GovCERT Austria

CERT.at

Bericht

Internet-Sicherheit

Österreich 2024

Inhaltsverzeichnis

Impressum

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

Konzeption und Redaktion: CERT.at

Herstellungsort: Wien, Februar 2025.

Vorwort: Wolfgang Rosenkranz (CERT.at)

Sehr geehrte Leserinnen und Leser,

das Jahr 2024 war für CERT.at – und vermutlich für viele andere Akteure in der Cybersecurity-Szene Österreichs - aus mehrfacher Sicht ernüchternd. Nach vielen Vorarbeiten auf privater und staatlicher Seite ist das NIS 2 Gesetz dann doch nicht in Kraft getreten. Bis zum letzten Moment gab es noch die Hoffnung, dass rechtliche Klarheit geschaffen werden kann, bevor das Parlament für die Neuwahl aufgelöst wird. Es war zwar nicht so, dass es keine Änderungswünsche am Letztentwurf gab, aber die rechtliche Unsicherheit mit einer in Kraft getretenen EU-Richtlinie und einem parallel fehlenden nationalen Gesetz ist keine gute Alternative zu einem nicht perfekten Gesetz.

Wir waren aber nicht alleine am 17. Oktober, als die EU-Frist zur NIS 2 Umsetzung abgelaufen ist. Ganze 23 Mitgliedsstaaten der EU haben es nicht geschafft, den nächsten Schritt in der gemeinsamen Erhöhung der Cybersicherheit in Europa zu gehen. Ob das bedeutet, dass die EU mit ihren Forderungen zu weit gegangen ist, oder ob es bedeutet, dass die Motivation zur Umsetzung ambitionierter Cybersecurity-Gesetze in mehreren Ländern zu gering war, ist schwer zu sagen. Wenn man der Diskussion zu NISG 2024 im österreichischen Parlament folgte, dann war das Problem wiederum ein rein politisches. Es wird in jedem Fall spannend sein zu sehen, wie die nächste Regierung NIS 2 – hoffentlich als NISG 2025 und nicht als NISG 2026 - in Österreich beschlussfähig machen wird. Fix ist, dass im Finanzbereich DORA nun vor NIS 2 umgesetzt wird. Mit 17. Jänner trat DORA automatisch in der EU in Kraft und bringt um einige Maßnahmen und Vorgaben mehr, als NIS 2 einführen wird. Der Vorteil dabei ist, dass alle anderen Sektoren sich ansehen können, wie der Finanzsektor mit diesen Vorgaben umgeht und was vermutlich mit NIS 3 auf alle anderen zukommen wird.

Das Jahr 2024 war aber auch aus anderer Sicht enttäuschend. So mussten wir als CERT im letzten Jahr sehr oft vor Schwachstellen in Sicherheitsprodukten warnen – oft vor neuerlichen Schwachstellen in Produkten derselben Hersteller. Das gerade Sicherheitsprodukte für Sicherheitsprobleme sorgen, ist extra ärgerlich. Dass es sehr schwierig ist, mit diesen internationalen Unternehmen eine gemeinsame Vorgangsweise bei der Information ihrer Kunden zu erreichen, reduziert den Ärger nicht unbedingt. Ob der Cyber Resiliance Act, die NISG-Umsetzung oder eine andere EU-Rechtsvorschrift die meistens internationalen Hersteller dieser Geräte zu mehr Kooperation bringen wird, bleibt abzuwarten.

Sicherheitstechnisch war 2024 geprägt von Phishing. Bei jeder Diskussion zur aktuellen Bedrohungslage, sei es im Austrian Trust Circle, im CERT-Verbund oder bei öffentlichen Veranstaltungen, war Phishing die am häufigsten genannte Bedrohung. Überspitzt gesagt wurden die Menschen im letzten Jahr zum schwächsten Glied in der Cybersecurity-Kette. Das muss sich ändern, denn wir können uns bei einer immer intensiveren Verwendung von digitalen Systemen nicht darauf verlassen, dass Menschen keine Fehler machen. Die Lösung wird nicht einfach sein und sie wird nicht aus einer einzelnen Komponente bestehen. Die CERTs sind als Informationsdrehscheiben ein Teil der Antwort, es muss aber auch innovative technische Antworten geben.

Positiv war 2024, dass wir mit dem Austrian Health CERT (AHC) nun auch ein Sektoren-CERT aus dem Gesundheitssektor in Österreich haben. Betrieben wird das Gesundheits-CERT bei der AGES, der österreichischen Agentur für Gesundheit und Ernährungssicherheit. Wir durften als

CERT.at die AGES bei der Gründung des AHC unterstützen und freuen uns auf die weitere Zusammenarbeit.

Das Jahr 2025 hat mit internationalen Krisen, fortgesetzten Kriegen und immer mehr Artificial Intelligence begonnen. Das Thema Cybersecurity ist zwar inzwischen ein überall unbestritten wichtiges Thema, es besteht aber die Gefahr, dass es durch alternative Themen wie Desinformation, Wirtschaftskrisen oder (geo-)politische Spannungen in den Hintergrund gerückt wird. Nicht nur in der allgemeinen Aufmerksamkeit, sondern auch in Bezug auf die Finanzierung der vielen Dinge, die noch zu tun sind, damit die Digitalisierung „cybersicher“ wird.

Als CERT.at werden wir wieder unser Bestes geben, damit das Thema im Vordergrund bleibt, damit die Community bestmöglich über Risiken und Gefahren informiert wird und damit jenen geholfen wird, die trotz aller Schutzmaßnahmen angegriffen werden. Ich wünsche Ihnen aber nun viel Vergnügen bei der Lektüre der Ereignisse von 2024 aus CERT-Sicht und freue mich auf die Zusammenarbeit im kommenden Jahr!

Wolfgang Rosenkranz

Teamleiter CERT.at

Kapitel 1

CERT.at und GovCERT Austria

CERT.at als nationales Computer-Notfallteam nach NIS-Gesetz und GovCERT Austria leisten einen wichtigen Beitrag für die IT-Sicherheit in Österreich und seiner Behörden. Eine enge Zusammenarbeit hilft dabei, Probleme flächendeckender angehen zu können.

1.1 CERT.at – Österreichs nationales CERT

CERT.at ist das nationale Computer-Notfallteam Österreichs (Computer Emergency Response Team) und spielt eine zentrale Rolle in der Cybersicherheitslandschaft des Landes. Es wurde 2008 in Zusammenarbeit mit dem Bundeskanzleramt (BKA) und der österreichischen Domain-Registrierungsstelle nic.at als Projekt ins Leben gerufen. Gemeinsam mit GovCERT Austria, das speziell für den öffentlichen Sektor zuständig ist, fungiert CERT.at als erste Anlaufstelle für IT-Sicherheitsfragen im nationalen Kontext. Zuständig ist das Team für alle Vorfälle, die nicht bereits durch spezialisierte CERTs, etwa Sektoren-CERTs wie das Energy-CERT un das Gesundheits-CERT, abgedeckt werden.

Seit 2019 erfüllt CERT.at zudem die Funktion des nationalen Computer-Notfallteams gemäß NIS-Gesetz. Dadurch ist die Zusammenarbeit mit Betreibern wesentlicher Dienste, kritischer Infrastrukturen und relevanten staatlichen Einrichtungen weiter intensiviert worden. Dies stärkt die Reaktionsfähigkeit auf nationale und internationale Cybersicherheitsvorfälle und ermöglicht eine engere Abstimmung zwischen Wirtschaft, Behörden und anderen Sicherheitsteams.

CERT.at überwacht laufend die Bedrohungslage, verbreitet sicherheitsrelevante Informationen, vernetzt sich aktiv mit nationalen und internationalen Partnern und reagiert auf potenzielle Risiken. Über die reine Reaktion auf Vorfälle hinaus engagiert sich CERT.at auch in der Prävention: Dazu gehören Maßnahmen zur Früherkennung von Bedrohungen, Notfallvorbereitungen, Aufklärungsarbeit sowie Beratung für Unternehmen, Organisationen und die Öffentlichkeit. Als zentrale Anlaufstelle für sicherheitsrelevante IKT-Ereignisse in Österreich fungiert CERT.at als vertrauenswürdige Informationsdrehscheibe, die Wissen bündelt und weitergibt.

CERT.at ist zudem ein zentrales Bindeglied zwischen anderen CERTs und CSIRTs (Computer Security Incident Response Teams), insbesondere in den Bereichen kritischer Infrastruktur und

der Informations- und Kommunikationstechnologie (IKT). Das Team gibt regelmäßig Warnungen und Hinweise zu aktuellen Bedrohungen heraus und bietet praxisnahe Empfehlungen für Unternehmen und Privatpersonen. Im Falle eines Angriffs auf IT-Systeme auf nationaler Ebene übernimmt CERT.at die Koordination der Reaktionsmaßnahmen und informiert Netzbetreiber:innen sowie zuständige Sicherheitsteams. Dabei liegt der Fokus auf der schnellen und effektiven Bewältigung von akuten Sicherheitsvorfällen.

Das Team besteht derzeit aus 9 Expert:innen und wird von Robert Schischka als Geschäftsführer sowie Wolfgang Rosenkranz als Teamleiter geleitet. Wichtig ist dabei eine klare Abgrenzung: CERT.at ist keine Ermittlungsbehörde und hat keine Eingriffsrechte in die österreichische Netzwerkinfrastruktur. Das Team arbeitet rein koordinierend und beratend, unterstützt aber aktiv dabei, Cybersicherheitsvorfälle zu bewältigen und Österreichs digitale Widerstandsfähigkeit zu stärken.

1.1.1 CERT-Beirat – Strategische Leitplanken

CERT.at wird in seiner strategischen Ausrichtung von einem eigens dafür eingerichteten Beirat begleitet. Dieses Gremium setzt sich aus Expert:innen zusammen, die einen repräsentativen Querschnitt der österreichischen Internetgemeinde abbilden.

Die Mitglieder des Beirats agieren als engagierte Botschafter:innen für CERT.at und tragen dazu bei, dass die Organisation ihre Aufgaben im Sinne der gesamten Gesellschaft wahrnimmt. Sie stellen sicher, dass CERT.at seine Maßnahmen und Strategien stets mit einem ganzheitlichen Blick auf die österreichische IT-Landschaft entwickelt und umsetzt.

