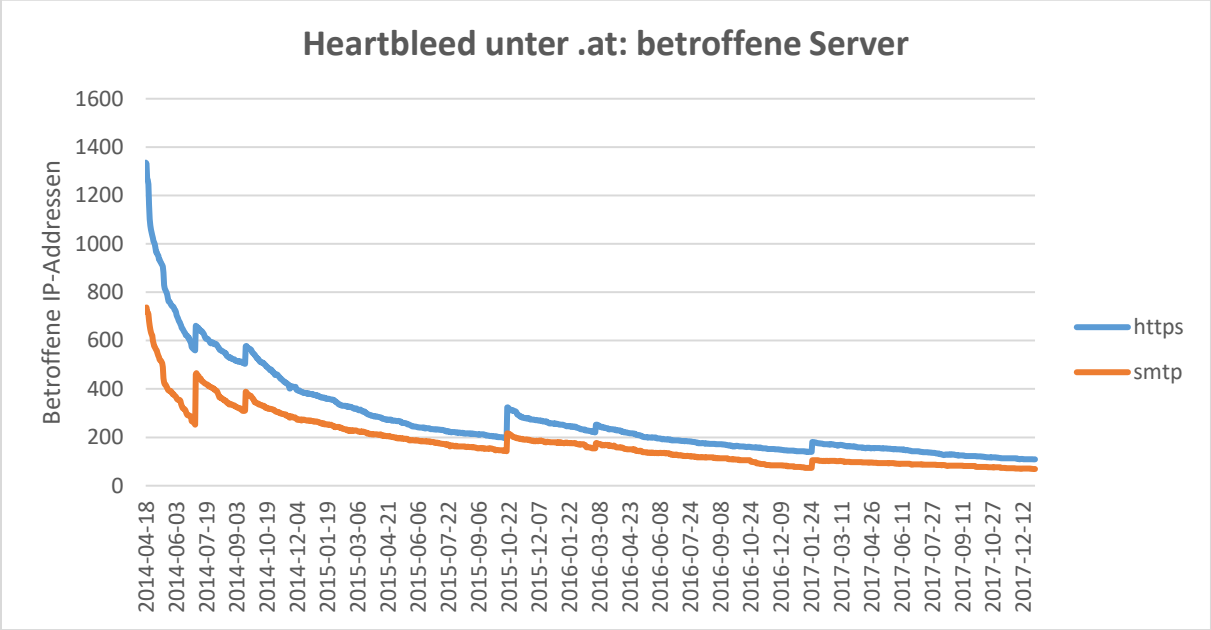


Abbildung 8: Anzahl der IP-Adressen der von Heartbleed unter .at betroffenen Server. Quelle: CERT.at 2018

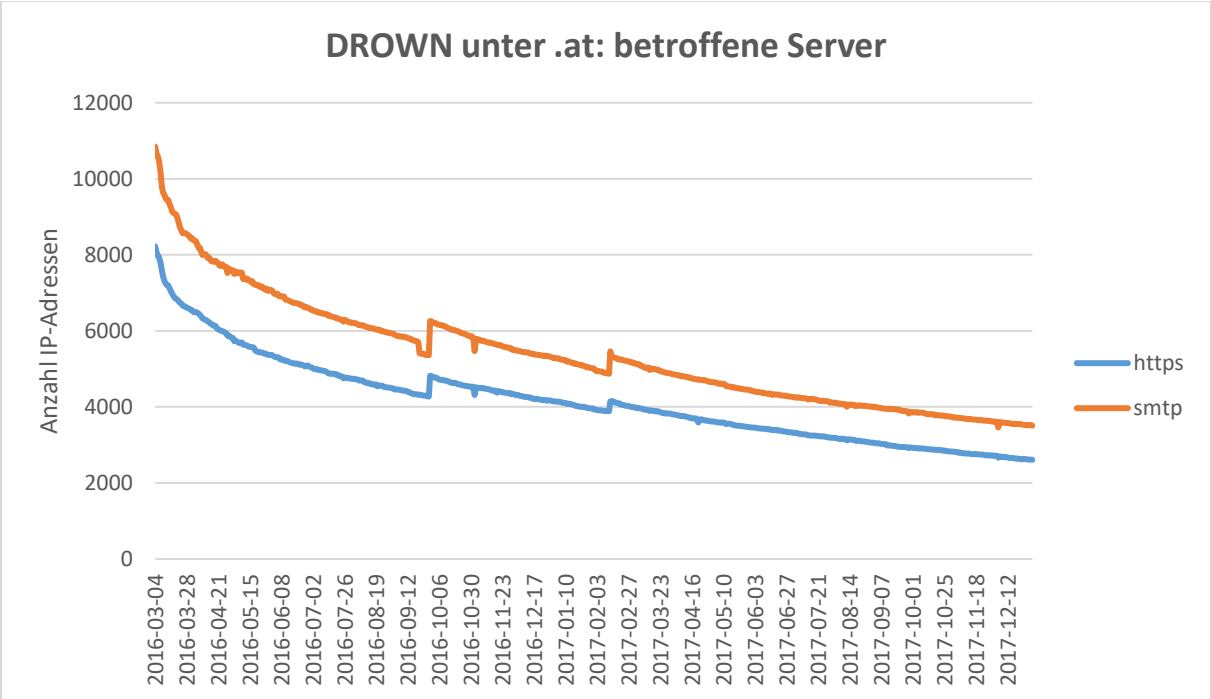


Abbildung 9: Anzahl der IP-Adressen der von DROWN unter .at betroffenen Server. Quelle: CERT.at 2018

Gehackte Webseiten in .at

CERT.at informiert Webseitenbetreiber wenn von außen erkennbar ist, dass deren Webseite gehackt wurde. Es werden dabei mehrere Fälle unterschieden:

Bei Hacks, die nur des Hacks wegen ausgeführt werden, prahlen die Angreifer auf diesen Seiten über ihre Leistung mit expliziten Texten und Bildern (zum Beispiel „Hacked by ...“). Diese Vorfälle werden in den Statistiken unter der Bezeichnung *Defacement* geführt.

