GovCERT Austria

CERT.at

Bericht Internet-Sicherheit Österreich 2018

1 Inhalt

Impressum

Medieninhaber und Verleger: nic.at GmbH, Computer Emergency Response Team Austria, Karlsplatz 1/3, 1010 Wien. Diese Publikation wurde in Kooperation mit dem Bundeskanzleramt erstellt. **Projektleitung:** Dimitri Robl, BA, CERT.at **Konzeption und Redaktion**: CERT.at (Mag. Otmar Lendl, Dimitri Robl, BA), Bundeskanzleramt (Dipl.-Ing. Mag. Andreas Reichard, M.Phil.)

Herstellungsort: Wien, Oktober 2019.

1 Vorwort

Erich Albrechtowitz

Leitung der Gruppe I/B
Bundeskanzleramt

Cybersicherheit und seine gesetzliche Grundlage in Österreich

Die weltweite, digitale Vernetzung hat auch im Jahr 2018 weiter zugenommen. Dieser Trend macht auch vor Österreich nicht halt. So konsumieren wir alle digitale Services, die unser Leben erleichtern und es werden digitale Dienste mit Selbstverständlichkeit von uns genutzt.

Doch all das wird von den Schattenseiten dieser Entwicklungen begleitet, welche 2018 ebenfalls zugenommen haben: Bedrohungen aus dem Cyberraum, Angriffe auf kritische Infrastrukturen und Anbieter digitaler Dienste, aber auch auf Kleinunternehmen und Einzelpersonen. Derartige Vorkommnisse waren 2018 in den Schlagzeilen präsent, die die Welt um uns und damit auch Österreich bewegten und so aufzeigen, dass das Thema Digitalisierung in unser aller Denken und Realität endgültig angekommen ist. Dabei ist die Frage, ob die Cybersicherheit in Österreich mit der steigenden Digitalisierung mithalten kann, eine, der sich ein Land wie Österreich stellen muss und auch kann.

Mit dem Österreichischen Netz- und Informationssystemsicherheitsgesetz (NISG), das Ende 2018 auf den Weg gebracht wurde, wurde die Möglichkeit geschaffen, Cybersicherheit als Voraussetzung für die digitale Souveränität Österreichs in Europa auf einer zeitgemäßen, rechtlichen Grundlage zu basieren, die in Einklang mit europäischem Recht steht.

Mit dem NISG hat Österreich aber nicht nur die Netz- und Informationssicherheitsrichtlinie der EU (NIS-Richtlinie) national umgesetzt, es wurden darin auch Strukturen und Prozesse rechtlich definiert, welche Österreich gegen mögliche Bedrohungen wappnen. Zusammen mit der Österreichischen Strategie für Cybersicherheit (ÖSCS) ist das NISG somit ein Werkzeug, das es uns ermöglicht, Österreich hinsichtlich Cybersicherheit im europäischen Vergleich nicht nur weiter voran-, sondern auch unter die Top-Länder in diesem Bereich zu bringen.

Eine wesentliche Rolle auf diesem Weg haben Partner, internationale, aber auch nationale, aus der öffentlichen Verwaltung, den privaten Sektoren, dem Forschungsumfeld, und besonders jene, die für die österreichische Bevölkerung und unser Land wesentliche Dienste erbringen. Zu diesen Partnern zählen wir im Bundeskanzleramt auch CERT.at, mit dem wir vor 10 Jahren in gemeinsamer Kooperation das im Bundeskanzleramt angesiedelte GovCERT Austria schufen.

Es gelang auf diese Weise, die strategische Expertise im Bundeskanzleramt mit der technischen Expertise von CERT.at zu verbinden, was 2018 unter anderem während der Teilnahme an mehreren Cyberübungen wie Cyber Europe, ASDEM oder EuroSOPEX erfolgreich in Form eines simulierten Cyberernstfalls erprobt wurde. Diese Synergien zwischen Bundeskanzleramt und CERT.at konnte in den vergangenen 10 Jahren weiter ausgebaut werden und die Früchte dieser Kooperation sprechen für sich: So ist GovCERT Austria, 10 Jahre nach seiner Gründung 2008, ein angesehener Player in der Cybersicherheit-Landschaft in Österreich, sowie in Europa und der Welt.

Mag. Robert Schischka

Leiter des Computer Emergency Response Teams (CERT.at)

10 Jahre CERT.at – Vertrauen ist wichtiger denn je

2018 war für uns alle insofern ein ganz besonderes Jahr, als wir vor 10 Jahren – genauer gesagt im Februar 2008 erstmals einer breiteren Öffentlichkeit die Gründung eines nationalen Computernotfallteams vorgestellt haben. Zur selben Zeit wurde auch in enger Kooperation mit dem Bundeskanzleramt das GovCERT für die Bereiche der öffentlichen Verwaltung ins Leben gerufen.

Zu dieser Zeit waren CERTs/CSIRTs zum Großteils nur in Fachkreisen eingeführte Begriffe und in der politischen Diskussion oder gar Rechtstexten de facto nicht zu finden. Nicht wenig Zeit verbrachten die Mitarbeiter und Weggefährten der ersten Stunde damit, immer wieder aufs Neue zu erklären, was ein CERT jetzt eigentlich genau macht, dass wir nichts mit Zertifikaten oder Zertifizierungen zu tun haben und auch mit keinen polizeilichen oder sonstigen hoheitlichen Befugnissen ausgestattet sind. Sehr gut kann ich mich auch an zahlreiche Diskussionen erinnern, bei denen die Grundideen des „Infosharings" auf freiwilliger Basis und kooperative Zusammenarbeit und Vertrauen als Erfolgsfaktoren von einigen geradezu belächelt wurde.

Seit damals hat sich einiges verändert, sowohl in der Bedrohungslage, die trotz hohem technischem Mitteleinsatz und großer Anstrengungen leider keineswegs abgenommen hat, aber auch im Bewusstsein um die Relevanz der IKT-Infrastruktur. Die Bereiche Sicherheit und Verfügbarkeit der Informationsnetze, Datensicherheit und Datenschutz sind heute zentrale Themen – nicht nur für Unternehmer und Techniker, sondern auch für die Politik, die diesen Ball unter anderem auch mit der NIS-Richtlinie und der Datenschutzgrundverordnung aufgegriffen hat. Aus Sicht eines CERTs ist es wirklich erfreulich, dass die Aufgaben und Tätigkeiten in diesen beiden Rechtsmaterien erstmals auf europäischer Ebene Erwähnung gefunden haben und somit für den für uns so zentralen Bereich der Informationsverarbeitung und Weitergabe Rechtssicherheit geschaffen wurde.

Die Umsetzung der NIS-RL in österreichisches Recht war von einem durchaus komplizierten Prozess an Konsultationen in diversen Arbeitsgruppen begleitet. Dieses Vorgehen führte naturgemäß zu einem erheblichen Zeitaufwand und einigen Ehrenrunden in der finalen Abstimmung. Im Ergebnis bin ich aber der Meinung, dass in Österreich ein ausgewogenes und gut sehr abgestimmtes rechtliches Rahmenwerk geschaffen wurde. Der eingeschlagene Weg mit zahlreichen Abstimmungen und einer echten Einbeziehung aller relevanten Stakeholder in Diskussionen auf Augenhöhe sind eine gute Grundlage für eine vertrauensvolle Zusammenarbeit in der realen Umsetzung der gesetzlichen Vorgaben.

Ein wesentlicher Baustein ist dabei auch die gesetzliche Verankerung der Meldewege für CERTs sowie das Festschreiben eines Melderechtes abseits von gesetzlichen Meldeverpflichtungen, die zwar in vielen Bereichen durchaus ihre Berechtigung haben, im Ergebnis alleine betrachtet aber zu kurz greifen. Dieses Information-Sharing auf Basis von Selbstorganisation der betroffenen Sektoren wurde von österreichischer Seite schon in die NIS-RL eingebracht und schließlich im österreichischen NISG konsequent weiter umgesetzt.

Ich muss gestehen, dass es mich auch ein bisschen stolz auf unsere Arbeit macht, wenn ich heute von vielen Mitstreitern aus allen Bereichen der Cybersecurity ein klares Bekenntnis zu Informationsaustausch und Kooperation auf Basis gegenseitigen Vertrauens höre. Kein noch so gutes System kann diesen menschlichen Faktor ersetzen.

In diesem Sinne möchte ich mich auch ganz herzlich bei allen Weggefährten für das Vertrauen und die langjährige Unterstützung bedanken. Ohne diese „Überzeugungstäter" könnten wir nicht erfolgreich arbeiten

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 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 10 Jahre CERT.at – ein Rückblick

Es ist wie bei den Masern, der Grippe oder anderen ansteckenden Krankheiten: Zunächst brechen sie bei einer Person in einem Dorf aus, dann steckt sich der Nachbar an, dann der Händler aus der nächstgrößeren Stadt und so geht es weiter. Gut, wenn es eine Stelle gibt, die früh informiert ist, die Bedrohung wahrnimmt und handelt – bevor sich die Krankheit weit verbreitet und sich nur noch mit größter Mühe bekämpfen lässt. Eine Stelle, die ÄrztInnen erklärt, wie sie die Krankheit behandeln, die Medikamente bereitstellt und die Bevölkerung aufklärt, wie sie sich schützen kann.

Für die Gesundheit im österreichischen Internet übernimmt CERT.at diese Funktion. CERT steht für „Computer Emergency Response Team", quasi die schnelle Eingreiftruppe für Notfälle im Netz. Seit seiner Gründung vor zehn Jahren hat sich CERT.at von einer Stiftungs-Initiative zur Schaltzentrale für Cyber-Sicherheit in Österreich mit gesetzlichem Auftrag entwickelt.

Der lautet: Sorgt dafür, dass Angriffe auf IT-Netze möglichst schnell erkannt und bekämpft werden! Tragt die sicherheitsrelevanten Informationen der IT-Fachleute zusammen! Macht niemandem Angst; aber warnt die Öffentlichkeit vor den Sicherheitsrisiken und klärt die Internet-NutzerInnen auf, dass sie nicht allem blind vertrauen dürfen.

Denn eine gesunde IT-Infrastruktur ist entscheidend für das Wohl des Landes. Kritische Sektoren wie Energie- und Wasserversorgung, Banken, Krankenhäuser, Kommunikationstechnologie oder die Lebensmittelversorgung können ihre Aufgaben nur erfüllen, wenn die IT gegen Angriffe gewappnet ist. Auch alle anderen Sektoren der Privatwirtschaft sind vernetzt und von der Datenverarbeitung durchdrungen – und damit unser tägliches Leben.

Jeder Sektor für sich ist bereits äußerst komplex. Doch erschwerend kommt für die Sicherheit hinzu: Keiner ist nach außen abgeriegelt, alle sind über das Internet miteinander verbunden, in

jeder Sekunde werden Millionen von Daten ausgetauscht. So könnten sich Angriffe schnell verbreiten.

Auch wenn jedes Unternehmen und jeder Sektor seine IT schützt, ist eine nationale Stelle nötig, bei der die Informationen zusammenlaufen. Denn nur in der Gesamtschau können sie ausgewertet werden, was eine schnelle Reaktion ermöglicht. Am Wiener Karlsplatz laufen die Fäden zusammen. Als unabhängige Plattform sammelt CERT.at Informationen zu Sicherheitsproblemen im österreichischen Internet, etwa zu infizierten PCs, zu manipulierten Webseiten oder fehlkonfigurierten Servern. All diese Informationen bündelt das Team, analysiert sie und identifiziert Bedrohungen. Es informiert umgehend die betroffenen Internet Service Provider (ISPs) oder EigentümerInnen der Domains, warnt andere SicherheitsexpertInnen und veröffentlicht Informationen zu größeren Attacken. Zudem geben die ExpertInnen Reports und Handlungsanleitungen heraus und beraten, wie sich die Gefahr bannen lässt. Damit ist CERT.at ein zentraler Teil der österreichischen IT-Sicherheitsstrategie.

Einnahmen aus der Domain-Verwaltung finanzieren die Netz-Sicherheit

Interessant ist die Entstehungsgeschichte von CERT.at. Im Jahr 1988, das Internet ist in Österreich noch hauptsächlich auf die Akademia beschränkt, koordiniert die Universität Wien die wenigen .at-Domains. Als deren Zahl rasant wächst, wird eine eigene GmbH gegründet, das „Network information center", kurz nic.at. Das Center ist bis heute die offizielle Registrierungsstelle für alle Domains mit den Endungen .at, .co.at und .or.at – insgesamt sind es inzwischen über 1,3 Millionen.

Nic.at ist jedoch weder eine Regierungsstelle noch ein klassisches Unternehmen. Die Gesellschaft gehört der gemeinnützigen Internet Privatstiftung Austria (IPA), die den Ausbau, die Verbreitung und die Nutzung des Internets in Österreich fördert.