Dadurch trägt der Beirat maßgeblich zur Stärkung der IT-Sicherheit sowie zur Erhöhung der Resilienz vernetzter Systeme in ganz Österreich bei.

Die Mitglieder des CERT-Beirats waren 2024:

- DI Philipp Blauensteiner (BVT)
- Mag. Wolfgang Ebner (BMDW)
- Michael Eichinger (BMI)
- Univ. Prof. Dr. Nikolaus Forgo (Universität Wien)
- Andreas Koman (Internetstiftung)
- Ing. Thomas Mandl (CDCE)
- Ing. Clemens Möslinger, BA MSc (BKA)
- Christopher Ozvald (BMG)
- Christian Panigl (UniVie/ACOnet/VIX)
- Univ. Prof. Dr. Reinhard Posch (TU Graz)
- Ing. Robert Scharinger, MBCS (Gesundheitsministerium)

- Lambert Scharwitzl (BMLV)
- Andreas Schildberger (BOKU)
- Robert Schischka (nic.at)
- Ing. Dr. iur Christof Tschohl (Research Institute & Co. KG)
- Christian Zec (BKA)
- Markus Kloibhofer (BMF)
- Franz Hoheiser-Pförtner (Wien)

1.1.2 Vernetzung

CERT.at ist keine isoliert arbeitende Einrichtung, sondern eine zentrale Koordinations- und Informationsstelle, die aktiv zur Sicherstellung der IT-Sicherheit in Österreich beiträgt. Im Falle eines Angriffs auf IKT-Systeme nimmt das Expert:innen-Team Kontakt mit den jeweiligen Netzbetreiber:innen und zuständigen Security-Teams auf, um schnell und effizient auf Vorfälle zu reagieren. Ziel ist es, Probleme rasch zu identifizieren, deren Auswirkungen einzudämmen und gemeinsam mit allen Beteiligten effektive Lösungen zu erarbeiten. Dabei handelt es sich um ein freiwilliges Angebot, das sich durch enge Zusammenarbeit und ein hohes Maß an Fachwissen auszeichnet.

Ein wesentlicher Bestandteil der Arbeit von CERT.at ist die Vernetzung mit anderen Organisationen, um Bedrohungen nicht nur lokal, sondern auch im internationalen Kontext effizient zu bekämpfen. Die Kooperation reicht von der EU-Agentur für Cybersicherheit (ENISA) über internationale Konzerne und CERTs/CSIRTs anderer Staaten bis hin zu nationalen Sicherheitsteams, Universitäten, Fachhochschulen und Forschungseinrichtungen. Auch engagierte Privatpersonen leisten wertvolle Beiträge zur gemeinsamen Sicherheit des österreichischen Internets. CERT.at ist dabei nicht nur Empfänger und Versender von Informationen, sondern unterstützt alle Akteure auch beim direkten Erfahrungs- und Informationsaustausch untereinander.

Durch diesen breit gefächerten Austausch und die gebündelte Expertise trägt CERT.at maßgeblich dazu bei, die digitale Resilienz des Landes kontinuierlich zu stärken und neuen Herausforderungen in der Cybersicherheit proaktiv zu begegnen.

1.1.3 Gesetzlicher Auftrag von CERT.at

Die Europäische Union hat die Bedeutung einer koordinierten und gemeinsamen Gefahrenabwehr im Bereich der Cybersicherheit längst erkannt. Ein bedeutender Meilenstein in dieser Entwicklung war das Inkrafttreten der NIS-Richtlinie („Directive on Security of Network and Information Systems“, kurz NISG) Mitte 2016. Diese Richtlinie schafft einen einheitlichen Rechtsrahmen, innerhalb dessen alle EU-Mitgliedstaaten ihre Kapazitäten zur Cybersicherheit ausbauen müssen. Sie definiert zudem verbindliche Mindestsicherheitsanforderungen sowie Meldepflichten für Betreiber kritischer Infrastrukturen und Anbieter essenzieller digitaler Dienste wie Cloud-Services oder Online-Marktplätze.

Österreich war in diesem Bereich bereits früh aktiv und hatte 2013 eine eigene IT-Sicherheitsstrategie vorgestellt, die viele der später in der NIS-Richtlinie verankerten Maßnahmen vorwegnahm. Eine wesentliche Neuerung brachte die Richtlinie dennoch mit sich: Sie verpflichtet jedes EU-Land dazu, ein offizielles Computer-Notfallteam (CSIRT) zu benennen, das für die Cybersicherheitskoordination auf nationaler Ebene zuständig ist.

Auf dieser rechtlichen Grundlage (§ 15 Abs. 3 NISG) wurde CERT.at im März 2019 vom Bundeskanzleramt (BKA) per Bescheid mit dieser Aufgabe betraut. Dabei blieben die Unabhängigkeit und Vertraulichkeit von CERT.at unangetastet – ein essenzieller Aspekt, um die vertrauensvolle Zusammenarbeit mit verschiedenen Akteuren sicherzustellen. Seither übernimmt CERT.at eine zentrale Rolle in der nationalen Cybersicherheitsstrategie und trägt maßgeblich zur Abwehr und Bewältigung digitaler Bedrohungen bei. Durch die enge Zusammenarbeit mit Behörden, Unternehmen und internationalen Partnern unterstützt es die Umsetzung der NIS-Richtlinie und stärkt die Resilienz der digitalen Infrastruktur in Österreich.

1.2 GovCERT Austria – Expertise im Behördenbereich

GovCERT Austria ist das Government Computer Emergency Response Team für die öffentliche Verwaltung in Österreich und fungiert als zentrale Anlaufstelle für staatliche Institutionen im Falle eines Cyberangriffs. Es wird vom Bundeskanzleramt betrieben und übernimmt die Funktion des Computer-Notfallteams gemäß NISG für den öffentlichen Sektor. Damit stellt GovCERT Austria sicher, dass Behörden auf nationaler, regionaler und kommunaler Ebene bestmöglich auf Cyberbedrohungen vorbereitet sind und im Ernstfall rasch und koordiniert reagieren können.

Auf internationaler Ebene agiert GovCERT Austria als offizieller Ansprechpartner für Regierungen und internationale Organisationen zu Fragen der Cybersicherheit. Es pflegt einen engen Informationsaustausch, sammelt und analysiert sicherheitsrelevante Erkenntnisse und gibt bei Bedarf Warnungen und Handlungsempfehlungen an inländische Stellen weiter. Durch diese Vernetzung trägt GovCERT Austria wesentlich dazu bei, globale Bedrohungslagen frühzeitig zu erkennen und effektive Gegenmaßnahmen zu entwickeln. Dabei arbeitet es in enger Zusammenarbeit mit CERT.at, wodurch Synergien optimal genutzt und Ressourcen effizient gebündelt werden.

Neben seiner Rolle als koordinierendes Notfallteam übernimmt GovCERT Austria weitere zentrale Aufgaben im Bereich der Cybersicherheit für die öffentliche Verwaltung. Es fungiert als Schnittstelle zwischen Bundesministerien, Landesregierungen, Städten, Gemeinden und verfassungsmäßigen Einrichtungen des Bundes und unterstützt diese bei der Bewältigung von IT-Sicherheitsvorfällen. Darüber hinaus leistet es einen entscheidenden Beitrag zur Prävention, indem es Bedrohungen frühzeitig identifiziert, strategische Sicherheitsmaßnahmen entwickelt und sicherheitstechnische Expertise bereitstellt.

Ein besonderer Fokus liegt auf der laufenden Überwachung der nationalen Bedrohungslage. GovCERT Austria analysiert sicherheitsrelevante Vorfälle im operativen IKT-Betrieb der öffentlichen Verwaltung, gibt frühzeitig Warnungen heraus und informiert über bestehende Risiken. Im Ernstfall reagiert es rasch auf Sicherheitsvorfälle, koordiniert Maßnahmen mit den betroffenen Stellen und leistet bei Bedarf auch direkte Unterstützung vor Ort.

Um seine Expertise kontinuierlich zu erweitern und die Zusammenarbeit mit nationalen und internationalen Partnern zu vertiefen, nimmt GovCERT Austria regelmäßig an Cyber-Übungen teil. Diese Simulationen ermöglichen es, realistische Angriffsszenarien durchzuspielen, Prozesse zu optimieren und das Sicherheitsniveau weiter zu erhöhen. Damit leistet GovCERT Austria einen essenziellen Beitrag zur Resilienz der öffentlichen Verwaltung und trägt dazu bei, Österreichs digitale Souveränität langfristig zu stärken.

1.2.1 Public-Private-Partnership mit vielen Vorteilen

Da das GovCERT als Public-Private Partnership (PPP) des Bundeskanzleramtes mit nic.at (dem Mutterunternehmen von CERT.at) eingerichtet wurde und auf das gleiche technische Team wie CERT.at zurückgreift, erhält der Staat Zugriff auf qualifizierte, technische Cybersicherheitsexpertise aus dem Privatsektor sowie auf das Kontaktnetzwerk von CERT.at, welches nationales und internationales Know-how und relevante Sicherheitsinformationen (z.B. klassifizierte Dokumente, White Papers usw.) bereithält.

Hinzu kommt die Mitarbeit an und das Teilen von gesamtstaatlichen Cyberlagebildern im Rahmen von OpKoord[1] und IKDOK[2] und die Teilnahme an Expert:innenworkshops, Trainings und sonstigen einschlägigen Fach- und Netzwerkveranstaltungen.

1.3 Kernaufgaben von CERT.at und GovCERT Austria

Die Bedeutung der von CERT.at und GovCERT Austria wahrgenommenen Aufgaben wird durch die zunehmende Bedrohungslage im Bereich der IT-Sicherheit immer deutlicher. In den letzten Jahren haben sich sowohl die Komplexität digitaler Systeme als auch die Zahl der vernetzten Geräte rasant erhöht. Gleichzeitig gehen Angreifer:innen immer professioneller, koordinierter und gezielter vor, was die Anforderungen an Cybersicherheitsmaßnahmen erheblich verschärft.

CERT.at und GovCERT Austria übernehmen in ihren jeweiligen Zuständigkeitsbereichen eine Vielzahl essenzieller Aufgaben, um diesen Herausforderungen wirksam zu begegnen. Durch ihre enge Zusammenarbeit stellen sie sicher, dass Cyberbedrohungen frühzeitig erkannt, analysiert und effektiv abgewehrt werden. Sie koordinieren Reaktionsmaßnahmen, geben fundierte Warnungen und Handlungsempfehlungen heraus und unterstützen betroffene Organisationen gezielt bei der Bewältigung von Sicherheitsvorfällen.