Weniger auffällig sind *Exploit-Packs*. Dabei handelt es sich um Manipulationen an der Webseite, welche gezielt die Brower der Besucher angreifen. Ist dieser verwundbar, etwa weil dieser selbst oder eines der installierten Browser-Plugins (Java, Flash, Silverlight, ...) nicht aktualisiert wurden, dann wird damit der PC (oder das Handy/Tablet) des Besuchers mit Malware infiziert.

Bei *Fake-Pharmacy-Hacks* liefern gehackte Webseiten andere Inhalte, wenn die Besucher über eine Suchmaschine auf die Webseite gelangen (abzuleiten aus den sogenannten *Referer*-Informationen). Dadurch erscheinen in den Ergebnissen einer Suchmaschine andere Inhalte auf, die im Großteil der Fälle für Potenzmittel aus dubiosen Quellen werben. Beim direkten Aufruf der Webseiten über das Adressfeld scheinen diese Inhalte nicht auf. Diese Vorfälle werden auch Google Conditional Hacks genannt.

Phishing-Seiten ahmen die Webseiten von Banken, Portale von Firmen, Webmail-Zugänge von Behörden und andere lohnenswerten Zielen nach und verleiten Opfer mit Spam-Kampagnen dazu, diese täuschend echt aussehenden Seiten zu besuchen, um sich dort anzumelden. Die Login-Daten werden dabei vom Angreifer gestohlen.

Unter *Search Engine Ranking Hacks* werden Verlinkungen verstanden, die darauf abzielen, die verlinkte Seite dadurch in den Suchergebnissen höher gelistet aufscheinen zu lassen.

CERT.at stehen mehrere Quellen für Informationen zu gehackten Webseiten zur Verfügung:

Suche mittels Suchmaschinen: Will man nach aktuellen Problemen verwundbarer Webseiten suchen, so kann man dazu auch gängige Suchmaschinen wie Google, Bing usw. benutzen. Dabei wird im Quellcode von Webseiten gezielt nach Auswirkungen von eingeschleustem, schadhaftem Code oder anderen Erkennungsmerkmalen gesucht (etwa bekannte Muster von Exploit-Packs), was ein Indikator dafür ist, dass eine Webseite für böswillige Zwecke missbraucht wird.

Blacklists: Von mehreren Internet Service Betreibern werden "Listen" von als (potentiell) bösartig oder gefährlich eingestuften IP-Adressen, Domains und URLs geführt. Internetnutzer sehen den Effekt dieser Blacklists vor allem dann, wenn ihr Browser vor dem Besuch einer Phishing-Seite warnt.

Die Täter selbst: So melden etwa einige der Einbrecher in Webseiten ihre "Defacements" bei zone-h.org. Gestohlene Daten aus Datenbankeinbrüchen landen auch oft auf "pastebin".

Wenn mehrere Webseiten eines Dienstleisters (Hosters) oder Webseiten, die mit der gleichen Software (Content-Management-System, kurz „CMS“) erstellt wurden, über die gleiche Schwachstelle fast gleichzeitig infiziert werden, sprechen wir von Massendefacements. Das führt diese nicht selten zu eindeutig erkennbaren Ausreißern in den Statistiken. Im Besonderen sind dabei die Defacements ab Ende Jänner 2017 zu erwähnen. So etwa wurde in den Versionen 4.7 und 4.7.1 des Content-Management-Systems Wordpress mehrere Sicherheitslücken gefunden, die eine Übernahme von darauf aufsetzenden Webseiten stark vereinfachten. Die Version 4.7.2 behob darauf diese Probleme und wurde am 26. Jänner 2017 veröffentlicht. Viele der Installationen wurden nicht oder nicht rechtzeitig aktualisiert, wodurch eine Welle an gehackten Webseiten folgte, die in den Statistiken klar erkennbar ist.

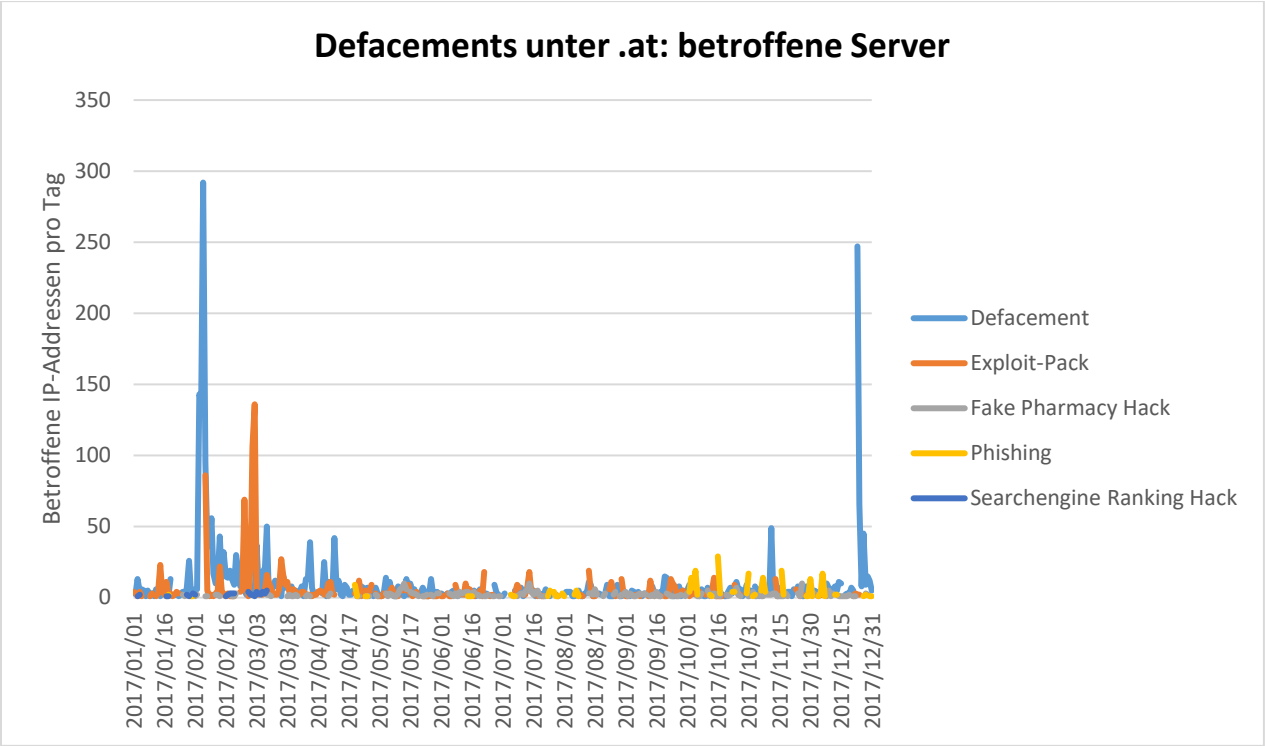


Abbildung 10: Probleme mit Webseiten. Quelle: CERT.at 2018

3.3 Reaktion – Hilfe bei Vorfällen

Im Jahr 2017 gab es drei größere Vorfälle, die auch breite Aufmerksamkeit in den Medien erfahren haben.