Und weil zur Förderung des Internets nicht zuletzt dessen Sicherheit gehört, gründete nic.at 2008 gemeinsam mit dem Bundeskanzleramt CERT.at. Das Team hat keinen privilegierten Zugang zu Informationen, greift nicht auf den Datenverkehr zu oder schneidet gar den Daten-Austausch mit. Es greift ausschließlich auf öffentlich verfügbare Informationen zurück oder geht Meldungen über sicherheitsrelevante Ereignisse nach.

Daneben leistet CERT.at umfangreiche Pressearbeit, um Bevölkerung und IT-Fachleute für Sicherheitsthemen zu sensibilisieren. Das Team steht JournalistInnen mit seiner Expertise zur Verfügung, berät Behörden und politische EntscheiderInnen.

Großes Vertrauen der IT-Sicherheitsbranche in CERT.at

Um auch kleine Sicherheitslücken früh zu erkennen, sind die ExpertInnen auf Hinweise etwa von IT-AdministratorInnen aus Unternehmen angewiesen. Um die zu bekommen, ist es gut, dass CERT.at wie die IPA-Stiftung und nic.at gerade *keine* Regierungsstelle oder Behörde ist. Denn sonst müsste das Team Pflichtverletzungen und Sicherheitslücken nachgehen oder polizeiliche Ermittlungen anstoßen.

Aber CERT.at ist keine Ermittlungs- oder gar Strafverfolgungsbehörde. Keine Information leitet das Team ohne den erklärten Willen eines Unternehmens weiter. Berichte über Sicherheitslücken oder Beinahe-Einbrüche gibt es nur anonymisiert und aggregiert weiter. So muss kein Unternehmen befürchten, dass seine Informationen bei Behörden oder gar durch Medien bekannt werden, dass sein Ruf oder sein Aktienkurs Schaden nehmen oder gar Strafen drohen. Das würde vor allem Unternehmen aus sensiblen Branchen wie Banken, Telekommunikationsunternehmen oder aus der Energieversorgung davon abhalten, vertrauensvoll über ihre Probleme zu sprechen. Da sie von CERT.at keine negativen Konsequenzen befürchten müssen, sprechen sie sehr offen auch über Vorfälle in ihrer IT-Struktur.

Das ist wichtig. Denn gerade diese Informationen sind entscheidend, um aus vielen Informationsteilchen ein möglichst vollständiges Mosaik über Gefahren und Sicherheitslücken zusammen zu stellen. „Wir lernen ja gerade von den Details", sagt CERT.at-Leiter Robert Schischka. „Weil die Unternehmen auf unsere Unabhängigkeit und Verschwiegenheit vertrauen können, erzählen sie viel eher, wenn etwas schiefgelaufen ist."

Dass sich diese Unabhängigkeit auszahlt, zeigen die Erfolge in den zehn Jahren seit Bestehen des CERT.at-Teams:

- DNS Poisoning a.k.a. „Kaminsky Bug" (US-CERT VU#800113): Bereits 2008, kurz nach der Gründung von CERT.at, wurde eine schwerwiegende Lücke in der damaligen DNS-Software entdeckt. Über sog. DNS Cache-Poisoning konnten AngreiferInnen dabei falsche Antworten in DNS-Resolver einschleusen, sodass diese bei einer Anfrage IP Adressen von Geräten retournierten, die von den AngreiferInnen kontrolliert wurden. CERT.at warnte vor der Lücke, informierte und unterstützte Betroffene und veröffentlichte einen Bericht über den Vorfall.
- Der Conficker Wurm: 2009, nur ein Jahr später, kam mit Conficker der nächste große Vorfall. Dieser Wurm verbreitete sich rasend schnell über eine Schwachstelle in Microsofts Windows RPC Dienst. Ein Patch war zwar zum Ausbruch bereits vorhanden, allerdings vielerorts noch nicht eingespielt. Obwohl der Wurm keine bösartige Schadsoftware nachlud, sondern sich „nur" von selbst weiterverbreitete und sich auf zahlreichen Windows-Maschinen installierte, war dieses „harmlose" Verhalten zum Zeitbruch des Ausbruchs nicht vorhersehbar. CERT.at konnte bei der Eindämmung des Problems helfen, indem es wiederholt Warnungen und Updates zu neuen Entwicklungen herausgab (siehe hier, hier, und hier), sowie Informationen zu Domänen, von denen der Wurm geladen wurde und fertige Konfigurationsfiles für Bind zur Verfügung stellte.
- Anonymous: Die Teams von CERT.at und GovCERT.gv.at waren bei mehreren Fällen im aktiv bei der Vorfallsbehandlung im Einsatz: So etwa wurde vor Ort Hilfe bei der Forensik, der Absicherung und der Medienarbeit geleistet sowie der Prozess der dauerhaften Korrektur begleitet. In den anderen Fällen agierte CERT (sowohl CERT.at,

als auch GovCERT.gv.at) als Koordinator im Hintergrund, um Erfahrungswerte zusammenzufassen und an Betroffene weiterzugeben. CERT.at veröffentlichte zu diesen Vorkommnissen zwei Special Reports, siehe hier und hier.

- Eine Bedrohung die CERT.at kontinuierlich begleitet sind DDoS Angriffe, bei denen versucht wird, ein System durch möglichst viele Anfragen von verschiedenen Servern in die Knie zu zwingen. Die Gründe für DDoS Attacken sind sehr unterschiedlich und reichen von einfachen „Scherzen" aus Langeweile bis hin zu politischen Aktivismus. In anderen Fällen sind die Motive wiederum krimineller Natur, wenn z.B. versucht wird ein Unternehmen zur Zahlung einer bestimmten Summe zu zwingen, indem bis dahin mit wiederholten Angriffen gedroht wird. Manchmal ist auch überhaupt kein Motiv erkennbar.
  Dementsprechend muss auf solche Attacken unterschiedlich reagiert werden – ein ganzes Security-Team tagelang zu beschäftigen, wenn sich im Endeffekt herausstellt, dass es sich um einen „Streich" gehandelt hat, ist nicht wünschenswert; gleichzeitig darf eine ernsthafte Bedrohung nicht vorschnell unterschätzt werden.
  Einige Beispiele, bei denen CERT.at über DDoS-Angriffe informiert hat, finden sich hier, hier, hier, hier und hier.

Es ist überaus klug, dass Unternehmen aus sicherheitsrelevanten Sektoren eigene CERTs gründen. Diese können sich auf spezifische Sicherheitsfragen ihrer Branche konzentrieren. Koordiniert und in die nationale Sicherheits-Architektur eingebunden wären sie wiederum über CERT.at. Im Fall der Energiebranche ist dies bereits geschehen: 2017 gründeten die Unternehmen das Austrian Energy CERT (AEC), das eng mit CERT.at zusammen arbeitet. Dieses Beispiel eines branchen-eigenen Teams wird auf internationalen Konferenzen mit großem Interesse verfolgt und soll künftig Schule machen. So wären etwa eigene CERTs der Sektoren Gesundheit, Finanzen und Telekommunikation sinnvoll.

Ein wichtiges Gremium für die österreichische IT-Sicherheit ist bereits heute der „Austrian Trust Circle": VertreterInnen von rund 60 Unternehmen aus den sechs sicherheitsrelevanten Sektoren wie Finanzdienstleister, Energieversorger, Industrie, Transport, Gesundheit sowie von Internet-Providern treffen sich unter der Moderation des CERT.at regelmäßig. In vertraulichem Rahmen tauschen sie Informationen aus, um Gefahren zu erkennen und Abwehrstrategien zu entwickeln. Entscheidend ist auch hier das Vertrauen.

Auch im öffentlichen Sektor gibt es ein solches CERT – das GovCERT Austria unter der Federführung des Bundeskanzleramts, für das CERT.at als technischer Dienstleister arbeitet. GovCERT Austria widmet sich den IT-Sicherheitsfragen für Regierungen und Verwaltungen im Bund, in den Ländern und auf kommunaler Ebene.

Wichtige internationale Vernetzung

Kooperation ist für CERT.at auch international wichtig. Denn wie bei einer Epidemie bieten Landesgrenzen auch vor HackerInnen, Cyber-Kriminellen und –SpionInnen keinen Schutz. Die ExpertInnen stehen im ständigen Kontakt mit der weltweiten IT-Sicherheitsbranche und

anderen nationalen CERTs. Sie sind in vielen internationalen Netzwerken aktiv, etwa dem Europäischen Dachverband TF-CSIRT[1], der FIRST und dem CSIRTs Network. Aus all diesen Quellen erhalten sie im Austausch Informationen, um Bedrohungen aus dem Ausland schnell zu erkennen.

Das international koordinierte Vorgehen bei Krisenfällen gehört ebenfalls zur CERT.at-Agenda. Um für diese Fälle bereit zu sein, nimmt CERT.at jedes Jahr an zahlreichen Konferenzen im nationalen, europäischen und internationalen Umfeld teil.

Gesetzlicher Auftrag des CERT.at

Die Europäische Union hat die Notwendigkeit einer gemeinsamen Gefahrenabwehr längst erkannt. Mitte 2016 trat die NIS-Richtlinie in Kraft, die „Directive on Security of **N**etwork and **I**nformation **S**ystems". Sie stellt einen einheitlichen Rechtsrahmen, innerhalb dessen jedes Land Kapazitäten für die Cyber-Sicherheit aufbauen muss. Zudem formuliert sie Mindestsicherheitsanforderungen und Meldepflichten für kritische Infrastrukturen und für Anbieter bestimmter digitaler Dienste wie Cloud-Services oder Online-Marktplätze.

Österreich hatte bereits 2013 eine IT-Sicherheits-Strategie vorgestellt, die viele Punkte der Richtlinie vorwegnahm. Eines ist jedoch neu: Die Richtlinie verlangt von jedem Land, dass es eine offizielle Meldestelle für Sicherheitsfragen einrichtet. Damit hat die Regierung seit April 2019 CERT.at betraut – und der einstigen Stiftungs-Initiative einen gesetzlichen Auftrag erteilt, ohne ihre Unabhängigkeit und Vertraulichkeit anzutasten. Das zeigt eindrücklich die Rolle, die das Team für die IT-Sicherheit in Österreich spielt. Um das Internet im Land gesund zu halten.

2.2 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.

[1] „CSIRT" steht für „Computer Security Incident Response Team" und wird synonym zu „CERT" verwendet.

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 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 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.

2.3 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

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

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 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.

2.4 CERT.at – Zertifizierungen im Jahr 2018

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 27001/2017 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 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 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. 2018 wurden weitere Maßnahmen gesetzt, um das Sicherheitsniveau auch künftig zu erhalten.

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 CERT.at, GovCERT und das IT-Sicherheitsjahr 2018

CERT.at fungiert als Informationsdrehscheibe für Cyber-Sicherheitsprobleme in Österreich, ist also zuständig für Sicherheitsprobleme des von Servern unter der Domäne .at und aller österreichischen IP-Adressen. Dabei hat es selbst kein Durchgriffsrecht und steht Betroffenen mit Informationen und Koordinationsleistungen zur Seite.

Als öffentlich sichtbarer Ansprechpartner für das Thema Cyber-Sicherheit stellt CERT.at Warnungen und Informationen für die Öffentlichkeit bereit. Jeder kann sich bei Interesse über die Homepage für Mailinglisten mit Warnungen und Informationen registrieren.

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.

GovCERT.at ist spezialisiert auf alle Cyber-Sicherheitsprobleme, welche die öffentliche Infrastruktur betreffen.

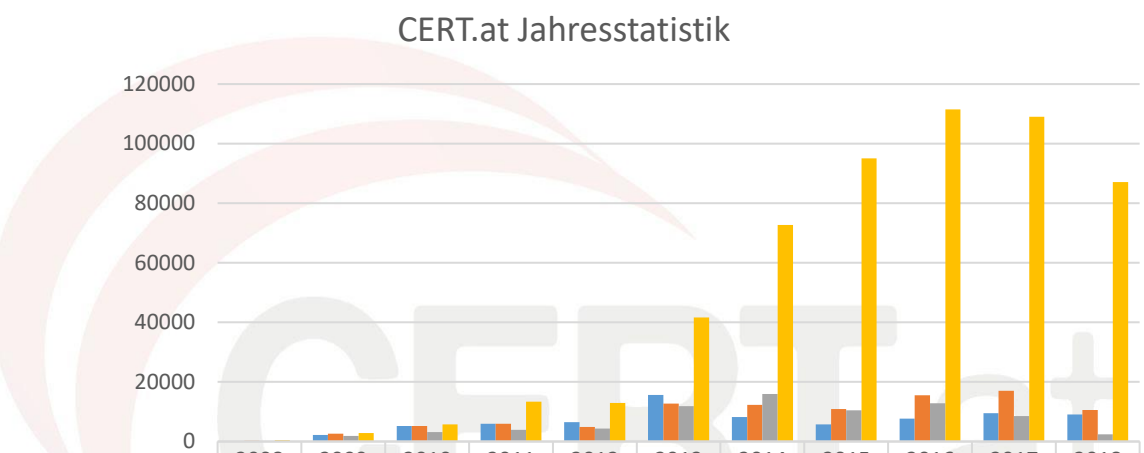
3.1 Die Kommunikation von CERT.at in Zahlen

Die eingehenden und ausgehenden Informationen werden bei CERT.at über ein Ticketsystem erfasst.