Neben der akuten Incident Response leisten beide Organisationen auch einen wichtigen Beitrag zur Prävention und Resilienzsteigerung. Sie sensibilisieren Unternehmen, Behörden und die Öffentlichkeit für aktuelle Gefahren, entwickeln Strategien zur Risikominimierung und fördern den kontinuierlichen Austausch mit nationalen und internationalen Partnern.

In einer zunehmend digitalisierten Welt sind die Aufgaben von CERT.at und GovCERT Austria unverzichtbar, um die Sicherheit und Stabilität der österreichischen IT-Infrastruktur nachhaltig zu gewährleisten. Ihr gemeinsames Ziel ist es, ein widerstandsfähiges, gut vernetztes und

[1] Staatliche **Op**erative **Koord**inierungsstruktur für den koordinierten Einsatz der Cyberkräfte
[2] Der **I**nnere **K**reis **d**er **o**perativen **K**oordinierungsstruktur nimmt zentrale Aufgaben der OpKoord wahr

proaktives Cybersicherheitsumfeld zu schaffen, das den steigenden Bedrohungen wirkungsvoll entgegentreten kann.

Information in allen Bereichen: CERT.at und GovCERT Austria verfolgen laufend die Nachrichtenlage zur globalen IT-Sicherheit. Daraus entstehen Warnungen (via Web, Mail, RSS, Presse) 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.

CERT.at stellt diese Warnungen und Zusammenfassungen zum Abruf auf der CERT.at-Website bereit (cert.at). Zusätzlich kann man diese Informationen nach Registrierung über die Website auch als E-Mail erhalten.

Netzwerkhygiene: CERT.at sammelt Informationen zu konkreten Sicherheitsproblemen im österreichischen Teil des Internet, wie etwa infizierte Computer, manipulierte Webseiten oder falsch konfigurierte Server. Dazu stützen sich CERT.at und GovCERT Austria neben eigener Sensorik auf Quellen[3] 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 laufend zu heben.

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

Vernetzung: Neben der reinen technischen Rolle der CERTs als Informationsdrehscheibe und Hilfe bei Vorfällen fungieren sie auch als Kristallisationspunkt für die Vernetzung der in diesem Bereich arbeitenden Fachleute. Das reicht von selbst organisierten Foren wie dem Austrian Trust Circle oder dem IT Security Stammtisch, der aktiven Teilnahme an anderen Veranstaltungen der IT Security Community bis hin zur Mitarbeit bei Forschungsprojekten. Ebenso liefern die CERTs bei Bedarf Entscheider:innen technische Expertise, um die Entwicklung von Gesetzen und Richtlinien im Sinne der Cybersicherheit positiv zu unterstützen.

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

1.4 Zertifizierungen 2024

1.4.1 ISO 27001 Zertifizierung

Unternehmen stehen vor der stetigen Herausforderung, ihre Daten und Netzwerke vor immer raffinierteren Angriffen zu schützen. Auch CERT.at trägt nicht nur Verantwortung für die IT-Sicherheit in Österreich, sondern muss ebenso die Sicherheit der eigenen Systeme und Infrastruktur gewährleisten. Der Schutz sensibler Informationen und die Widerstandsfähigkeit der internen IT-Umgebung sind essenzielle Voraussetzungen für eine effektive und vertrauenswürdige Arbeit.

Ein wichtiger Qualitätsnachweis in diesem Bereich ist die Zertifizierung nach ISO 27001:2013. Dieses international anerkannte Zertifikat bestätigt, dass ein Unternehmen IT-Sicherheit umfassend und systematisch verwaltet. Es umfasst nicht nur die technische Sicherheit und den Schutz physischer Infrastrukturen, sondern auch organisatorische Prozesse und Maßnahmen zur Risikominimierung. Die ISO 27001-Zertifizierung dient als sichtbares Gütesiegel nach außen und gleichzeitig als kontinuierlicher Ansporn zur Optimierung der eigenen Sicherheitsstandards. Um diesen hohen Standard aufrechtzuerhalten, unterziehen sich CERT.at und das Mutterunternehmen nic.at jährlich externen Audits, die sicherstellen, dass alle Anforderungen konsequent erfüllt werden.

Die Zertifizierung hat bei nic.at, der österreichischen Domain-Registrierungsstelle, bereits eine lange Tradition: Schon 2014 wurde das Unternehmen nach ISO 27001 zertifiziert. Beim ersten großen Re-Audit von nic.at drei Jahre später fiel die Entscheidung, auch für CERT.at (inklusive der für GovCERT Austria betriebenen Services) eine Zertifizierung anzustreben.

Nach einer intensiven Vorbereitungsphase und der Umsetzung aller notwendigen Sicherheitsmaßnahmen wurde CERT.at schließlich 2017 erfolgreich nach ISO 27001 zertifiziert. Diese Zertifizierung bestätigt nicht nur die Einhaltung höchster Sicherheitsstandards, sondern stärkt auch das Vertrauen von Partnern, Unternehmen und staatlichen Stellen in die Arbeit von CERT.at. Im Jahr 2024 wurde die Zertifizierung im Zuge eines Re-Audits erneut bestätigt – ein Beleg dafür, dass IT-Sicherheit hier nicht als einmaliges Projekt, sondern als fortlaufender Prozess verstanden wird.

1.4.2 TI Zertifizierung

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

Im Jahr 2017 hat CERT.at den Schritt von der TI-Akkreditierung hin zur Zertifizierung gemacht. Dieser Prozess, der durch das TF-CSIRT-Netzwerk und damit die Branche selbst durchgeführt wird, überprüft die Organisation, die internen Sicherheitsmaßnahmen und Arbeitsprozesse des betroffenen CERTs anhand des international anerkannten SIM3 Reifegradmodells. CERT.at konnte diesen Prozess erfolgreich abschließen und ist (mit Stand 2024) eines von 11 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 “accredited” geführt.

Kapitel 2

Das IT-Sicherheitsjahr 2024

CERT.at fungiert als Informationsdrehscheibe für alle Cybersicherheits-Themen in Österreich, ist also Ansprechpartner für sämtliche Sicherheitsprobleme von IKT-Geräten unter österreichischen IP-Adressen oder der Domäne ".at". Umgekehrt informiert CERT.at proaktiv Organisationen, die von Schwachstellen oder Cyberangriffen betroffen sind, bei Bedarf und Möglichkeit direkt oder über die Internet Service Provider (ISP) von diesen Bedrohungen.

Die dazu notwendigen Informationen stellt CERT.at aus einer Vielzahl an Informationsquellen zusammen, die wiederum zu einem großen Teil von der nationalen und internationalen Cybersecurity-Community erstellt und CERT.at zu Verfügung gestellt werden. Zusätzlich scannt CERT.at den österreichischen Adressraum bei Bedarf aktiv nach betroffenen Systemen, analysiert Schadsoftware und nimmt an Fachkonferenzen und in internationalen Gremien teil, um eine laufende Lagebeurteilung durchführen zu können.

Und nicht zuletzt wird über Community-Veranstaltungen wie den IT-Security-Stammtisch und den Austrian Trust Circle Information über aktuelle Trends und Angriffsmuster ausgetauscht, die ebenfalls (meistens anonymisiert) in das Lagebild einfließen kann.

Aus all diesen technischen und nicht-technischen Informationen entsteht der tägliche Blick auf das das "Cybersecurity-Österreich". Im Folgenden wird beschrieben, wie diese Informationen gesammelt und ausgewertet wurden und was sie über die IT-Sicherheitsjahr 2024 aussagen.

2.1 NIS Meldungen

Das NIS Gesetz von Ende 2018 sieht vor, dass freiwillige Meldungen und Pflichtmeldungen an die jeweils zuständigen Computer-Notfallteams übermittelt werden. CERT.at wurde am 20. März 2019 per Bescheid die Rolle des "nationalen Computer-Notfallteams" zugewiesen, seit diesem Tag ist auch das Meldeportal unter https://nis.cert.at/ online.

2024 sind in Summe 23 Pflichtmeldungen und 47 freiwillige Meldungen eingegangen,

Pflichtmeldungen sind im NISG laut §19 für "Betreiber wesentlicher Dienste" und laut §21 für "Anbieter digitaler Dienste" dann verpflichtend, wenn es zu einem Sicherheitsvorfall gekommen

ist. Einen solchen definiert das Gesetz als ”eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat”.

Die Schranke für eine freiwillige Meldung (§23 NISG) ist deutlich niedriger: einerseits reichen schon ”Risiken” und ”Vorfälle” bei Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste, um eine solche Meldung abzugeben, andererseits dürfen auch Einrichtungen, die keiner Meldepflicht unterliegen, Vorfälle und Risiken aus ihrem Bereich melden. Im Gegensatz zu Pflichtmeldungen können freiwillige Meldungen anonym erfolgen und CERT.at kann diese Meldung aggregiert an das Innenministerium zur Verbesserung des Lagebildes weiterleiten.