Ransomware/Wurm WannaCry (05 / 2017)

Seit 12.05.2017 war europaweit eine massive Welle der Verschlüsselungssoftware (Ransomware) durch "WannaCry" (auch WanaCrypt0r oder WannaCrypt genannt) zu beobachten. Durch das Ausnutzen einer Schwachstelle in Windows-Fileservern konnte die Malware direkt auf diesen aktiv werden und sich weiterverbreiten.

Ransomware ist grundsätzlich kein neues Phänomen, das dahinterstehende "Geschäftsmodell" wird schon seit Jahren erfolgreich angewandt, um von Opfern Geld zu erpressen. Die Liste der bekannten Ransomware-Varianten ist lang, bekannte Namen sind Locky, CryptoLocker, TeslaCrypt, Samsam oder Reveton. Auch Computer-Würmer, also Programme, die sich selbstständig weiterverbreiten, sind nichts Neues. Sie enthalten dazu eine Komponente, die aktiv nach einer Schwachstelle in anderen Computern sucht und diese ausnutzt, um sich selbst dorthin zu kopieren und zu starten.

Im Falle von Wannacry, welcher beide obigen Ansätze (also Ransomware und Computer-Würmer) kombinierte, führte diese zusätzliche Wurm-Funktionalität zu deutlich schwereren Schadensfällen im Vergleich zu klassischer Ransomware. Waren bisher primär Windows-Clients und die von den Usern schreibbaren Fileshares betroffen, so erreichte WannaCry durch das

Ausnutzen einer bereits seit Monaten bekannte Sicherheitslücke (MS17-010) auch Systeme, die bisher verschont blieben. Das führte dazu, dass es global zu einigen signifikanten IT-Ausfällen kam. Den Infizierten wurde versprochen, dass ihnen gegen Zahlung eines Lösegeldes ein Schlüssel zur Wiederherstellung der Daten übermittelt würde. In Österreich waren die Auswirkungen sehr gering, wohingegen europaweit in mehreren Staaten zahlreiche kritische Infrastrukturen betroffen waren.

Für CERT.at waren folgende Punkte relevant:

- Während dieses Vorfalls wurden erstmals die Standing Operational Procedures (EU SOPs) des CSIRTs Networks außerhalb einer Übung angewendet und ein gemeinsames europäisches Lagebild erstellt.

- Die Malware hatten einen „Kill-switch" eingebaut: eine Domain, deren Existenz die Ausführung der Schadensroutine weltweit abgebrochen hat. Ein Sicherheitsforscher hat dies schnell entdeckt und diese Domain registriert. Das hat einerseits viel Schaden verhindert, andererseits konnte über besagte Domain ein Sinkhole für bestehende Infektionen installiert werden. CERT.at bekam die Daten für Österreich (unter 100 IP-Adressen).

- In diesem Moment war der Schaden schon passiert, oder durch den Kill-switch verhindert worden. Die Ausbreitung von Würmern geht meistens so schnell, dass eine effektive Warnung nicht möglich ist.

- Die Erkenntnisse rund um diesen Vorfall mündeten in einen Blogpost, der einige Fragen zu den Hintergründen zu beantworten versucht.

NotPetya (07 / 2017)

Während europaweit die Schäden der Schadsoftware „WannaCry" noch nicht vollständig behoben waren, ereignete sich ab 27.06.2017 mit der Verschlüsselungssoftware (Ransomware) „NotPetya" eine neuerliche Welle von Cyber Angriffen.

Bei NotPetya ging man initial davon aus, dass es sich auch um Ransomware handelte, es stellte sich jedoch heraus, dass diese Malware keine finanzielle Motivation hatte, sondern destruktiver Natur war. NotPetya war ein sogenanter „Wiper", dessen Ziel es war, die betroffenen Systeme unbrauchbar zu machen. Die Schadsoftware wurde über kompromittierte Software-Updates einer legitimen Software, die für das Verfassen von ukrainischen Steuererklärungen zu verwenden ist, verbreitet. Zwar waren europa- und weltweit wiederum zahlreiche Unternehmen von der Infektion betroffen, doch zeigte sich bald, dass nur jene Unternehmen infiziert wurden, die Büros in der Ukraine unterhielten, und falls von dort aus die Infektionen mittels der Wurm-Funktionalität über das Firmen-VPN andere Standorte erreichen konnte. Der Aufbau und die Funktion der Schadsoftware deuten in diesem Fall weniger auf eine Bereicherungsabsicht der Täter, als auf eine gezielte Sabotage der Infrastruktur eines Landes (Ukraine) hin. Wie schon bei

»WannaCry« war auch hier die Mehrzahl der Angriffsvektoren bereits seit Monaten bekannt; fehlendes Patchmanagement und mangelndes Update-Bewusstsein ermöglichten trotzdem eine enorme Anzahl von Infektionen.

Aktuell gibt es innerhalb der Community keine exakten Statistiken, die Rede ist aber von ungefähr 2.000 Opfern (nicht infizierte Rechner, diese Anzahl ist viel höher). Sobald eine initiale Infektion mit NotPetya durch Ausnutzen bekannter Schwachstellen erfolgt, verbreitet sich die Malware innerhalb des eigenen Netzwerkes weiter und verschlüsselt alle Maschinen, die es finden kann. Diese sind danach unbenutzbar und müssen vollständig neu installiert werden.