Reports sind die Meldungen über Sicherheitsprobleme, die bei CERT.at eingehen, diese werden noch einmal differenziert in Fehlalarme und relevante Reports. Diese können sowohl über automatisierte Datenfeeds als auch als Meldung von Einzelpersonen bei CERT.at einlangen. Meldungen werden grundsätzlich vertraulich behandelt.

Incidents sind Reports, die von CERT.at als sicherheitsrelevant eingestuft werden.

Investigations bezeichnet die Kontaktaufnahme von CERT.at mit Betroffenen. Auch diese Kontaktaufnahme kann automatisiert oder persönlich erfolgen.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701	9537	9045
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055	10627
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556	2400
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003	87118

Seit 2016 wurden Berichte zu Sicherheitsvorfällen bei CERT.at durch die Software IntelMQ zunehmend automatisiert erstellt. IntelMQ wird von mehreren europäischen CERTs als Open Source Software entwickelt. Eine Folge dieser schrittweise erfolgten Umstellung ist es, dass Reports aus mehreren Datenquellen zuerst zusammengefasst und dann erst an Betroffene gesendet werden. Auch die Verarbeitung von fortlaufenden Datenstreams ist leichter möglich. Dadurch sind die Zahlen vor 2016 sowie die aus der Übergangsphase 2016/2017 und jene von 2018 nicht unmittelbar miteinander vergleichbar. Im Folgenden soll IntelMQ kurz vorgestellt werden.

3.2 Spotlight IntelMQ

Hintergrund

Gestartet wurde der Entwicklungsprozess von IntelMQ[4] 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 CERT.at beschlossen daher, selbst ein Tool zu entwickeln, das diese Schwächen nicht aufweist, denn rein manuelle Bearbeitung war und ist aufgrund der Masse an Daten nicht sinnvoll möglich.

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 unerlässlich.

4 Zusammengesetzt aus „Threat INTELligence" und „Message Queueing".

Diese Designprinzipien – Ease-of-Use und Kompatibilität – sind bis heute unverändert und maßgeblich für den Erfolg des Programms verantwortlich.

Viele CERTs 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.

Open Source

Um einerseits die Problematik der hohen Preise, aber auch die Abhängigkeit von einzelnen Personen/Firmen/Institutionen zu lösen, war von Beginn an klar, dass IntelMQ als Open Source Projekt realisiert werden sollte. Es wird daher bis heute im Rahmen des internationalen Incident Handling Automation Projects entwickelt.

Seit mehreren Jahren wird die Weiterentwicklung der Software führend von CERT.at getragen, mit vielen Beitragenen weltweit. Wir übernehmen dabei die Koordination und Planung, sorgen für die Kompatibilität zwischen den Versionen, prüfen Code von externen Beitragen und pflegen diesen ein. Außerdem kümmert sich CERT.at um das Release-Management.

Der Quellcode für IntelMQ ist unter folgender URL zu finden: https://github.com/certtools/intelmq/

Automatisierung

Die Verarbeitung großer Datenmengen kann mit IntelMQ automatisiert erfolgen. IntelMQ sammelt die eingehenden Datenfeeds und verarbeitet sie nach konfigurierbaren Kriterien. Die Daten werden dabei interpretiert, kategorisiert, angereichert und dedupliziert.

IntelMQ verfügt über eine graphische Oberfläche, die es zusätzlich erleichtert, die einzelnen Komponenten zu konfigurieren und das System zu überwachen. Außerdem ist es darüber möglich, einmalige Aussendungen zu generieren. Auf diesem Weg können CERTs innerhalb von kurzer Zeit eine große Menge an Betroffenen informieren, ohne hunderte E-Mails per Hand zu verfassen zu müssen. IntelMQ findet dabei die korrekten EmpfängerInnen automatisch anhand mehrerer Datenbanken.

3.3 Taxonomie

Um einen schnellen Informationsfluss zwischen den unterschiedlichen Cyber-Sicherheits-Akteuren gewährleisten zu können, braucht es eine gemeinsame Sprache. CERTs, 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.

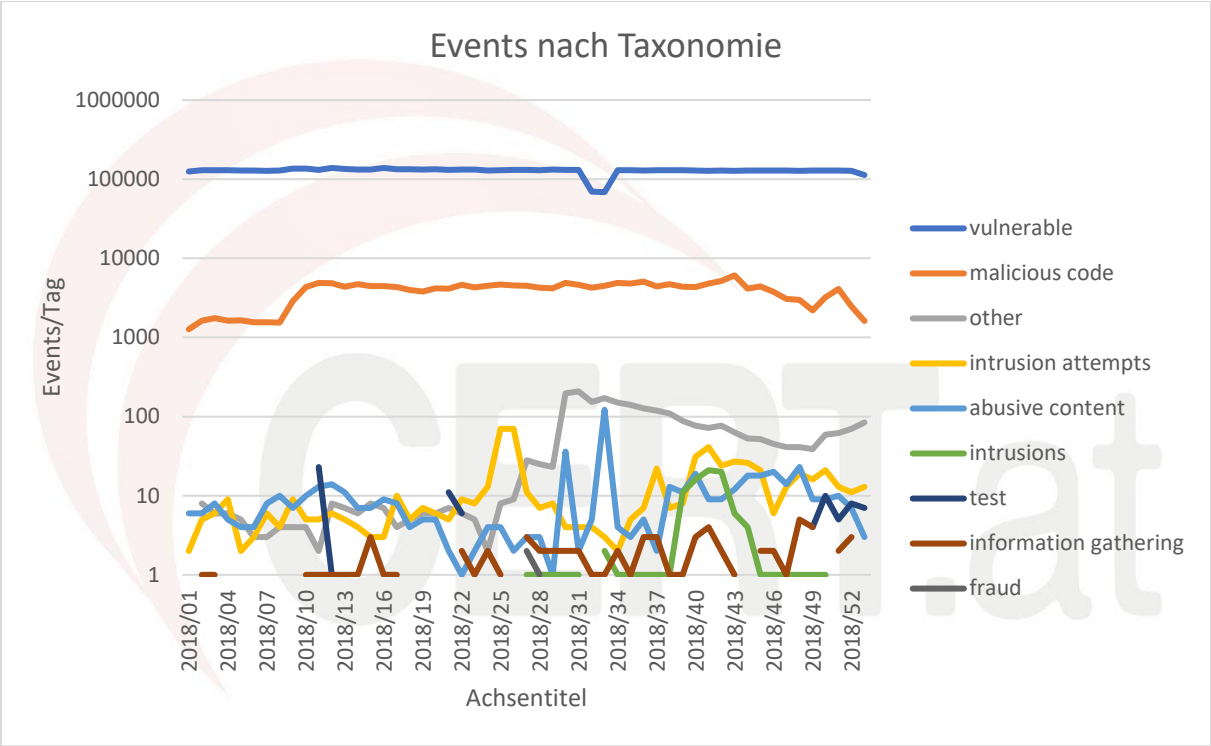
Die Taxonomie, auf die sich CERT.at stützt, ist die eCSIRT II Taxonomy. Die Kategorien dieser Taxonomie sind nicht exklusiv, d.h. mehrere Kategorien können auf einen Vorfall zutreffen.

In Bezug auf Probleme mit Webservern verwendet CERT.at eine noch genauere Aufspaltung der einzelnen Kategorien.

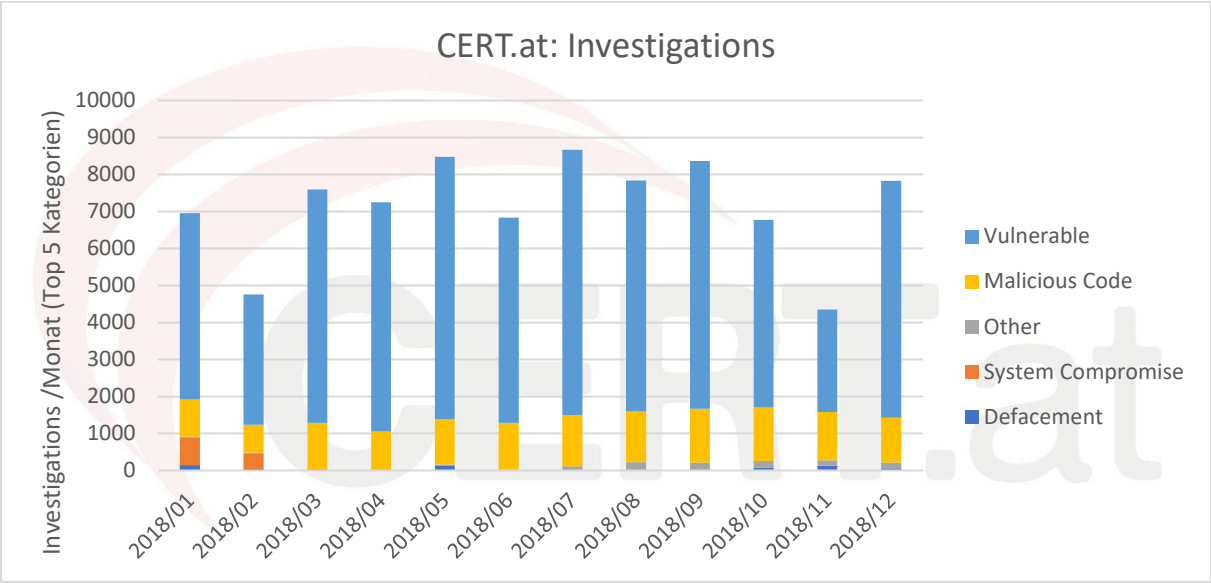
Auf Initiative der TF-CSIRT hat sich eine eigene Arbeitsgruppe gebildet, die sich mit der Weiterentwicklung einer einheitlichen Taxonomie beschäftigt (Reference Security Incident Classification Taxonomy).

eCSIRT II Taxonomy – ein kurzer Überblick

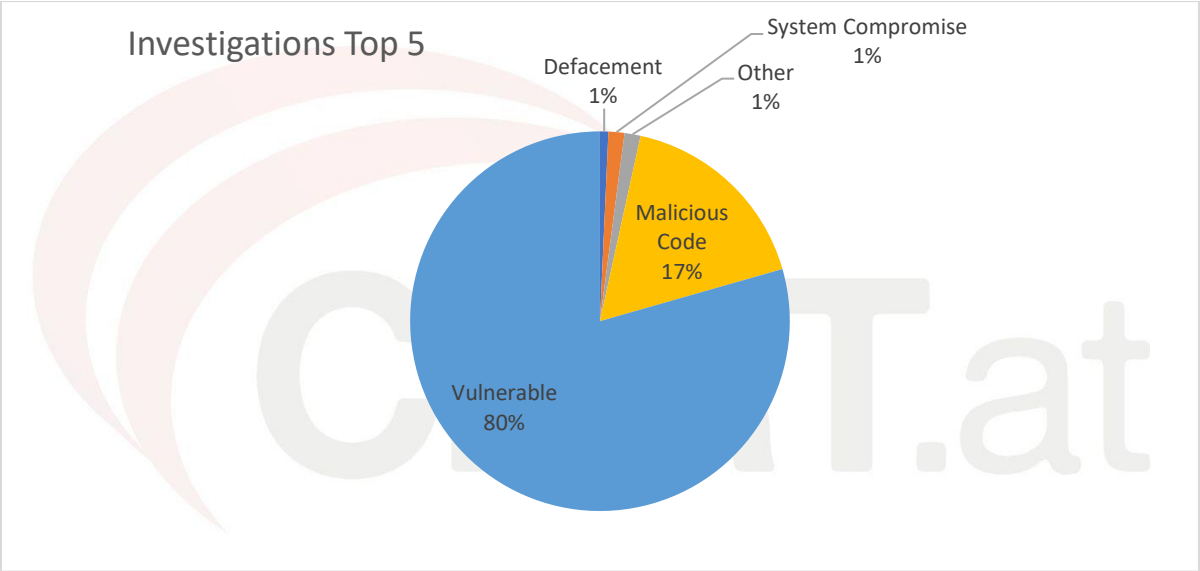
- Abusive Content (Missbräuchliche Inhalte)
- Malicious Code (Schädlicher Code): Software, die absichtlich in ein System eingebracht wird, um Schaden anzurichten.
- Information Gathering (Sammlung von Informationen): Davon umfasst sind: Scannen (Anfragen an ein System, um Schwachstellen zu finden), Sniffing (Netzwerkverkehr beobachten), Social Engineering.
- Intrusion Attempts (Versuchtes Eindringen)
- Intrusions (Eindringen): Erfolgreiches Eindringen in ein System. Das kann remote oder durch ein lokales unautorisiertes Eindringen erfolgen. In dieser Kategorie inkludiert sind auch Botnetze.
- Availability (Verfügbarkeit): Denial of Service-Attacken (DoS, DDoS) setzen Systeme mit einer Flut an Anfragen außer Betrieb. Ein Ausfall kann auch durch Sabotage auf lokaler Ebene oder durch Unfälle verursacht werden.
- Information Content Security (Sicherheit der Informations-Inhalte): Unautorisierter Zugang, Änderung von Informationen oder Fehler auf unterschiedlichen Ebenen.
- Fraud (Betrug): Unautorisierte Verwendung von Ressourcen, Copyright-Verletzungen, Maskierung, Phishing.
- Vulnerable (Schwachstellen): Für Missbrauch anfällig.
- Other (Anderes): Alle Vorfälle, die in keine bekannte Kategorie passen. Wenn die Fallzahlen in dieser Kategorie ansteigen, muss die Klassifikation überarbeitet werden.
- Test (Test): Für Testfälle.