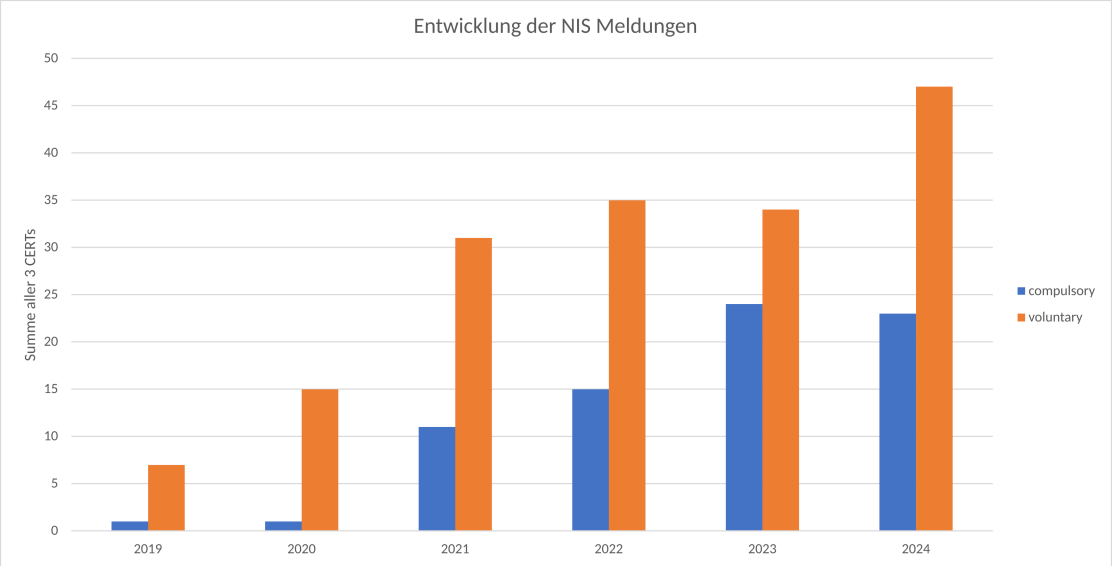


Abbildung 2.1: Entwicklung der NIS Meldungen seit 2019

Die Zahl der Meldungen liegt seit Inkrafttreten von NISG leider unter den Erwartungen. Insbesondere bei den freiwilligen Meldungen bestand die Hoffnung, dass diese die Grundlage für das nationale Lagebild zur Cybersicherheit in Österreich bilden werden. Aufgrund der geringen Anzahl an Meldungen liefert diese Informationsquelle keine ausreichende Datenbasis, um statistisch fundierte Aussagen treffen zu können.

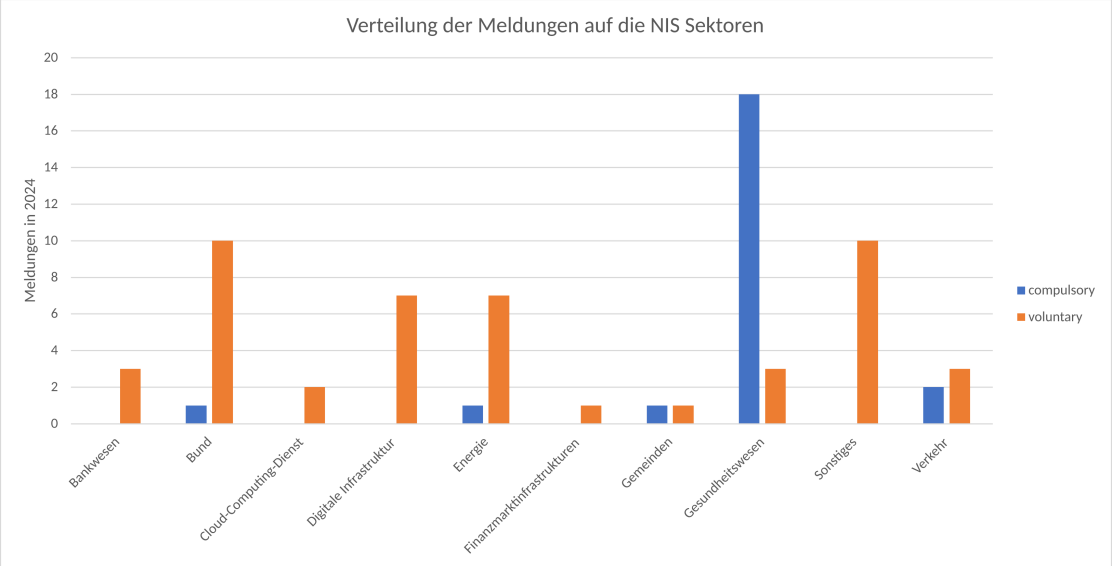


Abbildung 2.2: NIS Meldungen 2024: Sektorenverteilung

Wichtig ist auch der Hinweis, dass ein Ausfall eines IT-Systems, von dem ein Dienst abhängt, zu einer Meldepflicht führen kann – unabhängig von der Ursache. Daher sagt die Zahl der Pflichtmeldungen wenig über ”Cyberangriffe auf die kritische Infrastruktur” aus. Das wird noch deutlicher, wenn man berücksichtigt, dass die meisten dieser Meldungen bisher auf normale ”IT-Gebrechen” wie Hardwareausfälle, Softwareprobleme oder menschliche Fehler zurückzuführen waren.

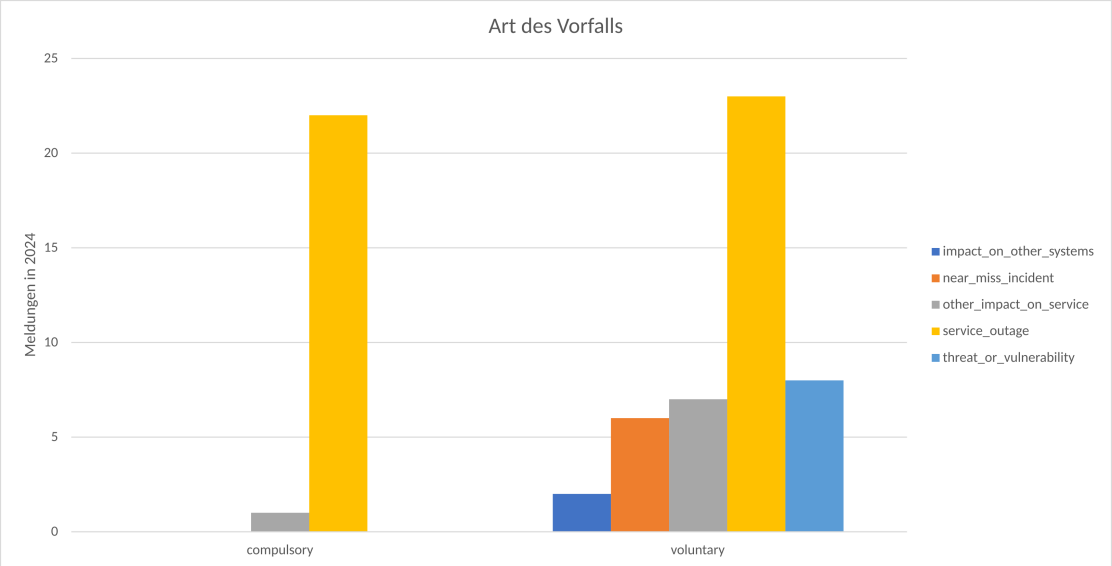


Abbildung 2.3: NIS Meldungen 2024: Art des Vorfalls

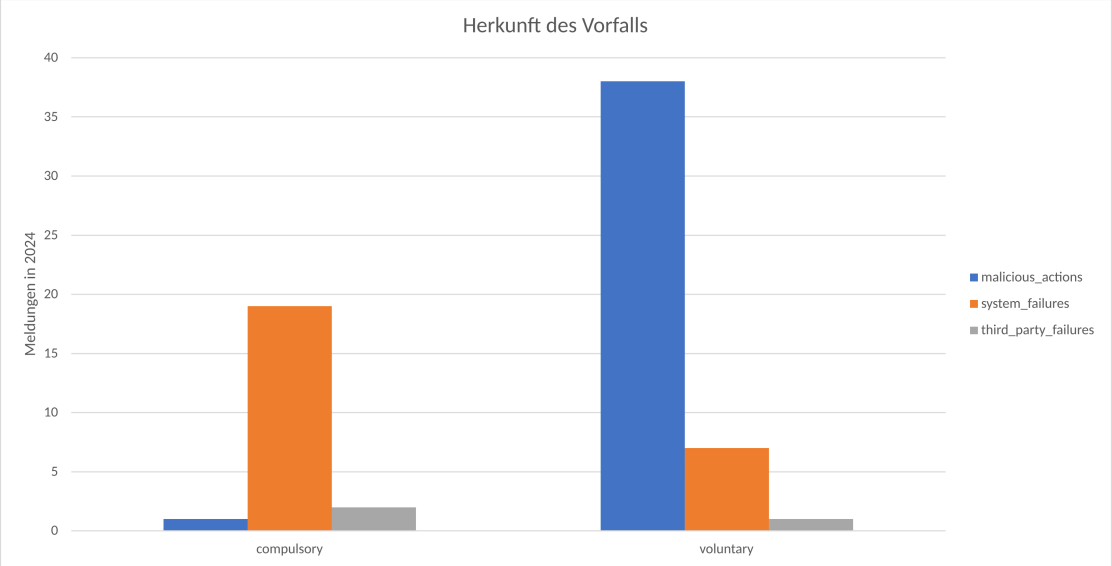


Abbildung 2.4: NIS Meldungen 2024: Herkunft des Vorfalls

2.2 Incident Reports, Incidents und Investigations

Eingehende und ausgehende Informationen werden bei CERT.at und GovCERT Austria über (voneinander getrennte) Ticketsysteme abgehandelt. Dabei wird bei Vorfällen zwischen Incident Reports, Incidents und Investigations unterschieden:

Incident Reports sind Meldungen über Sicherheitsprobleme oder -vorfälle, die bei CERT.at eingehen. Diese werden anschließend als relevant, informativ oder als Fehlalarm kategorisiert. Als "informativ" sieht CERT.at Meldungen an, bei denen eine Weiterverarbeitung aufgrund verschiedener Faktoren nicht sinnvoll ist; beispielsweise Hinweise auf Opfer von bereits geschehenen DDoS Angriffen. Hier ist es nicht hilfreich, die Betroffenen über vergangene Attacken zu informieren, die sie aller Wahrscheinlichkeit nach ohnehin bemerkt haben.