CERT.at war hier in Österreich in koordinierender Rolle tätig, sowohl was die Informationskonsolidierung mit dem internationalen Partner betrifft, als auch zwischen einzelnen Betroffenen auf nationaler Ebene. Weiters leitete CERT.at Informationen an seine Konstituenten weiter und lieferte sehr erfolgreich ein nationales Lagebild. CERT.at war außerdem in der Lage, einigen Unternehmen wertvolle Tipps zu geben, um eine Infektion durch andere, bereits infizierte Niederlassungen des Unternehmens zu verhindern. Auch bei NotPetya wurde, wie schon bei Wannacry, vom CSIRTs Network gemäß der EU-SOPs ein europäisches Lagebild erstellt.

BadRabbit

BadRabbit war ein weiterer Ransomwarevorfall bei dem die initiale Infektion mittels Drive-by-Angriff auf gehackten, legitimen, Nachrichtenseiten erfolgte. Die Anzahl der Betroffenen war hier wesentlich geringer als bei NotPetya.

Die allgemein akzeptierte Schätzung spricht international von rund 200 Fällen einer Infektion. Der Großteil der Opfer befand sich in Russland, gefolgt von der Ukraine und der Türkei. Nachdem es zum Zeitpunkt der Angriffe keine Betroffenen in Österreich gab, musste CERT.at nicht im Bereich Incident Response aktiv werden. Die Arbeit von CERT.at beschränkte sich auf proaktives Verteilen von Informationen an seine Konstituenten, sowohl im nationalen Bereich als auch in seiner Rolle im GovCERT. CERT.at übernahm auch die Rolle des Informationsvermittlers an Medienvertreter.

3.4 Übungen

Um den neuesten Stand der Entwicklungen auch in der Praxis Rechnung tragen zu können, spielen Cyber Übungen eine zentrale Rolle. Das Training für den Ernstfall überprüft die Praxistauglichkeit der organisatorischen Strukturen, Pläne und Notfalldokumentation, der Handlungsabläufe im Sinne der in der ÖSCS definierten Handlungsfelder, um stressbedingte Fehleranfälligkeit zu minimieren, sowie daraus entstandene, umgesetzte Maßnahmen.

KSÖ Cybersecurity Planspiel 2017

Zum vierten Mal veranstaltete das Kuratorium Sicheres Österreich (KSÖ) von 6. bis 7. November 2017 ein Cybersecurity-Planspiel. Dabei wurde die Fitness Österreichs im Kampf gegen Cyberattacken, Spionage und Onlinebetrug geübt. Gemeinsam mit dem Bundesministerium für Inneres (BMI) und dem Austrian Institute of Technology (AIT) probten rund 200 heimische IT-Sicherheitsexpertinnen und IT-Sicherheitsexperten aus 32 namhaften Organisationen, bestehend aus Behörden, Wirtschaft und Wissenschaft, den Ernstfall und stellten die aktuelle EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS) und die Datenschutzgrundverordnung auf eine Probe in der Praxis.

Die österreichische Strategie für Cyber Sicherheit sieht im Handlungsfeld »Strukturen und Prozesse« die regelmäßige Abhaltung von Cyber Übungen zwecks Testung von Abläufen des Cyber Krisenmanagement vor. Bereits seit dem Jahr 2012 sind die durch das Kuratorium Sicheres Österreich (KSÖ) gemeinsam mit dem Bundesministerium für Inneres (BMI) organisierten Planspiele ein wichtiger Bestandteil bei der Erprobung und Übung der organisatorischen und technischen Abläufe im Falle eines umfassenden Cyber Angriffes auf Unternehmen der kritischen Infrastruktur. Cyber Übungen wie etwa dieses Planspiel leisten einen erheblichen Beitrag zur Steigerung der Resilienz Österreichs und unterstützen damit die Erfüllung der Anforderungen der Österreichischen Strategie für Cyber Sicherheit.

Bereits 2012, 2014 und 2016 organisierte das KSÖ sogenannte „Cybersecurity Planspiele", um einerseits Awareness für das Thema Cybersicherheit zu generieren und andererseits die praktische Zusammenarbeit von Wirtschaft, Behörden und Wissenschaft bei der Bewältigung von Cyberbedrohungen zu testen und zu üben. Nachdem bei den vorangegangenen Planspielen die organisatorischen und rechtlichen Aspekte Vorrang hatten, bekam das Planspiel 2017 einen starken technischen Charakter. Zur Vernetzung der wesentlichen Akteure, spielte das Üben der Kooperation zwischen Staat und Wirtschaft dabei eine wesentliche Rolle. Aus diesem Grund wurden für das Planspiel 2017 auf Seite der Wirtschaft Vertreter kritischer Infrastrukturen und auf Behördenseite die für Cybersecurity zuständigen und im Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) vertretenen Ministerien (BMI, BKA, BMLVS, BMEIA) eingeladen. Als Bindeglied zwischen diesen Gruppen wurden (wie auch in dem NIS-Gesetz definiert) CERTs und Sektor-CERTs (derzeit: CERT.at, GovCERT und Austrian Energy CERT) eingesetzt.

Während in den Vorjahren der Fokus des Planspiels eher auf das staatliche Cyber Krisenmanagement (CKM) gesetzt wurde, standen 2017 die technische Bewältigung und die Zusammenarbeit mit der operativen Koordinierungsstruktur (OpKoord) im Vordergrund. Dabei wurde zum ersten Mal bei einem KSÖ-Planspiel die Ebene der operativen Koordinierungsstruktur vollständig erprobt und beübt.

Das Übungsszenario behandelte - in Folge von politischen Auseinandersetzungen rund um die Brexit-Verhandlungen - gezielte Cyber Angriffen auf Unternehmen der österreichischen Energieversorgung. Die Ziele lagen dabei einerseits in der konkreten technischen Bewältigung der Angriffe unter Verwendung von Werkzeugen an eigens für die Übung generierten Datenbeständen. Dies wurde durch die Spieler sehr positiv aufgenommen. Auf der nächsthöheren Ebene zielte die Übung darauf ab, dass Unternehmen die Notwendigkeit der Einbindung koordinierender, staatlicher Stellen erkennen und entsprechende Meldungen an die zuständigen Behörden absetzen, wie dies von der NIS-Richtlinie vorgesehen ist. Auf einer dritten Ebene wurden durch diese Übung die Vernetzung, der Austausch und die Diskussionen zwischen den beteiligten Behörden erprobt.