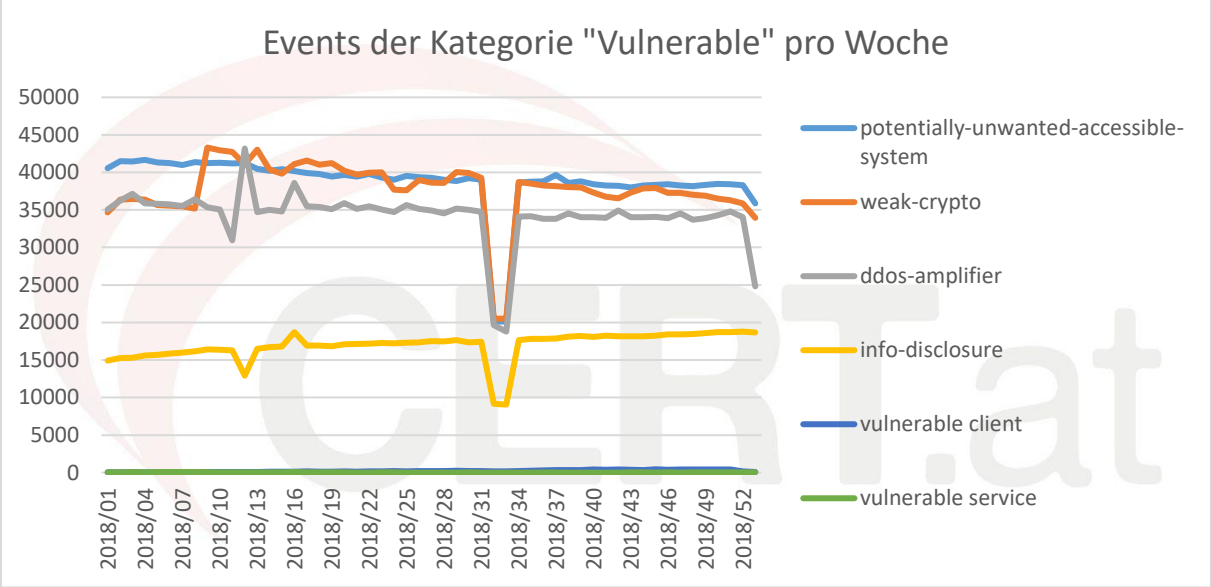
Ein „Event" in der obigen Graphik bezeichnet ein IT-Security relevantes Ereignis, das CERT.at gemeldet wurde. Betreffen mehrere Events einen einzelnen Anbieter (was häufig vorkommt), werden sie in einer Investigation zusammengefasst.



Über das Jahr verteilt ergibt sich im Tortendiagramm folgende Aufteilung:



Aus diesen Graphiken geht klar hervor, dass mit Abstand die meisten Investigations in die Kategorie „Vulnerable“ fallen. Diese kann noch weiter aufgeteilt werden:



In den Kalenderwochen 32 und 33 gab es technische Probleme mit einer unserer wichtigsten Quellen, was die Einbrüche in der Grafik erklärt.

3.4 Was sendet CERT.at an Betroffene aus?

Die obigen Übersichtsgraphiken über die Investigations von CERT.at aus dem Jahr 2018 zeigen, dass die Verwundbarkeit (vulnerable) von Systemen die zahlenmäßig größte Gruppe der Kontaktaufnahmen mit Betroffenen ausmacht. Dann folgen malicious code, other (worunter bei CERT.at hauptsächlich offene Proxy-Server kategorisiert werden), kompromittierte Systeme und verschiedene Kategorien von Website-Hacks.

3.5 Schwachstellen

CERT.at definiert verwundbare Systeme so:

Sie sind offen für Missbrauch aufgrund inhärenter Schwachstellen, die nicht behoben werden können. Ein offener rekursiver DNS Server kann auf dem letzten Software-Stand sein, aber trotzdem missbraucht werden.

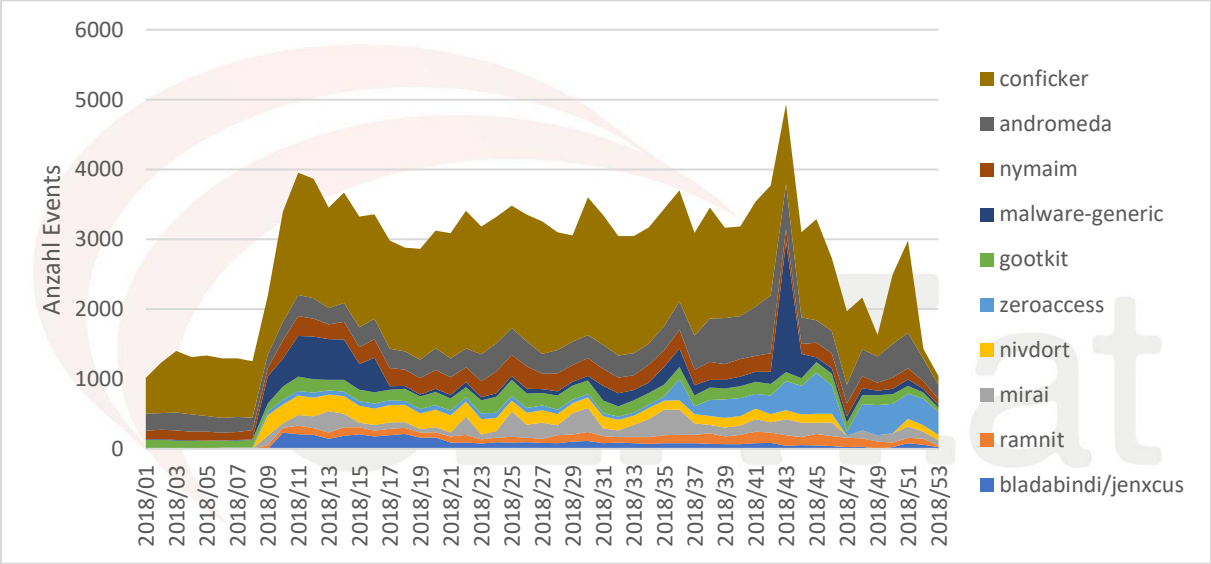
Nicht passwortgeschützt sind (z.B. Webcams, offene VNC Server ohne Passwort etc.).

Veraltete Software, die aktualisiert werden sollte.

Auch lange bekannte und behebbare Sicherheitslücken sind immer noch in den Statistiken von CERT.at zu finden (z.B. SSLv2 und Heartbleed**)**, da die Systeme von den Serverbetreibern nicht aktualisiert wurden.

3.6 Malicious Code

Als Schadprogramm oder Malware (Zusammensetzung aus engl. malicious, "bösartig" und Software) bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und schädliche Funktionen auszuführen. Dieser Begriff bezeichnet keine fehlerhafte Software, auch wenn diese Schaden anrichten kann. Malware wird von Fachleuten der Computersicherheitsbranche als Über-/ Sammelbegriff verwendet, um die große Bandbreite an feindseliger, unerwünschter Software zu beschreiben.



Die Grafik zeigt die Top 10 Malware, über die CERT.at zum Jahr 2018 Daten vorliegen. Da leider noch nicht jede Schadsoftware nachverfolgt werden kann, ist dies nur ein Ausschnitt der tatsächlichen Situation.

3.7 Gehackte Websites

CERT.at informiert Website-Betreiber, wenn von außen erkennbar ist, dass ihre Website gehackt wurde.

Defacement

Die gehackte Website wird für Besucher deutlich sichtbar verändert. Es geht dabei meist um Selbstdarstellung, manchmal sind auch politische Motive im Spiel. (In der eCSIRT II-Taxonomie wäre das Intrusion und Information Content Security).

Exploit Pack

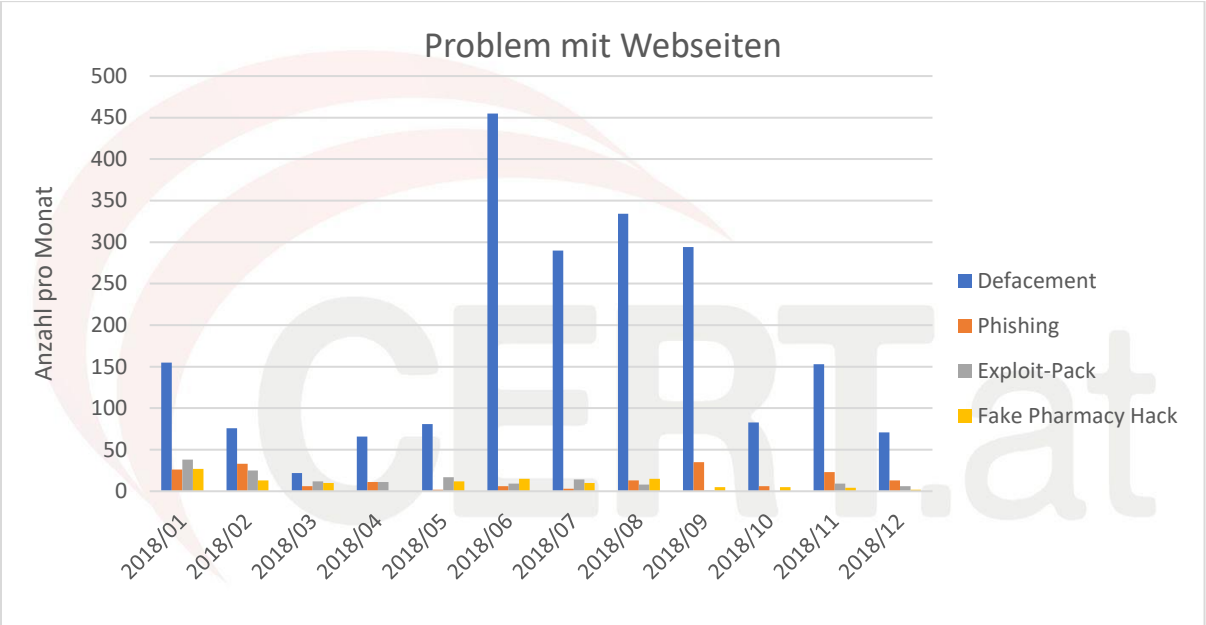
Dabei handelt es sich um Manipulationen einer Website, die über Schwachstellen im Browser eines Besuchers auf dessen Gerät übergreifen können, um es mit Malware zu infizieren. (In der eCSIRT II-Taxonomie wäre das Intrusion und Malicious Code.)

Fake Pharmacy Hack (Google Conditional Hack)

In diesen Fällen liefern Websites andere Inhalte, wenn Besucher über die Google-Suche auf die Website gelangen. In den meisten Fällen sind das Werbeinhalte für Potenzmittel aus dubiosen Quellen. Beim direkten Aufruf über die Adresszeile des Browsers scheinen die gefälschten Inhalte nicht auf. (In der eCSIRT II-Taxonomie wäre das Intrusion, Fraud und Information Content Security.)

Phishing

Phishing Websites ahmen die Websites von Banken, Behörden oder anderen Zielen täuschen echt nach und verleiten die Opfer dazu, ihre Zugangsdaten einzugeben. Diese Zugangsdaten werden dann von den AngreiferInnen gestohlen. Die Phishing Websites werden über Spamkampagnen verbreitet. (In der eCSIRT II-Taxonomie wäre das Abusive Content und Fraud.)



Für die Häufungen in der Grafik ist einerseits zeitliche Begrenzung vieler Kampagnen verantwortlich, andererseits kann es sich auch um eine Schwachstelle in weit verbreiteten CMS-Systemen handeln, die kurze Zeit automatisiert ausgenützt wird, bis ein Patch veröffentlicht wird.

3.8 Datenbasis

Wie kommt CERT.at zu Informationen über Sicherheitsprobleme? Hier folgt eine kurze Übersicht über die unterschiedlichen Datenquellen, die CERT.at heranzieht, um Betroffene von Sicherheitsproblemen zu informieren und sich einen Überblick über die aktuelle Cyber-Sicherheitslage in Österreich zu machen.