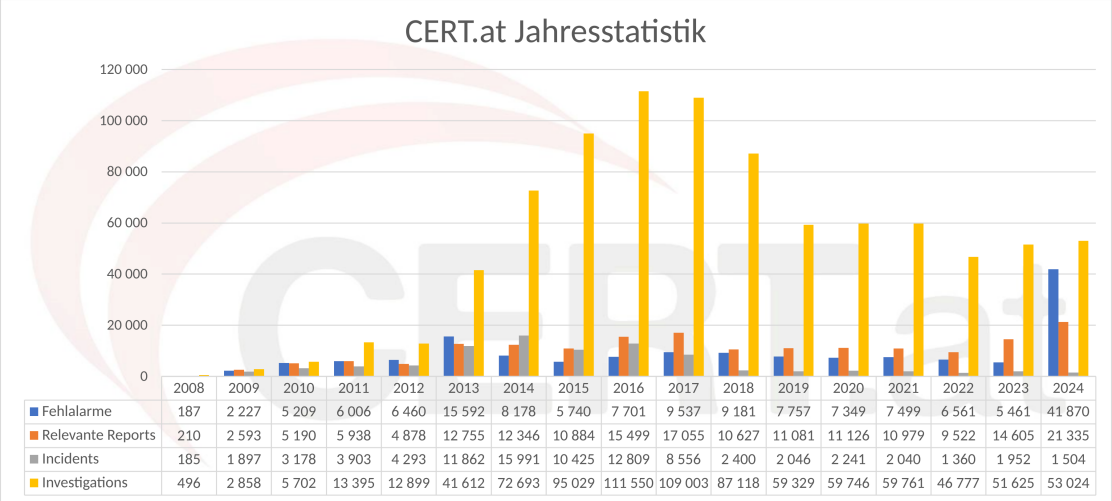
Incident Reports können sowohl von automatisierten Datenfeeds (siehe 2.5 Datenbasis) als auch von Privatpersonen stammen. Sie werden grundsätzlich vertraulich behandelt und können auch per PGP-verschlüsselte E-Mail übermittelt werden.[1]

Incidents werden aus Incident Reports generiert, die CERT.at als relevant eingestuft hat und denen daher nachgegangen wird.

Investigations schließlich meinen die Kontaktaufnahme von CERT.at mit Betroffenen. Auch diese Kontaktaufnahme kann automatisiert, wie im Falle von ISPs (Internet Service Providern), oder persönlich, wie bei einer Responsible Disclosure, erfolgen.

2016 wurde damit begonnen, die Abwicklung der Vorfallsbehandlung – wo immer möglich – zu automatisieren. Dieser Vorgang wurde Ende 2017 abgeschlossen, was es CERT.at ermöglicht,

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



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Fehlalarme	187	2 227	5 209	6 006	6 460	15 592	8 178	5 740	7 701	9 537	9 181	7 757	7 349	7 499	6 561	5 461	41 870
Relevante Reports	210	2 593	5 190	5 938	4 878	12 755	12 346	10 884	15 499	17 055	10 627	11 081	11 126	10 979	9 522	14 605	21 335
Incidents	185	1 897	3 178	3 903	4 293	11 862	15 991	10 425	12 809	8 556	2 400	2 046	2 241	2 040	1 360	1 952	1 504
Investigations	496	2 858	5 702	13 395	12 899	41 612	72 693	95 029	111 550	109 003	87 118	59 329	59 746	59 761	46 777	51 625	53 024

Abbildung 2.5: Incident Reports, Incidents und Investigations im Überblick

sich stärker auf Meldungen von Privatpersonen oder auch Firmen zu konzentrieren, anstatt täglich automatisierte Feeds manuell zu überprüfen. Eine weitere Folge dieses Umstands ist, dass Reports aus mehreren Datenquellen zuerst zusammengefasst, in ein einheitliches Format gebracht und danach gesammelt an Betroffene gesendet werden.

Diese Automatisierung geschieht mithilfe des Open Source Tools IntelMQ, das unter der Leitung von CERT.at von mehreren europäischen CERTs/CSIRTs entwickelt wurde und weiterentwickelt wird. Für nähere Informationen zur Software, siehe 2.6.1 IntelMQ.

Bei den Incident Reports und den Investigations überwiegt die Kategorie “vulnerable” bei weitem, während die Aufteilung bei den Incidents insgesamt wesentlich gleichmäßiger ist. Darin spiegelt sich die Tatsache wider, dass zu einem Incident mehrere Incident Reports und mehrere Investigations gehören können. Wenn es also in einem Monat ähnlich viele Incidents unter den Kategorien “vulnerable” und “malicious code” gibt, sagt dies erst einmal nichts über die Anzahl der zugehörigen Incident Reports und Investigations aus. Dadurch erklärt sich auch der Umstand, dass die Top 5 nicht identisch sind.

Ein Beispiel (mit erfundenen Zahlen): CERT.at erhält an einem Tag aus acht verschiedenen Quellen Incident Reports zu offenen DNS Resolvern (Taxonomie “vulnerable”) und aus einer Quelle Incident Reports zu IP-Adressen, hinter denen von einem bestimmten Trojaner befallene Geräte (Taxonomie “malicious code”) erkannt wurden.

Diese werden dann jeweils unter einem Incident für alle offenen DNS Resolver und einem Incident für alle mit diesem Trojaner infizierten Geräte zusammengefasst. Insgesamt wurden uns 100 offene DNS Resolver gemeldet, die sich auf 20 Netzbetreiber verteilen, was zu 20 Investigations unter diesem Incident der Kategorie “vulnerable” führt, aber nur drei mit dem Trojaner infizierte Geräte, was zu lediglich drei Investigations unter dem Incident der Kategorie “malicious code” führt. So kommen eine ähnliche Anzahl von Incidents, aber sehr unterschiedlich viele Incident Reports und Investigations zustande.

Diese Zahlen repräsentieren entsprechend der Definitionen oben also die Anzahl der ein- und ausgehenden E-Mails von CERT.at. Auf die dahinterliegenden Daten, die die IT-Sicherheitslage in Österreich beschreiben wird in 2.5 Datenbasis näher eingegangen.

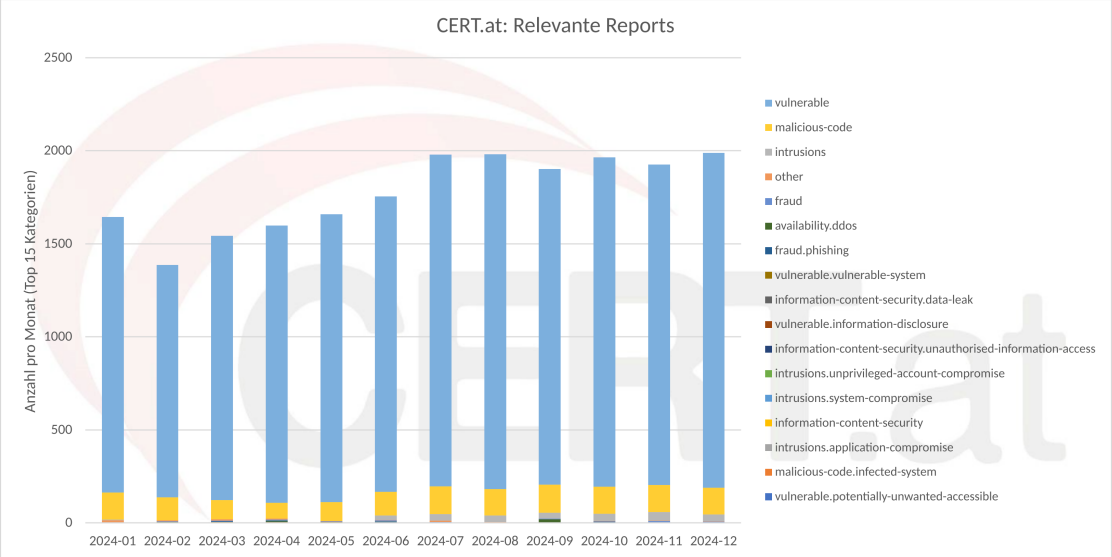


Abbildung 2.6: Incident Reports

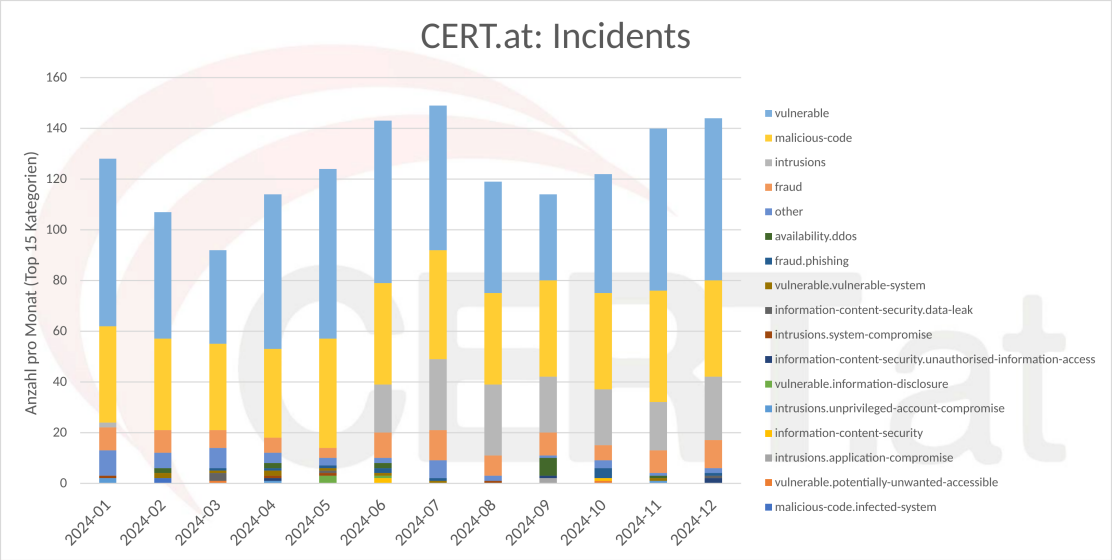


Abbildung 2.7: Incidents

2.3 Taxonomie

Um einen schnellen Informationsfluss innerhalb der IT-Sicherheits-Community gewährleisten zu können, braucht es eine gemeinsame Sprache. CERTs/CSIRTs, Strafverfolgungsbehörden, Sicherheitsfirmen und Sicherheitsforscher:innen müssen sich auf gemeinsame Richtlinien zum Austausch von Informationen einigen, um im Notfall schnell eingreifen zu können. Auch eine automatisierte Verarbeitung von Reports ist nur möglich, wenn sich alle einer einheitlichen Sprache bedienen.