Aufgrund der Vorgabe von Seiten der Übungsplanung, zu keinem Zeitpunkt die Ausrufung einer Cyber Krise zu provozieren, ermöglichte es, den Fokus konsequent auf den beteiligten Unternehmen und den staatlichen Partnern auf Ebene der operativen Koordinierung zu belassen. Der Innere Kreis der operativen Koordinierung (IKDOK) koordinierte, unterstützt von CERT.at und Austrian Energy CERT, die Gegenmaßnahmen vom ersten Eintreffen entsprechender Meldungen bis zur letztendlichen Bewältigung der Cyber Angriffe. Dabei konnte der IKDOK auf ein bereits hervorragend eingespieltes Team an staatlichen Akteuren aus mehreren verschiedenen Ressorts zurückgreifen. Diese konnten die im Rahmen der Erstellung des NIS-Gesetzes geplanten Kommunikations- und Koordinationsprozesse unter realitätsnahen Bedingungen testen und somit ebenfalls Erfahrungen sammeln.

Cyber Security Exercise der Central European Cyber Security Platform (CECSP) 2017 – Cyber Czech (Brünn)

Von 23. und 24. Mai 2017 führte das National Cyber Security Center in Brünn eine Wiederholung der technischen Cybersicherheitsübung Cyber Czech 2016 durch, an der Vertreter der CECSP-Länder Österreich, Tschechische Republik, Ungarn und Slowakei teilnahmen. Trainiert wurde in den Räumlichkeiten des zur Masaryk-Universität gehörenden Instituts für Informatik (ICS).

Die Übung wurde in Form einer Simulation in einer geschlossenen, speziell modifizierten technischen Umgebung durchgeführt, die Techniken und Manipulationen mit Inhalten ermöglicht, die in einem offenen Netzwerk eine ernsthafte Bedrohung darstellen würden. Die Vertreter der teilnehmenden Länder wurden in ein Red Team und ein Blue Team geteilt; beim Angriffsziel handelte es sich um die Zugsteuerung eines mit Atommüll beladenen Zuges, der vom Blue Team zu verteidigen war. Die Teilnehmer des Blue Teams mussten sich mit bis zu sechs Stunden andauernden, überaus komplexen Cyber-Angriffen auseinandersetzen.

Regelmäßig wurde evaluiert, welche Angriffe durch das Red Team erfolgreich, welche Systeme noch intakt und welche Services durch die fiktiven User noch verwendbar waren. Punktabzug gab es für Erfolge der Angreifer (Red Team), aber auch für Services, die von den Blue Teams selbst kaputt gemacht wurden. Wie im echten Leben war also die Erfolgsstrategie, den Betrieb nicht komplett zu behindern bzw. abzudrehen. Ebenfalls geübt und getestet wurden die technischen Fähigkeiten der Teilnehmer beider Teams, als auch der als besonders wichtig erachtete, länderübergreifende Informationsaustausch.

Besonders war bei dieser Übung der Ansatz, zum Teil echte User auf den Systemen zu haben, die kleine Aufgaben zu erledigt hatten, und mit diesen zu kommunizieren. Beispielsweise war diesen zu erläutern, warum bestimmte Dinge gerade nicht funktionierten oder dass vermehrt auf Phishing Mails zu achten ist. Dies erhöhte den Realitätsgrad der Übung. Ähnlich wie bei einer funktionierenden Zusammenarbeit mit der im Planspiel fingierten Presse und Behördenvertretern konnte man auch hier Pluspunkte auf seinem Konto sammeln.

Das Ziel dieser Übung bestand nicht nur darin, auf Angriffe und technische Probleme zu reagieren, sondern auch den Umgang mit der Medien-Öffentlichkeit zu üben, und zu sehen, wie diese Akteure von den Auswirkungen der getroffenen Entscheidungen beeinflusst wurden. Mit Hilfe dieses Medienaspekts konnten die Teams sehen und lernen, wie sie bei einer realen Cyber-Krise mit dem entstehenden, erhöhten Stress besser umgehen.

3.5 Networking

Vernetzung als Grundvoraussetzung für Vertrauensbildung

CERT.at arbeitet nicht im Verborgenen an der Sicherheit des österreichischen Internets. Nur durch intensive Vernetzung mit anderen relevanten Playern der Cybersecurity 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 richten sich in ihrer Arbeit an jede Österreicherin und jeden Österreicher. Diese sind Kunden – das Produkt, das sie konsumieren, ist die Sicherheit im Netz. Da es aber nicht möglich ist, jeden einzelnen Bürger direkt anzusprechen, interagieren CERT.at und GovCERT.at stellvertretend mit den wichtigsten Communities im Bereich Cybersicherheit. Das sind jene österreichischen Unternehmen und Institutionen im Sicherheitsbereich, die sich mit diesem Thema auseinandersetzen oder davon betroffen sind.

CERT.at und GovCERT.at 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 Player in Österreich. Sie sind aber auch international sichtbare Partner für ausländische CERTs. So bestehen eine intensive Zusammenarbeit und reger Informations- und Erfahrungsaustausch

mit Experten und ExpertInnen aus aller Welt. GovCERT ist dabei der staatliche österreichische Ansprechpartner für vergleichbare Stellen im Ausland sowie für internationale Organisationen zu Fragen der IKT-Sicherheit.

Vernetzung auf nationaler Ebene

Austrian Trust Circle

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 Experten-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.

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. Jeder einzelne Teilnehmer verpflichtet sich die Ziele – (1) einen regelmäßigen Informations- und Erfahrungsaustausch, (2) Identifizierung und Zugänglichmachen von Kernkompetenzen und (3) die Förderung der nationalen CERTs in allen Sektoren – im Sinne eines gemeinschaftlich geführten und auf Kooperation basierenden CERT-Verbundes zu verfolgen.

Mit Stand Ende 2017 nehmen 15 Teams am österreichischen CERT-Verbund teil.