3.8.1 Eigene Erhebungen

Scanning Tools

Für die Suche nach ausgewählten verwundbaren Software-Installationen verwendet CERT.at "masscan" oder andere Scanning Tools analog zu Suchmaschinen wie shodan.io. Dieser meldet sich als

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

Der Suchbereich beschränkt sich hierbei üblicherweise auf IP-Ranges mit Österreich-Bezug oder auf .AT domains.

Wie funktioniert das?

Hole aktuelle IP ranges von Österreich (bzw. alle .AT domains)

Mache einen initialen TCP handshake mit jeder IP dieser IP Liste auf dem jeweiligen öffentlich zugänglichen Port (siehe "Aktuelle Scans")

Speichere, ob dieser Port offen war. Wenn ja, gibt es eventuell einen Hinweis, dass die gescannte IP Adresse infiziert ist oder verwundbar ist.

Nach folgenden Verwundbarkeiten hat CERT.at im Jahr 2018 gescannt:

SSLv2

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, IMAPS und POPS aufzubauen. Ist eine Anfrage erfolgreich, verschickt CERT.at eine Warnung an die Betroffenen.

Heartbleed

Die Heartbleed Schwachstelle 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 extrahieren. Darunter können z.B. Passwörter oder ssh-Schlüssel sein.

Leider sind bis heute nicht auf allen Systemen die notwendigen Updates eingespielt worden, es gibt also immer noch verwundbare Server. CERT.at scannt alle .at-Domänen nach dieser Schwachstelle und informiert die Betroffenen über das Problem.

3.8.2 Externe Quellen

IT Firmen

Firmen wie Microsoft, die kommerzielle Sicherheitslösungen anbieten, arbeiten mit CERT.at und anderen CERTs zusammen, indem sie Daten kostenlos zur Verfügung stellen.

Researcher

Zusätzlich existieren Stiftungen und Non-Profit-Organisationen, die Daten für die Sicherheitscommunity erheben.

Die Shadowserver Foundation ist vor allem im Bereich Analyse von Botnetzen und Malware aktiv. Dazu werden Daten aus Honeypots herangezogen – das sind Systeme, die mit dem einzigen Zweck eingerichtet werden, dass sie von Malware angegriffen und ausgebeutet werden können. Die Aktivitäten werden für die Sicherheitsforscher aufgezeichnet. Die

Erkenntnisse daraus liefern wertvolle Analysedaten, um beispielsweise Botnetzen auf die Spur zu kommen und sie auszuschalten.

Spamhaus ist eine Non-Profit-Organisation, die sich auf Spamblocklists spezialisiert hat. Spamhaus arbeitet ebenfalls mit CERTs und Ermittlungsbehörden zusammen.

Suchmaschinen und Archive

Suchmaschinen wie Google oder Shodan inkludieren Hinweise über möglicherweise gehackte Websites oder Netzwerksicherheit in ihre Suchergebnisse.

Websites, die Opfer von defacements geworden sind, werden auf der Website von Zone-H archiviert.

Andere CERTs

Die Cyber-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, und von FIRST, einem globalen Forum für CERTs.

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

Ermittlungsbehörden

Wenn Ermittlungsbehörden ein Schlag gegen die Internetkriminalität gelingt, sammeln sie oft Daten aus der Beschlagnahmung von Domains oder Servern von Botnetzen. Dabei werden die ursprünglich von den Angreifern eingesetzten Steuerserver der Botnetze (sog. "Command and Control Server") durch Sensoren (diese werden "Sinkholes" genannt) ersetzt, die für die Strafverfolgungsbehörden mitprotokollieren, von welchen IP-Adressen infizierte Geräte neue Befehle abholen wollen. Diese 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 sogar Zugang zu Servern der AngreiferInnen zu erlangen. Die dort vorgefundenen Daten geben oft Aufschluss über die Vorgehensweisen und eingesetzten Tools der Kriminellen.

3.9 Reaktion – Hilfe bei Vorfällen

Im Jahr 2018 gab es einen größeren Vorfall, der auch breite Aufmerksamkeit in den Medien erfahren hat.

Spectre/Meltdown (01 / 2018)

2018 begann direkt fulminant mit der Veröffentlichung zweier Side-Channel Angriffe auf Intel-Prozessoren, die unter den Namen Spectre und Meltdown bekannt wurden. Auch wenn sich später herausstellte, dass das Ausnützen dieser Lücken hochkomplex ist, war dies zum Veröffentlichungszeitpunkt noch nicht ganz klar.

CERT.at veröffentlichte einen Blogpost dazu und organisierte zwei Treffen mit den Researchern aus Graz, die an der Entdeckung der Lücken beteiligt waren. Eines fand im Rahmen des monatlichen IT-Security Stammtisches statt und gab dadurch einem breiten Kreis an Personen, die in diesem Feld tätig sind die Möglichkeit, direkt Fragen zu stellen. Das andere wurde im Zuge des EGC (European Government CERTs) Meetings in Wien abgehalten, richtete sich also an Angehörige europäischer Government CERTs.

3.10 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.

ASDEM 2018

Bei der „Austrian Strategic Decision Making Exercise“, kurz ASDEM, handelt es sich um ein Planspiel, welches unter maßgeblicher Beteiligung des KdoFüU&CD, insbesondere in der Rolle seines Kommandanten als (ehemaliger) Cyber-Koordinator des BMLV, vom 20.02. - 21.02.2018 in WIEN an der LVAK stattfand. An dieser Veranstaltung nahmen 118 Personen aus dem IKDOK (BKA, BMLV, BMI, BMEIA, CERT) sowie aus dem Bereich der kritischen Infrastruktur teil. 70 internationale BeobachterInnen aus 21 Ländern und viele nationale BeobachterInnen von öffentlichen Institutionen und Firmen nahmen ebenfalls an der Übung teil.

Der Zweck der Übung bestand in der Überprüfung der gesamtstaatlichen Abläufe im Rahmen des Cyber-Krisenmanagements (CKM) zum Schutz der kritischen Infrastruktur bis hin zur Klärung des Überganges des zivil geleiteten CKM zum militärisch geleiteten Cyber-Verteidigungs-Fall, die Anwendbarkeit auf hybride Anlassfälle und die damit verbundenen politischen, rechtlichen und völkerrechtlichen Problemstellungen. Gerade die hybriden Angriffe, die zeitgleich in der digitalen und analogen Welt stattfanden, hoben diese Übung von anderen ab.

Der Fokus der Übung lag auf der strategischen (Entscheidungs-)Ebene sowie der Kommunikation innerhalb der Ministerien und der kritischen Infrastruktur. Daher wurden bei dieser Übung technische Problemstellungen nicht behandelt. Dementsprechend waren die CERTs nicht in Bezug auf ihre technischen Fähigkeiten gefragt, sondern in ihrer Funktion als Informationsdrehscheibe zwischen den relevanten Stellen im Sinne des NIS-Gesetzes, das damals schon in den Eckpunkten feststand. Zu dieser Funktion zählten die Rolle einer Schnittstelle zu den betroffenen, kritischen Infrastrukturen, das Bedienen internationaler Kontakte auf CERT-Ebene (v.a. über das EU CSIRTs Netzwerk), der Empfang von Meldungen sowie die Sammlung sektoraler Lagebilder inklusive deren Integration in die staatlichen Koordinationsgremien IKDOK und OpKoord.

Die Übung hob sich deutlich vom üblichen Schema der Krisenübungen ab und konnte dadurch interessante Erkenntnisse bezüglich des österreichischen Ansatzes des Cyber-Krisenmanagements (CKM) generieren.

Die Entwicklung der Übung wurde von Seiten Österreichs unterstützt, die Ausarbeitung erfolgte von Seiten der von der Europäischen Verteidigungsagentur (EDA) beauftragten "Estonian Defence League" (EDL), welche in die ASDEM integriert war und die Spielleitung stellte.

Cyber Europe und Cyber Europe Austria 2018

Alle zwei Jahre organisiert die Europäische Agentur für Netzwerk- und Informationssicherheit (ENISA) die größte pan-europäische IT-Notfall- und Krisenübung „Cyber Europe“. Im Jahr 2018 fand diese Übung bereits zum fünften Mal statt und konzentrierte sich auf ein Cyber-Bedrohungsszenario rund um den europäischen Flugsektor. Österreich beteiligt sich unter der Federführung des BKA schon seit 2010 an der Cyber Europe. Seit 2012 erfolgt dies in Form einer parallel abgehaltenen, nationalen Übung, der „Cyber Europe Austria“.

Für die Cyber Europe Austria 2018 (im Folgenden „CE.AT 2018“) wurde das von der ENISA entwickelte, internationale Rahmenszenario einer Cyberkrise im Luftfahrtsektor adaptiert und um österreichspezifische sowie die teilnehmenden Organisationen betreffende Handlungsstränge erweitert. Im Rahmen der CE.AT 2018 wurden gezielte und koordinierte Cyber-Angriffe auf öffentliche Stellen, Organisationen der zivilen Luftfahrt sowie IKT-Betreiber Österreichs simuliert. Im Rahmen dieser Simulation kam es dabei zu schwerwiegenden

Störungen und Ausfällen bei diesen Organisationen sowie massiven Störungen des Flugbetriebs in Österreich.

Im Verlauf der CE.AT 2018 wurden unter anderem die folgenden Angriffsszenarien simuliert:

- DDoS-Attacke gegen die öffentliche Infrastruktur des Flughafens Wien
- Malwarebefall von Netzwerk-Überwachungskameras im Luftfahrtsektor
- Manipulation von Webseiten (Defacements)
- Spear-Phishing-Attacken auf MitarbeiterInnen verschiedener Organisationen der zivilen Luftfahrt sowie der IKT-Betreiber
- APT-Angriffe (APT: Advanced Persistent Threat) und daraus resultierend, Verlust sensibler Daten
- Angriffe auf Flugverkehrsmanagement-Systeme (ATM) und insbesondere auf die Software zur Verwaltung der Flugplandaten
- Ransomware-Befall verschiedener Flughafensysteme
- Notlandung einer Boeing 777 am Flughafen Wien
- Störung der Kommunikation zwischen FluglotsInnen und Flugzeugen
- Totalausfall des Mobilfunknetzes am Flughafen Wien
- Komplikationen aufgrund von Drohnen im An- und Anflugbereich der Runways
- Störung des Differentiellen Globalen Positionierungssystems (DGPS)

An den beiden Übungstagen (06.06. und 07.06.2018) nahmen insgesamt 12 Organisationen aus Österreich an der CE.AT 2018 teil, davon sechs aus dem öffentlichen Bereich, vier Internet- und Serviceprovider, die Österreichische Gesellschaft für Zivilluftfahrt (Austro Control) sowie der Flughafen Wien. CERT.at beteiligte sich an der Übung in zweierlei Funktion, einmal im Rahmen seiner Funktion als operativer Arm von GovCERT Austria sowie als nationales CERT.

Neben dem Tagesbetrieb eines nationalen CERTs, der während der zweitägigen Übung natürlich weiterlief, nahm CERT.at an der nationalen Übung teil und übernahm zusätzlich während dem internationalen Teil der Übung zum wiederholten Male eine zentrale Rolle im CSIRTs-Netzwerk (CNW) der EU ein. Während der internationalen Übung fungierte CERT.at als Krisenmoderator („Facilitator Role“) für alle Teams des EU CSIRTs-Netzwerk, die an der internationalen Cyber Europe mitgewirkt haben.

Die Aufgaben in dieser Rolle bestanden zum einen in der Beobachtung der über diverse Kanälen geteilten Informationen (Email, Chat-Kanäle, eigens für die Cyber Europe erstelltes „Social Media Universum“ usw.) und zum anderen in der Koordination aller notwendigen Maßnahmen (Incident Response, Forensik, etc.) zwischen den CSIRTs der 28 Mitgliedsstaaten. Die administrativen Aufgaben umfassten unter anderem die Durchführung und Moderation von Telefonkonferenzen und deren Protokollierung, die Zusammenführung von Zwischenberichten der einzelnen Teams und die Erstellung des finalen Lageberichts für die EU.

Das vorrangige Ziel der internationalen Cyber Europe ist die Verbesserung der Kooperation auf europäischer Ebene. Im Zuge dessen bot sich 2018 die Möglichkeit, Prozess- und Kooperationsmechanismen, welche sich aus der EU NIS-Richtlinie ergeben, unter den

teilnehmenden Staaten im Rahmen eines Szenarios, in welchem ein internationaler, groß angelegter Cyberangriff auf die Fluginfrastruktur Europas abzielt, zu beüben.