Die Taxonomie, auf die sich CERT.at stützt, ist die ”Reference Security Incident Taxonomy”, die auf der älteren eCSIRT II Taxonomy (PDF) basiert. Die Kategorien dieser Taxonomie sind nicht

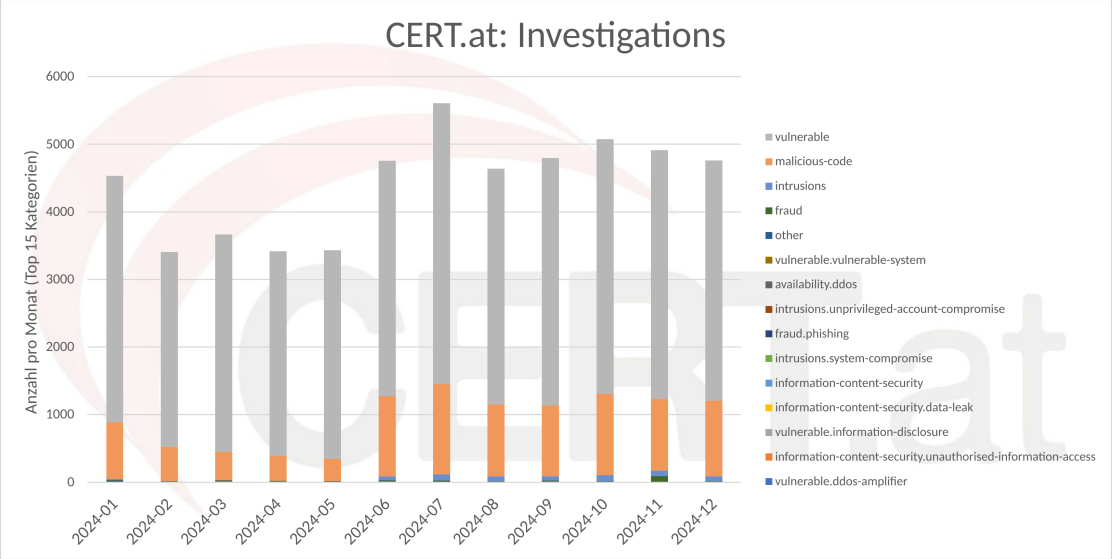


Abbildung 2.8: Investigations

exklusiv, d.h. mehrere Kategorien können auf einen Vorfall zutreffen.

Die Reference Security Incident Classification Taxonomy wird von einer eigenen Arbeitsgruppe der TF-CSIRT kontinuierlich weiterentwickelt, vgl. Reference Security Incident Taxonomy. Die aktuelle Version wird in einem lebenden Dokument auf GitHub veröffentlicht.

2.3.1 Reference Security Incident Taxonomy – ein kurzer Überblick

Abusive Content: Darunter fallen z.B. Spam, Hate-Speech, gewaltverherrlichende oder auch Child Sexual Abuse Material (CSAM).

Malicious Code: Gemeint sind dabei einerseits Computer, die Schadsoftware oder deren Konfiguration hosten bzw. als Command and Control Server fungieren und andererseits von Schadsoftware befallene Systeme.

Information Gathering: In dieser Kategorie finden sich neben rein technischen Vorgängen, wie dem Scannen nach Geräten, die für eine bestimmte Lücke anfällig sind, auch Social Engineering. Dabei wird versucht, über menschliche “Schwachstellen” an Informationen zu gelangen (z.B. per ”Phishing”).

Intrusion Attempts: Bei einem Versuch, in ein System einzudringen, können unterschiedliche Methoden angewandt werden, wie z.B. das Ausprobieren von Passwörter oder das Ausnützen bekannter oder noch nicht öffentlich bekannter Schwachstellen (”Zero-Days”).

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

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

Information Content Security: Hierunter fallen nicht authorisierte Zugriffe und Änderungen an Daten sowie Datenverlust. Wiederum gibt es unterschiedlichste Wege, wie so etwas zustande kommt, unter anderem durch gestohlene Zugangsdaten, fehlende Zugriffsbeschränkungen, kaputte Hardware, etc.

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

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

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

Test: Für Testfälle.

2.4 2024 im Detail

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

Im Verhältnis zu den Aussendungen ist zweierlei zu beachten:

1. CERT.at schickt Informationen zum gleichen Problem nur alle 30 Tage aus. Das heißt also, auch wenn wir z.B. jeden Tag die Information erhalten, dass auf IP Adresse X Port Y offen ist, obwohl er das wahrscheinlich nicht sein sollte, schicken wir das nicht täglich weiter, um die Betreiber/ISPs nicht mit Benachrichtigungen zu überfluten. Diese Deduplikation wurde in den Rohdaten noch nicht vorgenommen.

2. Gibt es in einem Netzwerk mehrere Fälle desselben Problems (z.B. Geräte, die für die gleiche Schwachstelle anfällig sind), leiten wir diese Informationen aggregiert an die Verantwortlichen weiter, d.h. hinter einer einzelnen Investigation können zahlreiche Datenbankeinträge a.k.a. “Events” stecken.

[2] Für eine genauere Beschreibung siehe 2.5 Datenbasis.

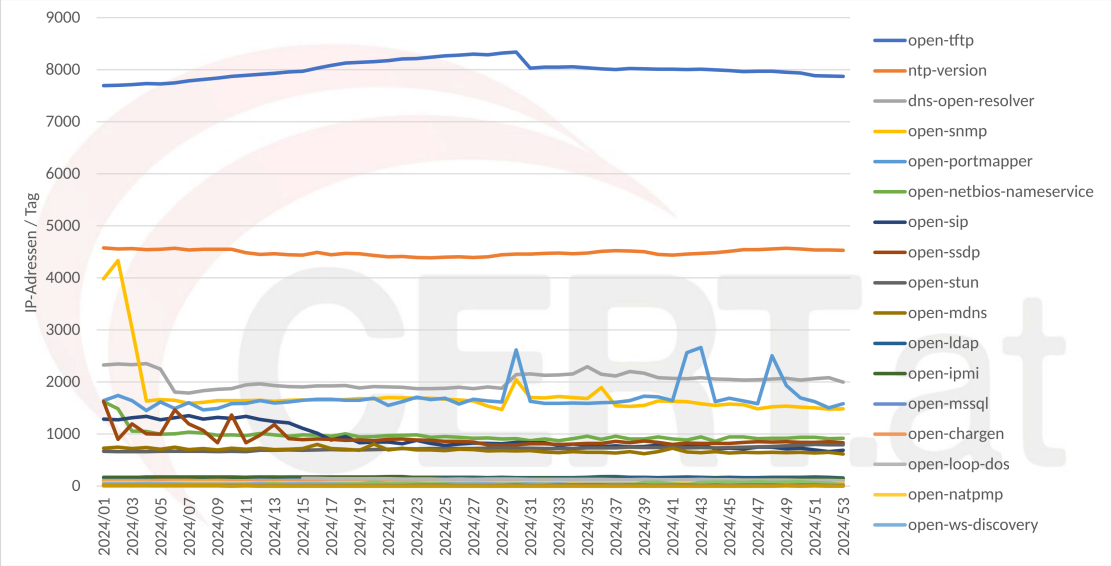


Abbildung 2.9: Events nach Taxonomie (logarithmische Skala)

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

2.4.1 Taxonomie “vulnerable”

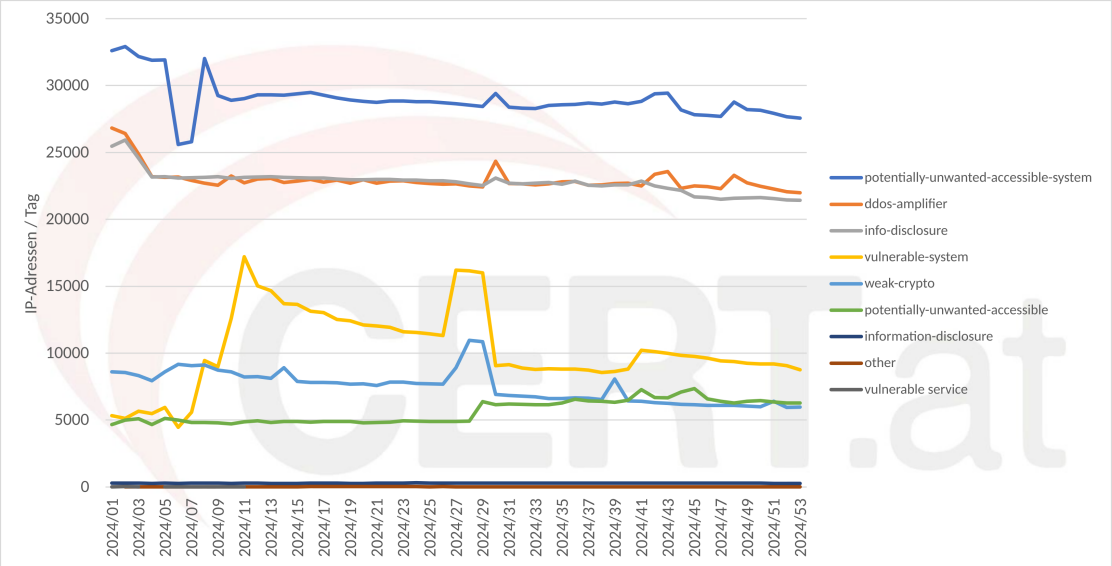


Abbildung 2.10: Alle Events der Taxonomie “vulnerable”

CWMP, RDP, Telnet, Portmapper und Netbios-Nameservice sind die Protokolle, die am häufigsten offen aus dem Internet erreichbar sind, obwohl es gute Gründe dafür gibt, sie besser abzu-

sichern. So sind etwa Fernwartungszugänge direkt per RDP oft ein Faktor bei Ransomwarevorfällen. (Abb. 2.11)