IKDOK/OpKoord

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

Der IKDOK umfasst das Cyber Security Center des Bundesministeriums für Inneres und das Cyber Verteidigungszentrum des Bundesministeriums für Landesverteidigung. Weitere staatliche Akteure und Einrichtungen sind im IKDOK vertreten. 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 werden im kommenden NIS-Gesetz einen klaren rechtlichen Rahmen bekommen.

IT-Sicherheit für Österreichs Energieunternehmen: Austrian Energy CERT - ein Vorreitermodell in der EU

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

Nach einer Vorlaufzeit von drei Monaten startete mit 1. November 2016 die erste von vier Phasen des Aufbaus des Austrian Energy CERT. Der Aufbau erfolgte schrittweise und konnte im Mai 2018 erfolgreich abgeschlossen werden.

Jetzt im Vollausbau sind Basisservices, erweiterte Services und eine Ruferreichbarkeit rund um die Uhr etabliert. Durch den gemeinsamen Aufbau eines brancheneigenen Austrian Energy CERT werden Bewusstsein und Prävention im Energiesektor gestärkt. Jedes einzelne Energieunternehmen kann im Notfall auf Experten und ein gemeinsames, auf Energiefragen spezialisiertes Notfallteam zugreifen. Diese Dienstleistung ist nur eine Maßnahme aus dem umfassenden Servicekatalog, der u.a. die Lagebilderstellung, die Bearbeitung von Sicherheitsmeldungen, die Einschätzung der Bedrohungsvektoren, etc. enthält.

Bei der Implementierung hat die österreichische Energiewirtschaft besonderes Augenmerk auf ein enges Zusammenwirken des Austrian Energy CERT mit anderen Initiativen in diesem Bereich (z.B. CERT.at und GovCERT) gelegt. Daher ist das Austrian Energy CERT bei der nic.at GmbH angesiedelt, die auch das nationale CERT.at betreibt. Dies ermöglicht eine rasche und effiziente

Umsetzung und nutzt sowohl die bestehende Expertise als auch das vorhandene Know-how. Dadurch ist es gelungen, die größtmöglichen Synergien zu erzielen und die bestehenden Schnittstellen optimal zu nutzen. Ziel ist es, dass an Stelle einer Behörde das Austrian Energy CERT auch die gesetzlich anerkannte Meldestelle ist. Mit diesem Modell ist Österreich Vorreiter in der europäischen Union. Somit wird die Branchen-Initiative auch laufend von der Arbeitsgemeinschaft E-CERT auf europäischer Ebene vorgestellt. Gelegenheiten dafür boten sich in direkten Gesprächen mit den Themenverantwortlichen der Europäischen Kommission und anderer europäischer Cyber Security relevanter Organisationen, sowie im Zuge der österreichischen Ratspräsidentschaft.

Beim EU-Neighboring Countries Meeting for Critical Infrastructure Projects (CIP) in Wien war Stefan Wagenhofer als Vorsitzender des Arbeitsgemeinschaft E-CERT vom Bundeskanzleramt eingeladen, dieses vorzustellen. Die Delegierten der Kommission, allesamt Experten in Sachen Sicherheit, waren sehr interessiert zu erfahren wie das österreichische Modell der Energieunternehmen funktioniert. Viele Branchen in anderen Ländern haben die NIS-Richtlinie noch nicht in dem Umfang umgesetzt, wie dies die Energiewirtschaft in Österreich getan hat. Die Kombination einer Arbeitsgemeinschaft, die Sektor übergreifend aus allen Energieunternehmen besteht und ein gemeinsames Energy CERT betreibt, war für die meisten Teilnehmer neu und sehr interessant. Daher gab es hohes Interesse an unseren Erfahrungen zum Aufbau, der Struktur und Arbeitsweise. Das Austrian Energy CERT wurde als Vorzeigemodell von den Delegierten gelobt und weitere Einladungen folgten.

Am Oktober 2018 fand weiters in Brüssel eine von der Österreichischen Ratspräsidentschaft, der EU-Kommission und dem Institut der deutschen Wirtschaft veranstaltete High-level Konferenz zum Thema „Cyber Security in the Energy Sector" statt.

Bereits in der Begrüßung wies die österreichische Botschafterin Dr. Elisabeth Kornfeind auf die Bedeutung der Elektrizitätswirtschaft für alle Sektoren, sowie auf die stark steigenden Cyber-Bedrohungen hin. Der Leitsatz der österreichischen Präsidentschaft, „A Europe that Protects" hat gerade auch für die Digitalisierung und die kritische Infrastruktur Bedeutung. Dies unterstrichen seitens der EU-Kommission auch der Generaldirektor für Energie Dominique Ristori und seitens des EU-Parlaments Peter Kouroumbashev als Schatten-Rapporteur für den Cybersecurity Act und der Leiter des österreichischen GovCERT im Bundeskanzleramt, Clemens Möslinger.

Walter Fraißler, stellvertretender Vorsitzender der Arbeitsgemeinschaft E-CERT, konnte bei dieser Gelegenheit das Austrian Energy CERT vorstellen. Bei den rund 200 Teilnehmern an der Konferenz stieß dieses als europaweites Vorbild auf großes Interesse.

Näheres über die Arbeitsgemeinschaft E-CERT finden Sie unter:
http://www.aec.arge.or.at/index.php/de/home.html

Näheres über das Austrian Energy CERT finden Sie unter: https://energy-cert.at/

Vernetzung auf zwischenstaatlicher Ebene

Auch der direkte und persönliche Austausch mit CERTs aus Nachbar- und Partnerländern ist wesentlich für Abstimmungen sowie für Updates zu Problemlagen und neuen Entwicklungen.

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, wie zum Beispiel die wichtige und weiter oben beschriebene Übung in Brünn 2017.

Vernetzung auf europäischer und internationaler Ebene

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 Playern im europäischen Cybersecurity-Bereich Auskunft gibt.

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. In der zweiten Hälfte 2018 übernahm CERT.at den Vorsitz des Netzwerkes, welcher zusammen mit der EU-Ratspräsidentschaft in diesem Zeitraum bei Österreich liegt.

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 ist. Die Gruppe bildet eine informelle Vereinigung, dessen

Mitglieder in Fragen hinsichtlich der Reaktion auf Vorfälle effektiv zusammenarbeiten. Im Gegensatz zum CSIRTs Network ist EGC eine Initiative der CERTs selbst und basiert nicht auf einem gesetzlichen Auftrag.