Die Cyber Europe Austria ermöglicht es, nationale Strukturen, Kooperations- und Kommunikationsprozesse auf ihre Effektivität und Effizienz zu testen, um so Stärken und mögliche Defizite aufzuzeigen. Die Beteiligten können auf diese Weise die Vorbereitung auf einen Cyberernstfall optimieren und damit die Resilienz Österreichs erhöhen. Neben der Ausarbeitung von Handlungsempfehlungen aus den Resultaten von Cyber Übungen wie der Cyber Europe Austria, spielen die Kontinuität und das regelmäßige Überprüfen von Strukturen und Prozessen eine große Rolle, um mit den Entwicklungen von Cyberbedrohungen Schritt halten zu können und so eine nachhaltige Widerstandsfähigkeit dagegen zu erreichen. All das konnte den Teilnehmern im Rahmen der Cyber Europe Austria 2018 ermöglicht werden.

3.11 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.

Die s IT Solutions, Mitglied im ATC Finance, beschreiben in folgendem Gastbeitrag den Wert einer ATC-Mitgliedschaft aus ihrer Sicht.

Gastbeitrag: Die aktive ATC-Mitgliedschaft bewirkt eine Stärkung der Widerstandsfähigkeit gegenüber Cyber-Angriffen in Österreich

Julian Obenland, Christian Wagner und Roland Supper

Die Erste Group ist mit circa 16 Millionen KundInnen und mehr als 2500 Filialen in verschiedenen Ländern eine der größten Bankengruppen in Zentral- und Osteuropa. In Österreich sind die Erste Bank Oesterreich und die Sparkassen Mitglieder der Erste Group. Als IT-Dienstleister der Erste Bank und Sparkasse sowie der Erste Group ist s IT Solutions AT Spardat GmbH (kurz s IT Solutions Austria) eine wichtige Organisation in der Gruppe. Ein wesentlicher Schwerpunkt von s IT Solutions Austria ist der Schutz vor Cyber-Angriffen. Deren Abwehr obliegt der Verantwortung des hierfür etablierten Cyber Defense Centers, welches seit 2015 unter der Leitung von Herrn DI (FH) Roland Supper steht. Im Cyber Defense Center analysieren mehr als 20 MitarbeiterInnen täglich sieben bis acht Millionen Log-Daten mithilfe von Automatisierung und spezifischen Tools, um verdächtige Aktivitäten (z.B. global gesteuerte Angriffswellen auf Banksysteme) rechtzeitig zu entdecken. Neben der Analyse von verdächtigen Aktivitäten umfasst das Aufgabengebiet des Cyber Defense Centers noch weitere wichtige Tätigkeiten: Security Governance, Security Mangement, IT Risk Management, Compliance.

Im Jahr 2018 waren Finanzinstitute mit unterschiedlichen Angriffsszenarien konfrontiert, darunter fielen unter anderem:

Angriffe auf KundInnen sowie auch auf die Infrastruktur mit gezielter und zugeschnittener Malware (z.B. Banktrojaner auf mobilen Endgeräten).

Stark verbreitete Phishing-Attacken auf KundInnen mittels täuschend echt wirkender gefälschter Webseiten.

Die jahrelange Erfahrung der einzelnen Mitglieder des Cyber Defense Centers hat gezeigt, dass die Widerstandsfähigkeit gegenüber Cyber-Angriffen durch einen aktiven und intensiven Austausch sowie eine enge Zusammenarbeit mit Organisationen im Finanzsektor erheblich gestärkt werden kann. Weiter ist festzuhalten, dass die Erkenntnis zur Stärkung der Cyber-Sicherheit zum Schutz des europäischen Binnenmarktes auch von Seiten der europäischen Gesetzgebeung erkannt wurde. Hierzu ist auf die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union zu verweisen.

Zur Erhöhung des Reifegrades der Cyber-Sicherheit und somit zur Stärkung der Widerstandsfähigkeit, ist s IT Solutions Austria seit Jahren ein aktives Mitglied des Austrian Trust Circles (ATC) Finance.

Welche Vorteile bringt der ATC für österreichische Unternehmen aus unserer Sicht?

Eine hochprofessionelle Plattform zum vertraulichen und interaktiven Informationsaustausch im Hinblick auf aktuelle Cybersicherheitsangriffe (z.B. Wirtschaftsspionage), geeignete Schutzmaßnahmen (z.B. Good Practices), Tipps zum Sicherheitsmanagement und Sicherheitsvorfallbehandlung.

Die ATC-Mitgliedschaft bietet durch die Expertise der Mitglieder eine kostenfreie Möglichkeit zum Ausbau der hauseigenen Cyber-Sicherheitskompetenzen. Zusätzlich werden regelmäßig Fachvorträge zu spezifischen Themengebieten von FachexpertInnen aus der Cyber Security-Community vorgetragen.

Aufgrund der engen Zusammenarbeit und Kooperation zwischen dem GovCERT, CERT.at und dem österreichischen Bundeskanzleramt reflektiert die Arbeit des ATC aktuelle Impulse und zukünftige Aktivitäten sowie Themenschwerpunkte betreffend Cyber Security.

Durch den interaktiven Austausch und die Vernetzung der ATC-Mitglieder kann über die eigenen Unternehmensgrenzen hinaus ein gutes Bild über die aktuelle Cyber-Sicherheits-Lage in Österreich erworben und kontinuierlich adaptiert werden.

Durch den aktiven Erfahrungsaustausch erhalten ATC-Mitglieder Zugriff auf aktuelle Bedrohungsszenarien im eigenen Sektor.

Neben der aktiven Partizipation am Austrian Trust Circle betreibt s IT Solutions Austria das hauseigene sCERT (CERT der österreichischen Sparkassengruppe) und ermöglicht auch hier eine nationale sowie internationale Vernetzung in der Cyber Security-Community, wodurch s IT Solutions Austria einen breiten Überblick über die aktuelle Cyber Security Thread-Landschaft in Österreich und global erhält.

s IT Solutions Austria hat das sCERT aufgebaut und stellt diese Dienstleistungen auch seinen Netzwerk-/Rechenzentrumskunden zur Verfügung (Erste Group). Zu den Aufgaben von sCERT zählt unter anderem der proaktive und reaktive Umgang mit allen möglichen Arten von IT-Sicherheitsvorfällen, aktive Awareness sowie Cyber Threat Intelligence.

Abschließend kann gesagt werden, dass der Austausch in der Community essentiell ist, um eine hohe Widerstandsfähigkeit des europäischen Bankensektors gegenüber Cyber-Angriffen zu etablieren. Der ATC bietet uns hierfür eine perfekte Plattform.

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 2018 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 haben mit Inkrafttreten des NIS-Gesetzes Ende 2018 einen klaren rechtlichen Rahmen bekommen.

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

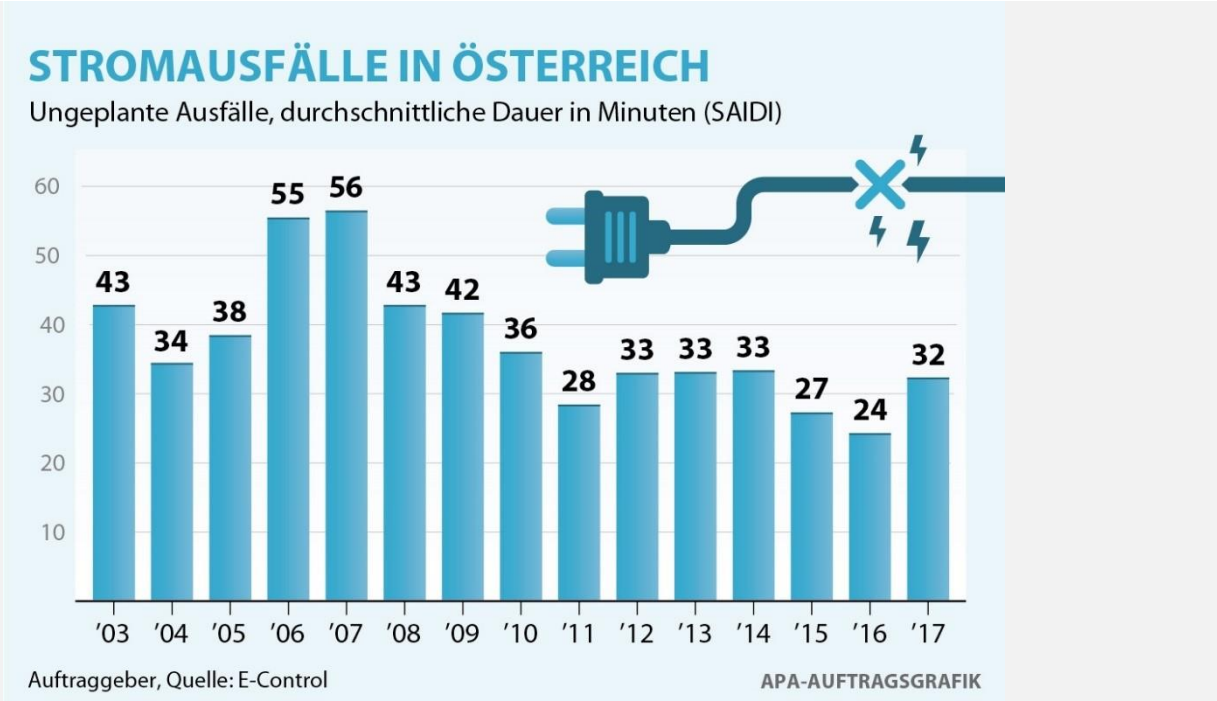
Nach der NIS-Richtlinie der europäischen Union sind alle Betreiber kritischer Infrastruktur verpflichtet, Hackerattacken oder Softwareprobleme an eine Meldestelle zu berichten. In einem einzigartigen Modell hat sich die gesamte Energiewirtschaft Österreichs (Strom, Gas und Vertreter der Ölwirtschaft)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

Im folgenden Gastbeitrag geben das AEC und Österreichs Energieunternehmen einen Einblick in ihre Zusammenarbeit.

Gastbeitrag: Die österreichische Energieversorgung

Die österreichische Energieversorgung ist weltweit eine der stabilsten – Beim Strom gab es im Jahr 2017 nur 32 Ausfallsminuten. Dennoch ist das österreichische Stromnetz keine Insel. Es hängt europaweit mit den Netzen anderer Länder zusammen und das geordnete Funktionieren des Stromnetzes verlangt ein komplexes Zusammenspiel nationaler und internationaler Player.

Fällt ein Teil des Stromsystems aus, kann das unkontrollierbare Kaskadeneffekte nach sich ziehen. Auch das Wieder-Hochfahren des Stromnetzes geschieht im Fall eines Ausfalles nicht auf Knopfdruck, sondern muss abgestimmt und Schritt für Schritt erfolgen.



Betrachtet man den österreichischen Bruttoinlandsverbrauch an Energie, so fällt vor allem der relativ hohe Anteil an erneuerbaren Energien am Gesamt-Energiemarkt auf – vor allem Wasserkraft (9,6%) und biogene Energien (16,8 %) sind im Vergleich zur Gesamt-EU stark vertreten, während Atomkraft als Energielieferant nur im Fall von Stromimporten eine (sehr untergeordnete) Rolle spielt.

Nach Öl ist Gas (22,4% des Verbrauchs) der wichtigste Energieträger, der über ein Netz aus Rohr-Leitungen verteilt wird. Die Physik der Gasnetze unterscheidet sich von jener des Stromes grundsätzlich. Hier werden nicht Elekronen, sondern Moleküle bewegt. Dennoch kann man sich den hierarchischen Aufbau des Netzes analog zum Stromnetz vorstellen. Es gibt internationale und überregionale Transit-Leitungen sowie ein regionales Verteil-Netzwerke, das sich bis zum einzelnen Endverbraucher verzweigt. Analog zur Spannung in den Stromnetzwerken ist der Druck in den überregionalen Verteilnetzen der Gasbranche höher als in lokalen Netzen.

Österreich ist in Bezug auf Gas vor allem ein Transitland – das weitertransportierte Gas übersteigt den Eigenverbrauch Österreichs um das fünffache. Über den Verteilerknoten in Baumgarten wird Erdgas aus Russland, Norwegen und anderen Ländern übernommen und nach Deutschland, Frankreich, Italien, Slowakei, Ungarn, Slowenien und Kroatien weiterverteilt. Das österreichische Gasnetz ist also nicht nur aus Sicht Österreichs, sondern auch aus Sicht der EU eine kritische Infrastruktur, da eine Unterbrechung der transnationalen Leitungen in Österreich auch Engpässe für andere Mitgliedstaaten bedeutet.

Gas spielt auch eine wichtige Rolle in der Stromerzeugung, da erneuerbare Energien nur begrenzt speicherbar sind – wie etwa Wasser in Speicherkraftwerken – oder tageszeitlichen und saisonalen Schwankungen unterliegen (wie Wind- und Sonnenenergie). Gas- und Stromversorgung sind also eng miteinander verknüpft.