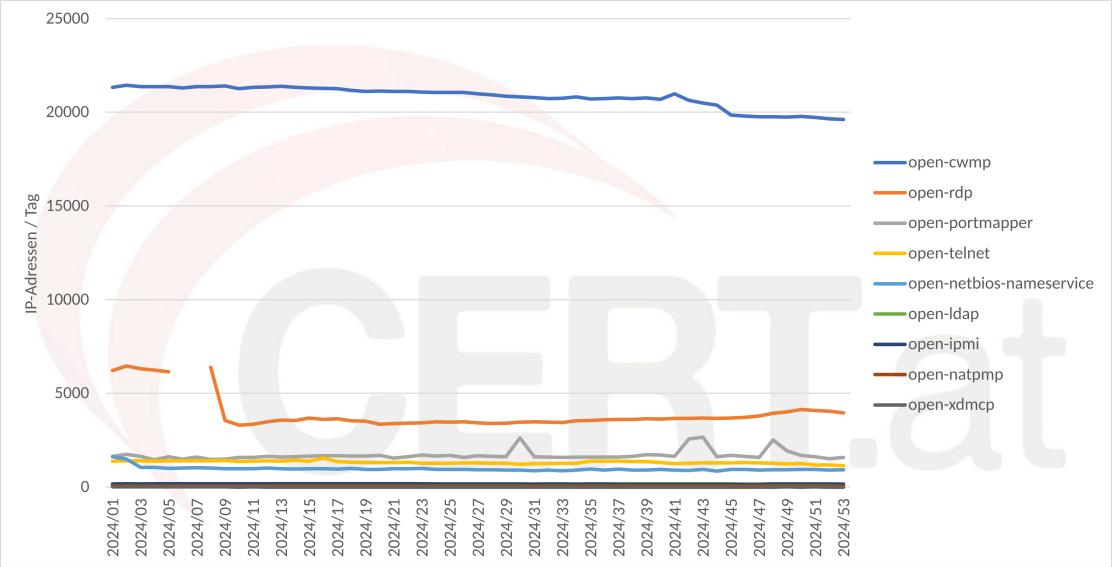


Abbildung 2.11: Ports, die nicht öffentlich erreichbar sein sollten

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

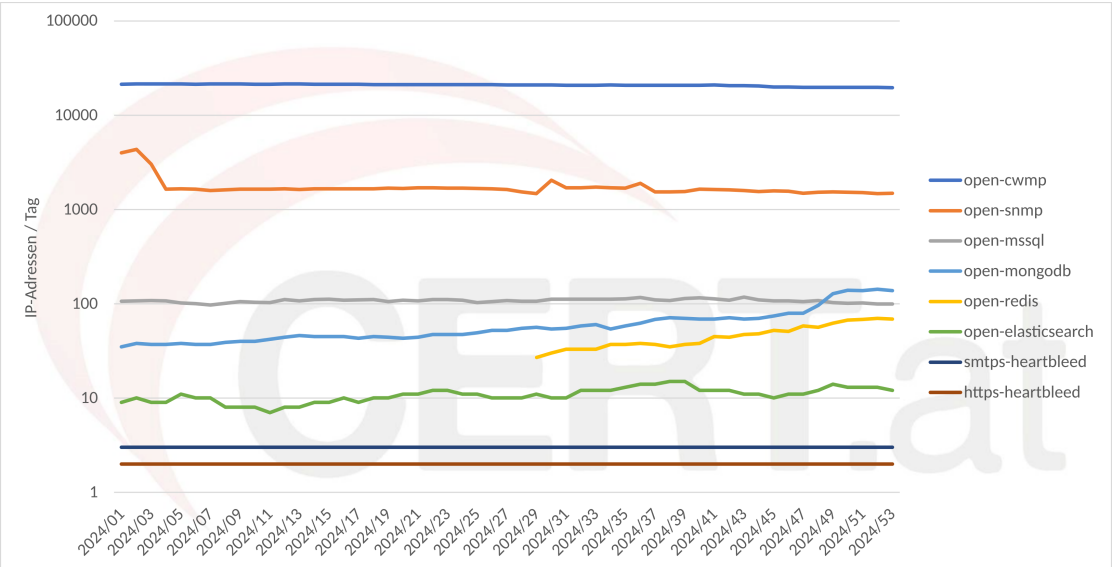


Abbildung 2.12: Services, über die sensible Informationen gewonnen werden können

”Verwundbar” kann aber auch heißen, dass der Computer anfällig dafür ist, sich für Angriffe auf Dritte einspannen zu lassen. Mit Hilfe solcher Reflektoren/Verstärker können Tätergruppen starke DDoS-Angriffe starten, die etwa für Erpressungsversuche (siehe 2.8 Hilfe bei Vorfällen) benutzt werden. (Abb. 2.13)

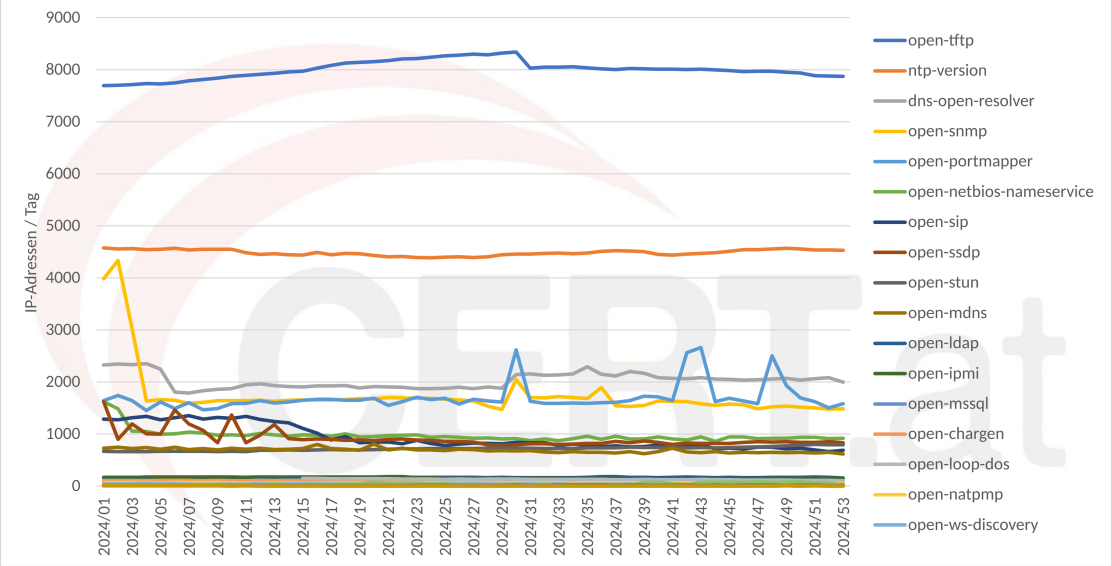


Abbildung 2.13: Geräte, die für UDP DDoS Amplifikation missbraucht werden können

Wie auch in den Jahren zuvor, fiel 2024 der größte Teil der von uns behandelten Meldungen in die Kategorie “vulnerable”, weshalb wir sie etwas näher vorstellen.

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

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

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

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

Shodan “Verified Vulnerabilities”

Im Jahr 2020 veröffentlichte die Suchmaschine Shodan ein neues Feature zur Schwachstellenanalyse. Diese “Verified Vulnerabilities” zeigen ihrem Namen nach entsprechend Schwachstellen an, die Shodan gefunden und verifiziert hat.[3] Diese Funktionalität ist nur für eine begrenzte

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

Anzahl von IP Adressen anwendbar; im Falle von CERT.at sind das all jene, die in Österreich geolokalisiert sind. Diese Informationen werden automatisiert an ausgesuchte Netzverantwortliche geschickt, um diese bei der Erhaltung der ”Netzhygiene” zu unterstützen.

2.4.2 Veraltete Kryptographie

Verschlüsselung bei Web- und E-Mail-Servern ist heutzutage erfreulicherweise weit verbreitet. Allerdings werden immer wieder Schwachstellen in kryptographischen Verfahren gefunden, die eine Aktualisierung der betroffenen Server notwendig machen. Das geschieht leider nicht immer sofort und zieht sich meist über viele Jahre oder sogar Jahrzehnte, bis es keine verwundbaren Server mehr gibt.

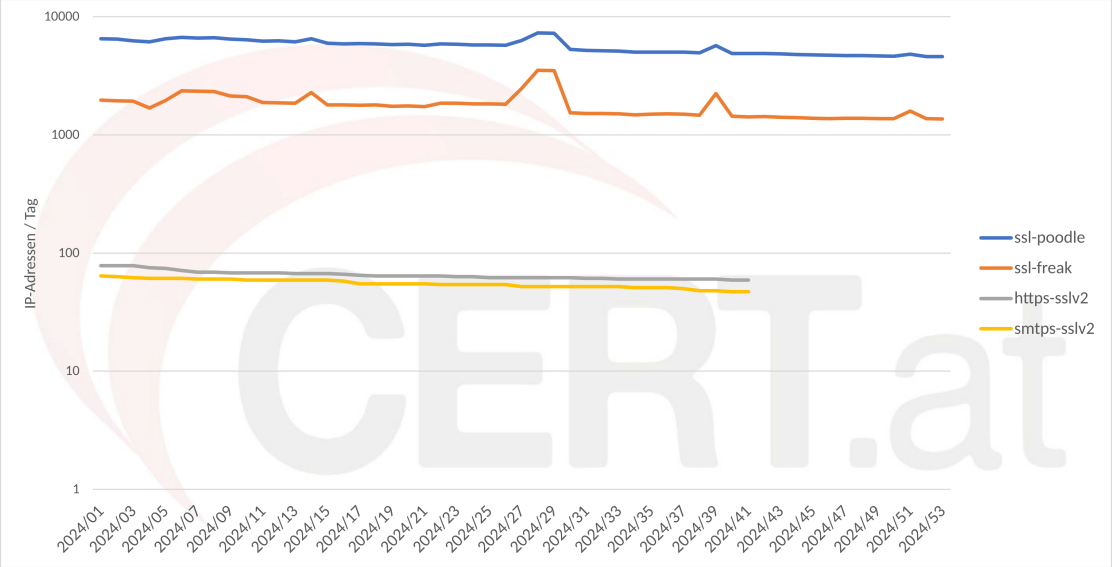


Abbildung 2.14: Unsichere Kryptographie

2.4.3 Malware

Im Jahr 2024 blieb Malware ein zentrales Thema im Bereich der Cybersicherheit. Trotz verbesserter Schutzmechanismen und verstärkter Sensibilisierung haben Cyberkriminelle ihre Methoden weiterentwickelt, insbesondere durch den Einsatz von Künstlicher Intelligenz zur Automatisierung und Tarnung von Angriffen.

Ransomware blieb eine der größten Bedrohungen, wobei gezielte Angriffe auf Krankenhäuser, Bildungseinrichtungen und Versorgungsunternehmen weltweit zunahmen. Neben den finanziellen Schäden standen zunehmend auch die Gefährdung menschlicher Sicherheit und die Unterbrechung kritischer Dienstleistungen im Fokus.

Dennoch gab es auch 2024 bedeutende Erfolge im Kampf gegen Malware: Internationale Ermittlungen führten zur Zerschlagung mehrerer Hackergruppen. Zudem konnten wichtige Command-and-Control-Server ausgeschaltet und gestohlene Daten sichergestellt werden.