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

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 Sicherheitsvorfälle ermöglicht.

Auf Grund der Größe (FIRST hat mehr als 400 Mitglieder) stehen nicht mehr einzelen Vorfälle im Fokus von FIRST, sondern vielmehr der Erfahrungsaustausch, Lobbying und das gemeinsame Entwickeln von Standards. So etwa wird das System der Kennzeichnung von Information (Traffic Light Protocol) und die Metrik zur Bewertung von Schwachstellen (CVSS) von FIRST betreut. Das Netzwerk trifft sich zum einen bei der jährlichen internationalen Konferenz und zum anderen bei zahlreichen themen- oder regionsspezifischen Treffen. Mit Aaron Kaplan war im Jahr 2017 ein Österreicher und Mitarbeiter von CERT.at Teil des Vorstands von FIRST.

3.6 Andere Kooperationen

Connecting Europe Facilities (CEF) Program

Co-financed by the European Union
Connecting Europe Facility

"Strengthening the CERT Capacity and IT security readiness in Austria"

CERT.at reichte 2016 im Rahmen des Connecting Europe Facilities (CEF) Program ein EU Projekt zum Thema "Strengthening the CERT Capacity and IT security readiness in Austria" (2016-AT-IA-0089) ein, das 2017 in vollem Umfang bewilligt wurde. Ziel des Programms ist die Stärkung des nationalen CERTs in Anbetracht der nationalen NIS-Gesetzgebung. Ausgebaut werden bei dem bis September 2019 laufenden Projekt sowohl die personellen Ressourcen, Trainings, Code-Weiterentwicklungen als auch der Ausbau der Backend-Server und der Sicherheits-Architektur von CERT.at. Spezielles Augenmerk wird dabei auf den Ausbau der bei CERT.at liegenden Incident Handling Automatisierungs-Platform "IntelMQ" gelegt, welche bereits weiter oben erwähnt wurde. CERT.at liegt mit einer bereits 50%igen erfolgreichen Umsetzung gut im Zeitplan.

IntelMQ ist eine Lösung für IT-Sicherheitsteams (CERTs, CSIRTs, Missbrauchsabteilungen, ...) zum Sammeln und Verarbeiten von Sicherheitsfeeds (z. B. Protokolldateien) mithilfe eines Nachrichtenwarteschlangenprotokolls. Es handelt sich um eine Initiative von IHAP (Incident Handling Automation Project), die konzeptionell von europäischen CERTs / CSIRTs während mehrerer InfoSec-Veranstaltungen entworfen wurde. Sein Hauptziel ist es, den Einsatzkräften eine einfache Möglichkeit zu geben, Bedrohungsdaten zu sammeln und zu verarbeiten und so die Vorfallbearbeitungsprozesse von CERTs zu verbessern.

Mitarbeit an nationalen Forschungsprojekten

CERT.at beteiligte sich auch 2017 an einer Reihe nationaler Forschungsprojekte, durch welche neue Ansätze und technische Möglichkeiten untersucht und Lösungen entwickelt wurden.

CISA (KIRAS)

Das Projekt **Cyber Incident Situational Awareness** (CISA) bündelt eine Reihe von Forschungsaktivitäten und -maßnahmen im Bereich des Aufbaus von Awareness und Know-How von nationalen Akteuren. Zielsetzung ist es, eine Definition des Begriffs „Cyber Situational Awareness" (Lageverständnis) zu erreichen und ein wissenschaftlich fundiertes Konzept für den Prozess zur Etablierung allumfassender Cyber Situational Awareness aus technisch-operativen Informationen aus dem Cyberspace zu erarbeiten.

CERT-KOMM II (KIRAS)

Im Rahmen des **Computer Emergency Response Team Kommunikations-Modell II** (CISA-KOMM II) werden gemeinsam mit den Projektpartnern der Fakultät für Informatik (Multimedia Information Systems Research Group) der Universität Wien, dem Fachbereich für Infrastrukturelle Sicherheit der Donau-Universität Krems, dem Research Institute AG & Co KG, der IKARUS Security Software GmbH und dem Bundeskanzleramt die Rahmenbedingungen von CERTs analysiert. Ziel ist es, jene Faktoren zu identifizieren, von denen eine erfolgreiche Kommunikation zwischen CERTs abhängt. Am Ende des Projekts wird, ausgehend von den Ergebnissen von CERT-KOMM I, ein Kommunikationsmodell der CERTs untereinander und mit privatwirtschaftlichen Partnern entwickelt.

ACCSA (KIRAS)

CERT.at beteiligt sich an den **Austrian Cyber Crises Support Activities** (ACCSA), die darauf abzielen, Akteure 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.

4 EU NIS-Richtlinie & nationale Cybersicherheitsgesetz

4.1 Netz- und Informationssicherheitsgesetz

Die fortschreitende Digitalisierung unserer Gesellschaft bedingt ein steigendes Risiko durch Angriffe auf die Informations- und IT-Sicherheit. Aus diesem Grund verabschiedete die Europäische Kommission am 7. Februar 2013 eine Mitteilung zur "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum" sowie einen Vorschlag für eine „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (EU 2016/1148) - kurz „NIS-Richtlinie" genannt.

In der Strategie werden die Vorstellungen der EU auf dem Gebiet der Cybersicherheit anhand von fünf Prioritäten dargelegt:

- Widerstandsfähigkeit gegenüber Cyber-Angriffen.
- Drastische Eindämmung der Cyber-Kriminalität.
- Entwicklung einer Cyber-Verteidigungspolitik und von Cyber-Verteidigungskapazitäten im Zusammenhang mit der gemeinsamen Sicherheits- und Verteidigungspolitik (CSDP).
- Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit.
- Entwicklung einer einheitlichen Cyberraum-Strategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU.

NIS-Richtlinie: Umsetzung aus österreichischer Sicht

Ziel der am 8. August 2016 in Kraft getretenen NIS-Richtlinie ist der EU-weite Aufbau eines hohen Sicherheitsniveaus der Netz- und Informationssysteme, die Schaffung eines einheitlichen Rechtsrahmens für den Aufbau nationaler Kapazitäten für die Informations- und IT-Sicherheit, sowie die Förderung einer stärkeren Zusammenarbeit der Mitgliedsstaaten. Die NIS-Richtlinie definiert aber auch Mindestanforderungen und Meldepflichten für die Betreiber kritischer Infrastruktur und Anbieter definierter digitaler Dienste.