Die Speicherkapazität der österreichischen Gasspeicheranlagen reichen aus, um 90% des österreichischen Jahresverbrauchs an Gas vorzuhalten, die Speicherkapazität des Gasnetzes selbst ist ebenfalls beträchtlich und verhindert kurzfristige Ausfälle.

Physik und Vertrauen

Was sind die wichtigsten Parameter, damit wir uns zu jeder Tages- und Nachtstunde darauf verlassen können, dass die Energieversorgung zuverlässig funktioniert?

Für das Funktionieren des österreichischen und auch des transnationalen Stromnetzes ist es essentiell, dass Stromerzeugung und -verbrauch sich die Waage halten. Wird zu wenig Strom produziert, fällt der Strom aus. Kommt es zu Überkapazitäten, sind Überlastungsschäden an Stromleitungen, Kraftwerken und Endgeräten die Folge, die wiederum zu einer automatischen Abschaltung von Teilen des Stromnetzes führen. Das österreichische Stromnetz ist Teil des europäischen Verbundnetzes. Verfügbare Energiemengen und Leistungen werden zwischen den Ländern und Unternehmen auf Energiebörsen gehandelt, jedoch muss für ein Funktionieren des Netzes jederzeit gewährleistet werden, dass es nicht zu größeren Schwankungen in Frequenz oder Spannung kommt.

Historisch mussten sich Stromerzeuger also immer schon darum bemühen, gleichzeitig mit der Verteilung des Stromes auch dafür zu sorgen, dass Informationen zwischen den unterschiedlichen Akteuren des Strommarktes abgestimmt werden, um Netzausfälle zu vermeiden.

Daher spielt der Einsatz von Informationstechnologien seit jeher eine Schlüsselrolle für das Funktionieren der Stromversorgung.

Auch im Gasnetz ist die transnationale Zusammenarbeit über Jahrzehnte eingespielt und die Homogenisierung des Gas-Binnenmarktes ist weit fortgeschritten.

Warum ein branchenspezifisches CERT für den Energiesektor?

Der Einsatz von Informations- und Kommunikationstechnologien (IKT) und die zunehmende Vernetzung in der Energiewirtschaft bringt spezifische Risiken mit sich, die gesondert beobachtet werden müssen.

Im Jänner 2019 berichteten die Medien, dass man knapp einem europaweiten Stromausfall entgangen sei, da es einen Datenfehler in der Frequenzregelung eines deutschen Energieversorgungsunternehmens gegeben hatte. Wenn der Strom flächendeckend auch nur für wenige Stunden ausfällt, ist das nicht nur für jeden einzelnen betroffenen Haushalt ein Problem. Der volkswirtschaftliche Schaden, der angerichtet wird, ist beträchtlich, und die gesamte Kommunikations-, Verkehrs- und Versorgungsinfrastruktur ist betroffen. Ähnliches gilt für Gas, das neben der Wärme- und Energieversorgung in Haushalten besonders in der

Wärmeintensiven Industrie (Hochöfen, Glaserzeugung) zum Einsatz kommt. Beide Energieträger gehören zu Recht zur Kritischen Infrastruktur.

Darum wurde unter der Federführung der E-Control Austria als zuständige Regulierungsbehörde gemeinsam mit den BranchenvertreterInnen der österreichischen Energiewirtschaft, dem Bundeskanzleramt und den sicherheitsrelevanten Bundesministerien im Jahr 2012/13 eine Risikoanalyse über den Einsatz von IKT in der Energiebranche erstellt. Eine der resultierenden Maßnahmen waren Überlegungen zum Aufbau eines eigenen CERT für den Energiesektor.

Die ARGE E-CERT und das Austrian Energy CERT

2015 wurde bei der Branchenvertretung Oesterreichs Energie eine eigene Arbeitsgemeinschaft eingerichtet (ARGE E-CERT), um den Aufbau eines Computer Emergency Response Teams, das speziell auf die Bedürfnisse des Energiesektors abgestimmt ist, rechtlich, organisatorisch und technisch zu begleiten.

Alle wichtigen Player des Energiesektors sind in der ARGE E-CERT vertreten. Derzeit sind das 21 Mitglieder bestehend aus den 13 größten Verteilnetzbetreibern, dem österreichischen Strom-Übertragungsnetzbetreiber, 4 Gas-Verteilnetzbetreibern und Gas-Übertragungsnetzbetreibern, Österreichs größtem Stromhändler und Stromerzeuger und einem Verband von österreichischen kleineren Energieunternehmen sowie einem bedeutenden Unternehmen aus der Ölbranche.

Die Initiative, ein eigenes Austrian Energy CERT (AEC) als Public Private Partnership einzurichten, kommt also aus der Branche selbst und wird von der Zielgruppe des AEC aktiv unterstützt. Die Energiebranche hat damit den Vorteil, einen zentralen Ansprechpartner für Sicherheitsfragen zu haben, der genau auf ihre Bedürfnisse zugeschnitten ist. Europaweit ist das AEC das erste branchenspezifische CERT für den gesamten Energiesektor und dient als

Vorzeigeprojekt, das europaweit Beachtung findet. Der Aufbau des AEC wurde 2016 gestartet, im Mai 2018 ging es in den Vollbetrieb über.

Was tut das Austrian Energy CERT?

Das AEC stärkt die Resilienz des österreichischen Energiesektors, da es einen zentralen Ansprechpartner gibt, der sich mit IT-Sicherheitsfragen des Energiesektors beschäftigt. Das übergreifende Know-how der Unternehmen kann gebündelt und die Erfahrung eines Unternehmens an die anderen übertragen werden. Die Schadensminimierung im Fall von Cyber-Sicherheitsvorfällen ist das erklärte gemeinsame Ziel.

Gleichzeitig ist das AEC in verschiedene internationale Netzwerke eingebunden, die sich mit Cyber-Sicherheit beschäftigen (Europäisches CSIRT-Netzwerk, FIRST, Trusted Introducer, CERT Verbund Österreich) und kann so das Know-how der Cyber-Sicherheitsbranche für den Energiesektor aufbereiten.

Es bietet eine neutrale Informationsdrehscheibe und unterstützt im Fall von Sicherheitsvorfällen die Energieunternehmen. Das AEC arbeitet auch eng mit den staatlichen Behörden zusammen und ist in die operative Koordinierung (OpKoord) eingebunden. Präventions- und bedarfsorientierte Schulungsarbeit runden das Profil des AEC ab.

Da die Energiebranche selbst den Aufbau des AEC initiiert und umgesetzt hat, ist die Zusammenarbeit von großem gegenseitigem Vertrauen geprägt.

Nach dem ersten Jahr im Vollbetrieb zeichnet sich ab, dass das Bewusstsein für Cyber-Sicherheit im Energiesektor durch den Austausch mit dem AEC gewachsen ist und durch den wechselseitigen Austausch weiter in verbesserte Sicherheit investiert wird.

Quellen:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwj54YfW48DiAhVGwMQBHUiJC_0QFjAAegQIBRAC&url=https%3A%2F%2Fwww.apg.at%2F-%2Fmedia%2FCD93015C46A64C86A7F357C81B89C515.pdf&usg=AOvVaw2_0eUScwGKlJhmgnbJoy17

https://www.truppendienst.com/fileadmin/user_upload/Einzelbeitraege/pdf/2017/Fallstudie_BLACKOUT_Stand_28_11_17.pdf

https://www.e-control.at/statistik/strom/statistik-fuer-versorgungsqualitaet/stoerungsstatistik

https://derstandard.at/2000096185439/Europas-Stromnetz-stand-am-Rande-des-Totalausfalls

http://www.udo-leuschner.de/basiswissen/SB124-08.htm

https://www.eccuro.com/artikel/478-wie-funktioniert-eigentlich-das-stromnetz

https://www.ea.tuwien.ac.at/fileadmin/t/ea/lehre/bachelorarbeiten/Edler_-_das_oesterreichische_Gasnetz.pdf

https://www.initiative-gas.at/fileadmin/content/Downloads/Gas-Der-Schluessel-in-eine-gruene-Zukunft.pdf

https://austria-forum.org/af/AustriaWiki/Gas_Connect_Austria

http://www.europarl.europa.eu/factsheets/de/sheet/45/energiebinnenmarkt

---

Ein weiterer Player in der nationalen Zusammenarbeit im Bereich der IT-Sicherheit ist die CSP, die im folgenden Gastbeitrag vorgestellt wird.

Gastbeitrag: Cyber Sicherheit Plattform (CSP)

Dr. Wolfgang SCHWABL – Co-Vorsitzender der CSP

Im Sommer 2018 meldete sich im Bundeskanzleramt eine ausländische Handelsdelegation, die ich als Vertreter der CSP offiziell empfangen durfte. Einer der Delegierten hätte gehört, dass Österreich über eine Plattform verfüge, die für Cybersicherheit sorge. Ich war überrascht von der Tatsache, dass die CSP bereits über die Grenzen Österreichs hinaus bekannt geworden war und Neugier der Gäste erweckte. Mir entging die Enttäuschung der weit gereisten Gäste nicht, nachdem ich ihnen erklärte, dass die CSP keine technische Wunderwaffe gegen Cyberangriffe sei, die unseren Staat schütze.

Die Cyber Sicherheit Plattform (CSP) wurde durch eine Initiative des Bundeskanzleramtes 2015 als Public-Private-Partnerschaft ins Leben gerufen, um allen Verantwortlichen und besonders Interessierten eine Möglichkeit zur Mitwirkung für mehr Cybersicherheit in Österreich zu geben. Die CSP setzt sich zusammen aus VertreterInnen strategischer Infrastrukturen, Behörden, Ministerien, Universitäten und Forschungseinrichtungen, Firmen der Informations- und Kommunikationstechnik (IKT), Vereinen, Medien und sonstiger besonders interessierter Personen. Die Teilnahme ist persönlich, nicht übertragbar und an das Einverständnis mit dem Code-of-Conduct der CSP gebunden. Teilnehmende erklären durch die Zustimmung unter anderem, dass sie bereit sind zur Cybersicherheit Österreichs beizutragen.

Der Vorsitz der CSP wird durch Wahl aus dem Kreis der TeilnehmerInnen für 3 Jahre festgelegt. Seit Beginn im Jahr 2015 haben Dr. Thomas STUBBINGS und ich dieses Ehrenamt inne. Unsere Wiederwahl im Jahr 2018 ist eine Anerkennung unserer Tätigkeiten, die mich besonders ehrt.

Die CSP zählt ca. 250 Personen. 2-3mal jährlich finden Sitzungen statt, an denen ca. 60% der TeilnehmerInnen anwesend sind. Unsere Sitzungen haben informativen Charakter, wo auch Raum für Fragen, kurzen Diskussionen und persönlichen Gesprächen gegeben ist. Für die inhaltliche Arbeit gibt es Arbeitsgruppen, die ihre Ergebnisse in den Sitzungen präsentieren. Besonders stolz sind wir auf das Ergebnis einer Arbeitsgruppe, welche die „Computer Baseline Security Requirements" erarbeitet hatte, die sogar in eine Empfehlung der ENISA eingearbeitet wurden (siehe ENISA: "Indispensable baseline security requirements for the procurement of secure ICT products and services", Jän. 2017)

Von besonderer Bedeutung ist die Tatsache, dass die CSP den Werdegang des NIS (Netz- und Informationssystemsicherheits-) Gesetzes (NISG, BGBl. I Nr. 111/2018) in Österreich begleitet und Vorschläge für wichtige Details erarbeitet hatte. Auch außerhalb der CSP gab es andere Initiativen, z.B. im Rahmen des Rechts- und Technologiedialogs des Kuratoriums Sicheres Österreich (KSÖ), der ISPA und der WKÖ, die ebenfalls ihre Beiträge zum NIS-Gesetz erarbeiteten und Ideen beigesteuert hatten. Besonders erwähnenswert ist die Tatsache, dass die zuständigen LegistInnen der beteiligten Ministerien diese Vorschläge aufmerksam mitverfolgt haben und Wesentliches ins Gesetz übernahmen. Obwohl das Inkrafttreten des NIS-Gesetzes länger dauerte als wir glaubten, so können wir in Österreich stolz darauf sein, dass aus NIS mehr für die Cybersicherheit geschaffen wurde, als die Richtlinie (EU) 2016/1148 (NIS-RL) vorgegeben hätte. Diese Besonderheiten sind:

Es wurden übergreifende Koordinierungsstrukturen (§ 7 NISG) geschaffen, die das effiziente Bearbeiten von Cybervorfällen gestatten. Das sind

IKDOK – der Innere Kreis der Operativen Koordinierungsstruktur, dem Vertreter des BKA, BMI, BMLV und BMEIA angehören, und OpKoord – die operative Koordinierungsstruktur, die aus IKDOK, den (anerkannten) Computer Notfallteams und ggf. auch Vertretern der von einem Vorfall betroffenen Organisationen besteht.

Diese Strukturen bestanden de-facto bereits vor dem Inkrafttreten des NISG. Sie wurden bereits in früheren Cyberkrisenübungen trainiert und haben gezeigt, dass in Österreich eine übergreifende Kooperationsfähigkeit bei Cyberangriffen existiert.