Die NIS-RL verpflichtet die Mitgliedstaaten, eine nationale NIS-Strategie zu erarbeiten. Weiters haben bestimmte Unternehmen aus wirtschaftlich oder gesellschaftlich wichtigen Sektoren adäquate Sicherheitsmaßnahmen einzuführen und gröbere Störfälle zu melden. Beinhalten sollte diese die strategischen Ziele, Prioritäten und Maßnahmen, um in den einzelnen Mitgliedstaaten ein hohes Sicherheitslevel der Netz- und Informationssysteme zu erreichen. Die NIS-Richtlinie befindet sich derzeit in Umsetzung in den Nationalstaaten.

Einrichtung von CSIRTs und NIS-Behörden in den Mitgliedsstaaten

Die NIS-Richtlinie hält auch fest, dass jeder Mitgliedstaat ein oder mehrere Computer Security Incident Response Teams (CSIRT) einzurichten hat, denen u.a. Aufgaben wie die mögliche Entgegennahme von Cyber Vorfallsmeldungen, die Ausgabe von Frühwarnungen, die Reaktion

auf Sicherheitsvorfälle oder auch die dynamische Analyse von Risiken und Vorfällen zukommen. Österreich verfügt mit dem GovCERT und dem CERT des Energiesektors (Austrian Energy CERT) bereits jetzt über einige CSIRTs, welche im Sinne der NIS-Richtlinie als Meldestellen für freiwillige und verpflichtende Vorfallsmeldungen aus dem jeweiligen Sektor (öffentlicher Sektor für GovCERT, Energiesektor für AEC) fungieren.

Weiters sind in den Mitgliedstaaten eine oder mehrere nationale Behörden einzurichten, die unter anderem die Bewertung der Sicherheit von Netz- und Informationssystemen vornehmen und verbindliche Anweisungen zur Abhilfe bei festgestellten Mängeln erteilen können. Als Verbindungsstelle zwischen den Mitgliedstaaten, der Kooperationsgruppe und dem CSIRT-Netzwerk ist zudem in jedem Mitgliedstaat eine nationale, zentrale Anlaufstelle ("Single Point of Contact"; SPOC) einzurichten.

Wie auch auf Richtlinien-Ebene sind die obersten Ziele des nationalen Gesetzgebers die Prävention gegen Sicherheitsvorfälle, die Netz-und Informationssysteme betreffen, sowie die Gewährleistung einer raschen und professionellen Reaktion darauf. Zu diesem Zweck werden die (teilweise schon bestehenden) nationalen Strukturen samt Aufgabenzuteilungen und Befugnisse durch gesetzliche Regelungen festgelegt. Bei Erarbeitung der nationalen Umsetzung der Richtlinie wurde darauf geachtet, einen gut funktionierenden Koordinationsmechanismus zu schaffen, da die NIS-Richtlinie viele unterschiedliche Bereiche betrifft. Diese sind für Betreiber wesentlicher Dienste die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Trinkwasserversorgung, Gesundheitsdienste und Internetinfrastrukturen. Weiters sind von der Richtlinie auch bestimmte (größere) digitale Diensteanbieter betroffen, welche Online Marktplätze, Suchmaschinen oder Cloud Computing Dienste anbieten.

Es wurde ein Rechtsrahmen geschaffen, in dem sowohl Betreiber wesentlicher Dienste als auch digitale Diensteanbieter adäquate Sicherheitsmaßnahmen einführen und erhebliche Störfälle melden. Zudem wurde die Möglichkeit für den freiwilligen Austausch über Risiken, aktuelle Bedrohungen und Vorfälle der von einem Störfall betroffenen Einrichtungen untereinander , sowie mit den Computer-Notfallteams und staatlichen Stellen, auf der Basis gegenseitigen Vertrauens, geschaffen. Das vom Bundeskanzleramt in Form einer interministeriellen Arbeitsgruppe verfasste Netz- und Informationssystemsicherheitsgesetz befand sich bis 31.10. 2018 im Prozess der parlamentarischen Begutachtung.

4.2 Österreichische Strategie für Cyber Sicherheit (ÖSCS)

Die österreichische Strategie für Cyber Sicherheit (ÖSCS) stammt aus dem Jahr 2013 und ist ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums und der Menschen im virtuellen Raum unter Gewährleistung der Menschenrechte. Die ÖSCS hat zum Ziel, die Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyber Raum zu verbessern. Sie soll aber auch dazu beitragen, Bewusstsein über und Vertrauen in die digitale Sicherheit in der österreichischen Gesellschaft zu schaffen.

Die Strategie für Cyber Sicherheit leitet sich aus der Österreichischen Sicherheitsstrategie (ÖSS) ab und orientiert sich an den Prinzipien des Programms zum Schutz kritischer Infrastrukturen (SKI). Die ÖSCS definiert Chancen und Risiken im Cyber Raum sowie die Prinzipien einer modernen Cyber Sicherheitspolitik. Des Weiteren legt die ÖSCS fest, welche strategischen Ziele im Bereich Cyber Sicherheit verfolgt werden sollen. Darüber hinaus werden Handlungsfelder und Maßnahmen zur Erhöhung der digitalen Sicherheit aufgelistet.

Die Strategie für Cyber Sicherheit bildet das Fundament der gesamtstaatlichen Zusammenarbeit in diesem Bereich und beruht auf den Prinzipien Rechtstaatlichkeit, Subsidiarität, Selbstregulierung und Verhältnismäßigkeit. Die nationale und internationale Absicherung des Cyber Raums ist eine der obersten Prioritäten Österreichs. So sind ein offenes und freies Internet, der Schutz personenbezogener Daten, die Unversehrtheit von miteinander verbundenen Netzwerken die Grundlage für globalen Wohlstand, Sicherheit und Förderung der Menschenrechte.

Weitere Informationen finden Sie im Bericht Cyber Sicherheit 2018 des Bundeskanzleramtes: https://www.bundeskanzleramt.gv.at/cyber-sicherheit-egovernment