Das NIS Gesetz gilt nicht nur für die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste, sondern auch für die Einrichtungen der öffentlichen Verwaltung (siehe § 22 NISG). Bei Angriffen aus dem Cyberraum kann es jede Organisation treffen. Deshalb ist es vernünftig, gleiche Schutzvorkehrungen sowohl für private Betreiber als auch für die öffentliche Verwaltung vorzuschreiben.

Unabhängig von der Meldepflicht des NISG, haben alle Firmen, Organisationen und sogar öffentliche Einrichtungen ein „Melderecht" von Cybervorfällen und -risiken (siehe § 23 NISG – Freiwillige Meldungen). Dieses Recht gestattet ausdrücklich die Datenweitergabe von personenbezogenen Daten, die sehr oft Teil der technischen Evidenz (z.B. Logfiles, E-mails)

eines Angriffs sind. Diese freiwillige Meldung ist eine Besonderheit im österreichischen Recht, die sachlich eine sehr große Chance für mehr Cybersicherheit für uns alle ist.

Die Meldepflicht (§19, §21) des NISG greift, nachdem etwas Gravierendes passiert ist, ein krisenhafter Cybervorfall die Dienste eines Unternehmens in die Knie gezwungen hat, das Versagen eines digitalen Dienstes von der Öffentlichkeit wahrgenommen wird, oder gar unser gewohntes Leben beeinträchtigt wird. Viele ExpertInnen sind der Meinung, dass aus den Pflichtmeldungen nur einige, wenige Erkenntnisse für mehr Cybersicherheit in Österreich gewonnen werden. Wesentlich mehr Informationen liefern die freiwilligen Meldungen. Alle Einrichtungen haben die Möglichkeit ihre Beobachtungen über Anomalien und bedenkliche Ereignisse im Cyberspace mitzuteilen, lange bevor der Zustand auftritt, dass die Situation meldepflichtig wird. Genau das ist der Mehrwert der freiwilligen Meldung im NISG.

Dank der außerordentlichen Kooperationsfähigkeit, dem starken Willen mehr für Cybersicherheit zu tun, der praxisbewährten CERT-Strukturen, die dank der Initiative der nic.at schon 10 Jahre bestehen, und nun der neu geschaffenen Rechtssicherheit der freiwilligen Meldung im NIS-Gesetz, hat Österreich beste Voraussetzungen für mehr Cybersicherheit. Deshalb appelliere ich an alle VertreterInnen der Betreiber strategischer Infrastrukturen, der Anbieter digitaler Dienste und der Einrichtungen der öffentlichen Verwaltung: Nützen Sie die Möglichkeit der freiwilligen Meldung! Melderecht vor Meldepflicht. Sollte im Cyberspace etwas Außergewöhnliches beobachtet werden, was eine potentielle Gefahr auch für andere Organisationen sein könnte, dann empfehle ich CISOs, CSOs, CERT-, oder IT-LeiterInnen, diese Beobachtung mit allen technischen Details zu melden! DAS ist ein wesentlicher Beitrag zu mehr Sicherheit in Österreich.

Gemeinsam sind wir sicherer, helfen Sie bitte mit!

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. Im folgenden Beitrag soll das CSIRTs Network etwas genauer vorgestellt werden.

Cyber-Sicherheit als transnationales Thema

CERTs (Computer Emergency Response Teams) waren schon immer auf transnationale Zusammenarbeit angewiesen. Die Option, nicht mit ExpertInnen anderer Länder zu kooperieren, existierte in diesem Kontext schlicht nicht.

Diese Zusammenarbeit wurde 2017 in der Europäischen Union gesetzlich durch die NIS-Richtlinie (Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz-und Informationssystemen in der Union) aufgegriffen und in Form des CSIRTs-Netzwerks (Computer Security Incident Response Teams) verankert. Es wurde also vor allem eine neue Vernetzungsplattform auf EU-Ebene für bestehende CERTs der Mitgliedstaaten geschaffen.

Grundlagen des CSIRTs-Netzwerks

Die ExpertInnengemeinschaft, auf die das CSIRTs-Netzwerk aufbaut, ist seit jeher eine internationale. Historisch ist die Zusammenarbeit von verschiedenen CERTs oft „bottom up" rund um eine kleine Gruppe von ExpertInnen entstanden. Diese Netzwerke mit unterschiedlichen Schwerpunkten bestehen zusätzlich zum CSIRTs-Netzwerk weiter (zB Task Force CSIRT, European GovCERT Group auf europäischer Ebene und FIRST auf globaler Ebene).

Auf der Grundlage gemeinsamer technischer Ziele ist eine Verständigung in Bezug auf Cyber-Sicherheit möglich, die die politische Ebene allein nicht leisten könnte. Geteilte technische Expertise, Normen der Kommunikation und best practices bilden die Grundlagen, die es den ExpertInnen ermöglichen, über politische und kulturelle Grenzen hinweg zu kooperieren. Sie sichern die schnelle Weitergabe von Information an Betroffene von Cyber-Angriffen, den Erfahrungsaustausch der SicherheitsexpertInnen und die Koordination von Aktivitäten, um Schaden zu verhindern oder einzudämmen.

Policy-ExpertInnen bezeichnen diesen technischen Diskurs zur Cyber-Sicherheit rund um die CERTs als „Wissenschaftsdiplomatie", die eine fundamentale Rolle bei der Sicherung und Aufrechterhaltung der Integrität und Sicherheit des Internets spielt, die auf rein politischer Ebene nicht abgedeckt werden kann.

Das CSIRTs-Netzwerk in der EU

Das CSIRTs-Netzwerk setzt sich aus bereits bestehenden CERTs der einzelnen Mitgliedstaaten zusammen. Die NIS-Richtlinie zielt auf die Sicherung wichtiger Infrastruktur der Mitgliedstaaten ab, daher können die VertreterInnen im CSIRTs-Netzwerk aus einem oder mehreren CERTs (nationale oder Branchen-CERTs) kommen. Gleichzeitig sind die nationalen CERTs, die hier zusammentreffen, in den Staaten an unterschiedlicher Stelle angesiedelt (etwa im Sicherheitssektor oder wie in Österreich als Public Private Partnership).

Die seit 2004 bestehende ENISA (European Union Agency for Network and Information Security) entwickelt eine europäische Strategie und Policy für Cyber-Sicherheit und unterstützt die Zusammenarbeit des CSIRTs-Netzwerkes administrativ.

Die NIS Cooperation Group, die gemeinsam mit dem CSIRTs-Netzwerk durch die NIS-Richtlinie Anfang 2017 konstituiert wurde, arbeitet auf Ebene der EU-Kommission zusammen, um den Austausch zwischen den Mitgliedstaaten auf Policy-Ebene zu gewährleisten.

Österreichischer Vorsitz des CSIRTs-Netzwerkes

In der zweiten Hälfte 2018 übernahm CERT.at parallel zum Ratsvorsitz Österreichs den Vorsitz des CSIRTs-Netzwerkes. Damit spielte CERT.at in diesem Jahr eine besonders wichtige Rolle für die Weiterentwicklung der Zusammenarbeit. Der erste Bericht über die Aktivitäten und Erfolge des CSIRTs-Netzwerkes an die NIS Cooperation Group wurde im Rahmen des Vorsitzes

Österreichs vorgelegt und wichtige Schritte in Richtung einer gemeinsamen Arbeits-Infrastruktur gesetzt.

Was braucht es also konkret, um eine Basis für die Zusammenarbeit im CSIRTs-Netzwerk zu schaffen?

Vertrauensaufbau

An erster Stelle stehen ein gegenseitiges Kennenlernen und der Aufbau von Vertrauen, damit im Ernstfall eine schnelle und reibungslose Zusammenarbeit möglich ist. Denn im Gegensatz zum organischen Wachstum bestehender ExpertInnennetzwerke wurde die Struktur des CSIRTs-Netzwerkes neu geschaffen und umfasst VertreterInnen von CERTs aus allen Mitgliedstaaten.

Dazu sind drei Treffen im Jahr vorgesehen, 2018 fanden diese in Sofia, Athen und Wien statt. Auf organisatorischer Ebene wurden eine Geschäftsordnung (Terms of Reference, Rules of Procedure) sowie Kommunikationsregeln für den Einsatz im Ernstfall (Standard Operating Procedures) beschlossen an deren Verfassung CERT.ats Teamleiter Otmar Lendl federführend beteiligt war. Ein Arbeitsplan mit kurz-, mittel- und langfristigen Zielen und KPIs (Key Performance Indicators) wurde ebenfalls ausgearbeitet.

Kommunikation

Um eine reibungslose Kommunikation auch abseits von Treffen zu gewährlisten, einigte man sich in Arbeitsgruppen auf ein Portal zum Austausch von Daten, das stetig weiterentwickelt wird. Mailinglisten für administrative Angelegenheiten sowie Kommunikationsschnittstellen für Sicherheitsvorfälle wurden eingerichtet. Zur alltäglichen schnellen Kommunikation dient ein Chat, der sich als „rotes Telefon" im Notfalleinsatz bewährt hat.

Ein regelmäßiger „cyber weather report" bietet einen schnellen Überblick über die aktuelle Bedrohungslage für die Öffentlichkeit.

Weitere Arbeitsgruppen kümmern sich um gemeinsame Tools und technische Grundlagen wie einheitliche Taxonomien für Sicherheitsvorfälle.

Capacity Building/Organisationsentwicklung

Um die Funktionalität der technischen und organisatorischen Lösungen, die in den Arbeitsgruppen des CSIRTs-Netzwerkes gefunden werden, zu überprüfen, finden regelmäßig Übungen statt. Im Jahr 2018 wurden die CyberSOPex und Cyber Europe mit Erfolg abgehalten.

Ein weiterer wichtiger Baustein des CSIRTs-Netzwerks ist die Organisationsentwicklung der einzelnen staatlichen CERTs. Festgelegt wurde ein Reifegradmodell, das in einem peer reviewed Prozess gegenseitig evaluiert wird.

Zudem wurde ein Austauschprogramm ins Leben gerufen, im Rahmen dessen es möglich ist, die CERTs anderer Länder zu besuchen und aus deren praktischen Erfahrungen zu lernen. Einen Teil der Finanzierung übernimmt die EU im Zuge eines CEF (Connecting Europe Facilities) Projektes.

Gemeinsame Einsätze

Nicht zuletzt hat sich die Zusammenarbeit im CSIRTs-Netzwerk auch bei der Hauptaufgabe der CERTs bewährt, dem fortlaufenden Monitoring und der Vernetzung und Information bei Sicherheitsvorfällen im Internet. Deshalb sind neben der Aufbau- und Kooperationsarbeit im Hintergrund auch die regelmäßigen Vorfälle gleichzeitig Messlatte für das Funktionieren der Kooperation als auch Prüfstein für die Weiterentwicklung der Zusammenarbeit.

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, 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 ersten Halbjahr 2018 ein Österreicher und Mitarbeiter von CERT.at Teil des Vorstands von FIRST.

3.12 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.

Mitarbeit an nationalen Forschungsprojekten

CERT.at beteiligte sich auch 2018 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

Mit dem neuen „Netz- und Informationssystemsicherheitsgesetz" setzt Österreich die europäische NIS-Richtlinie um.

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, ist am 29. Dezember 2018 in Österreich das NIS-Gesetz in Kraft getreten (BGBL I Nr. 111/2018). Im Anwendungsbereich des NIS-Gesetzes befinden sich Einrichtungen mit einer hohen Bedeutung für das Funktionieren des Gemeinwesens, weshalb ihre Netz- und Informationssysteme besonders schutzbedürftig sind – so etwa in den Sektoren Energie, Luft-, Straßen- und Schienenverkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur.

Das Gesetz überträgt Aufgaben, die sich aus der Richtlinie ergeben, auf bestehende Strukturen. So legt es Maßnahmen fest, mit denen in den neuralgischen Bereichen ein hohes Sicherheitsniveau erreicht werden soll. 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. Für Betreiber wesentlicher Dienste in den genannten Sektoren, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung führt das Gesetz diverse Pflichten ein. Neben dem Absichern der Netz- und IT-Systeme, die für einen wesentlichen Dienst etwa im Bereich der Flugsicherung verwendet werden, wird auch das Melden von Sicherheitsvorfällen vorgeschrieben.

Nähere Regelungen für die Betreiber dieser „wesentlichen Dienste", wie etwa Sicherheitsvorkehrungen, werden sich in der zu dem NIS-Gesetz zu erlassenden NIS-Verordnung wiederfinden.

Zudem regelt das Gesetz Aufgaben und Zuständigkeiten für die mit der Umsetzung betrauten Behörden sowie deren Befugnisse. Der Bundeskanzler ist gemäß NIS-Gesetz für strategische Aufgaben zuständig, der Bundesminister für Inneres für operative.

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