2.4.4 Warnings

Im Falle schwerwiegender Sicherheitslücken veröffentlicht CERT.at Warnungen, um Betroffene schnellstmöglich zu informieren. Grundsätzlich müssen für eine Warnung folgende Kriterien erfüllt sein:

1. Die Lücke ist leicht ausnutzbar
2. Die Betroffenen sind sehr zahlreich, z.B. Schwachstellen in Webbrowsern und/oder bieten wichtige Dienste für viele andere an, z.B. Schwachstellen in Mail-Servern
3. Es gibt bereits Updates oder Workarounds, um das Problem zu beheben

Im Einzelfall können auch nur einzelne dieser Voraussetzungen erfüllt sein, wenn dies sinnvoll erscheint. CERT.at Warnungen können alternativ auch als (Feed) bzw. (E-Mail-Abo) bezogen werden.

Im Folgenden werden die Warnungen, die 2024 ausgesendet wurden, aufgelistet. Detailbeschreibungen finden sich auf der CERT.at-Website.

- 11. Jänner 2024: Kritische Sicherheitslücken in Ivanti Connect Secure und Ivanti Policy Secure - aktiv ausgenützt - Patches verfügbar
- 9. Februar 2024: Kritische Sicherheitslücken in Fortinet FortiOS, Updates verfügbar
- 29. März 2024: Kritische Sicherheitslücke/Hintertüre in xz-utils (CVE-2024-3094)
- 12. April 2024: Kritische Sicherheitslücke in Palo Alto PAN-OS (Global Protect) aktiv ausgenützt - Patches verfügbar
- 2. Mai 2024: Kritische Sicherheitslücken in ArubaOS - Updates verfügbar
- 29. Mai 2024: Sicherheitslücke in Check Point Network Security Gateways (Mobile Access) - Fix verfügbar
- 30. Juli 2024: Kritische Sicherheitslücke in VMware ESXi - aktiv ausgenutzt - Update verfügbar
- 24. Oktober 2024: Kritische Zero-Day Schwachstelle in FortiManager wird aktiv ausgenutzt - Update verfügbar
- 15. November 2024: Kritische Sicherheitslücke in Laravel Framework - Updates verfügbar

2.4.5 Aktuelles

Wenn wir auf einen Artikel, ein Advisory, einen Exploit, etc. stoßen, von dem wir denken, dass es möglichst schnell bekanntgemacht werden sollte, verfassen wir einen Anreißertext und veröffentlichen es hier. Das können z.B. Updates zu aktuell laufenden Malware-Kampagnen sein, bei denen schnelle Reaktion wichtig ist.

Aktuelles von CERT.at kann alternativ auch als (Feed) bezogen werden.

Im Folgenden werden die Nachrichten, die 2024 als ”Aktuelles” ausgesendet wurden, aufgelistet. Detailbeschreibungen finden sich auf der CERT.at-Website.

- 25. Jänner 2024: Potentielle Remote Code Execution in Jenkins - Patch verfügbar
- 3. Februar 2024: Sicherheitsvorfall bei der AnyDesk Software GmbH
- 7. Februar 2024: Kritische Sicherheitslücke in JetBrains TeamCity On-Premises
- 7. Februar 2024: Vermehrte Ransomware-Angriffe mit Lockbit 3.0
- 9. Februar 2024: Neue Security Advisories für Ivanti Connect Secure und Policy Secure und SonicWall SonicOS SSL-VPN
- 22. Februar 2024: Angriffe gegen ConnectWise ScreenConnect
- 23. Februar 2024: Weitere Informationen zu Angriffen gegen ConnectWise ScreenConnect
- 18. März 2024: Kritische Sicherheitslücke CVE-2024-21762 in Fortinet FortiOS wird aktiv ausgenutzt
- 28. März 2024: Pre-Ransomware Aktivität: Schadakteure nutzen CitrixBleed (CVE-2023-4966) noch immer und verstärkt für Initialzugriff
- 3. April 2024: Farbpatronen für den Keksdieb
- 10. April 2024: Verzögerte Aussendung der CERT.at-Tagesberichte
- 16. April 2024: Schwere Sicherheitslücke in PuTTY - CVE-2024-31497
- 7. Juni 2024: Sicherheitslücke (CVE-2024-4577) für Remote-Code Ausführung in PHP-CGI / XAMPP entdeckt
- 13. Juni 2024: Microsoft Patchday Juni 2024 - CVE-2024-30080, CVE-2024-30078
- 26. Juni 2024: Supply-Chain-Angriff gegen polyfill.js
- 28. Juni 2024: Akute Welle an DDoS-Angriffen gegen österreichische Unternehmen und Organisationen
- 28. Juni 2024: Sicherheitsvorfall beim Hersteller der Fernwartungslösung TeamViewer
- 1. Juli 2024: regreSSHion: Remote Unauthenticated Code Execution Vulnerability (CVE-2024-6387) in OpenSSH server
- 3. Juli 2024: MikroTik Router als DDoS Quellen: Zahlen für Österreich
- 18. Juli 2024: Schwerwiegende Sicherheitslücke in Cisco Secure Email Gateway
- 19. Juli 2024: CrowdStrike Agent erzeugt Bluescreen of Death (BSOD) Dauer-Schleife auf Windows Systemen - Fehlerhaftes Update für Falcon Sensor

- 14. August 2024: Microsoft Patchday August 2024 - mehrere aktiv ausgenutzte Schwachstellen
- 14. August 2024: Mehrere schwerwiegende Sicherheitslücken in Ivanti-Produkten - Updates verfügbar
- 14. August 2024: Versuchte Leistungserschleichung bei Sicherheitsunternehmen
- 6. September 2024: Sicherheitslücken in Veeam Backup und Replication - Updates verfügbar
- 6. September 2024: Aktive Ausnutzung einer Sicherheitslücke in SonicWall SonicOS (CVE-2024-40766)
- 16. September 2024: Akute Welle an DDoS-Angriffen gegen österreichische Unternehmen und Organisationen
- 2. Oktober 2024: Aktive Ausnutzung einer Sicherheitslücke in Zimbra Mail Server (CVE-2024-45519)
- 22. Oktober 2024: Auch ein .rdp File kann gefährlich sein
- 25. Oktober 2024: Denial of Service in Cisco ASA und FTD und weitere Cisco Advisories
- 11. November 2024: Zugangsdaten aus 2023 für Zugriff ausgenutzt - ”Helldown Leaks”-Ransomware kompromittiert Unternehmen über Zyxel-Firewalls
- 12. November 2024: Sicherheitslücken in Citrix Virtual Apps and Desktops
- 18. November 2024: Akute Welle an DDoS-Angriffen gegen österreichische Unternehmen und Organisationen
- 10. Dezember 2024: Stark gestiegenes Aufkommen an Microsoft Remote Desktop Protokoll (RDP) Scanning
- 13. Dezember 2024: Social Engineering nach Mailbombing

2.4.6 Weitere Informationsangebote

Neben den ”Warnings” und den Aussendungen zu ”Aktuelles” können die Tagesberichte (”Dailies”), Blog-Artikel der CERT-Mitarbeiter:innen sowie Berichte zu Speziellen Themen über die CERT-Website abgerufen werden:

- Tagesberichte
- Blogartikel
- Spezielles

2.5 Datenbasis

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

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

2.5.1 Eigene Erhebungen

Scanning Tools

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

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

bei den gescannten Systemen und können daher von diesen eindeutig erkannt werden. Die Liste der aktuellen Scans findet sich auf der CERT-Website (cert.at). Der Suchbereich beschränkt sich hierbei üblicherweise auf IP-Ranges mit Bezug zu Österreich oder auf .at-Domains.

Ablauf eines Scans Der Ablauf eines Scans stellt sich gewöhnlich folgendermaßen dar:

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

2024 führte CERT.at folgende Scans regelmäßig durch:

SSLv2 ist ein 1995 veröffentlichtes Protokoll zur Verschlüsselung von z.B. Web- und E-Mail-Verkehr. Es weist gravierende Schwachstellen auf Protokoll-Ebene auf und sollte daher

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

nicht mehr eingesetzt werden. CERT.at versucht dabei mit allen .at-Domains eine SSLv2 Verbindung für HTTPS und SMTP mit STARTTLS aufzubauen. Ist eine Anfrage erfolgreich, verschickt CERT.at eine Warnung an die Betroffenen.

Heartbleed war ein Fehler in der OpenSSL Bibliothek (CVE-2014-0160), der 2014 veröffentlicht und behoben wurde. Mit diesem Fehler können entfernte AngreiferInnen sensible Daten aus dem Hauptspeicher des Servers (z.B. Passwörter oder Session-Cookies) extrahieren. Leider sind bis heute nicht auf allen Systemen die notwendigen Updates eingespielt worden, es gibt also immer noch verwundbare Server.

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

CVE-2021-34473 besser bekannt als ”ProxyShell”, ist eine Sicherheitslücke, die es Angreifer:innen ermöglich, ohne jegliche Authentifizierung beliebige Befehle als ‘NT Authority\-System‘ über das Netzwerk auszuführen. Innerhalb weniger Tage wurde über Internetweite Scans nach verwundbaren Servern berichtet. CERT.at sucht via Shodan nach potentiell verwundbaren Installationen in Österreich und verifiziert die Ergebnisse mit Hilfe der Logik eines nmap NSE-Scripts eines Researchers. Zusätzlich haben wir alle Geräte, die uns im Zuge der Scans zu CVE-2021-26855 als Exchange Server gemeldet wurden, miteinbezogen.

CVE-2021-26855 wurde Anfang März von Microsoft außerhalb des üblichen Updatezyklus mittels eines Patches behoben. Diese, zu dem Zeitpunkt der Veröffentlichung der Aktualisierung bereits aktiv ausgenutzte, Schwachstelle in Microsoft Exchange Server 2013, 2016 und 2019 ist besser bekannt als ”ProxyLogon”, ermöglicht die Kompromittierung aus dem Internet erreichbarer Systeme.

QNAP NAS Geräte mit Photo Station Im November 2019 veröffentlichte die Firma QNAP Patches für mehrere kritische Schwachstellen in ihren NAS-Geräten. Im Mai 2020 wurde Exploit-Code dazu veröffentlicht. CERT.at hat daher mithilfe der Suchmaschine shodan.io nach potentiell verwundbaren Geräten in Österreich gesucht und die Betroffenen informiert. Selbstverständlich wurde die Lücke dabei nicht ausgenutzt.

CVE-2020-0688 ist eine Schwachstelle in einigen Versionen des Exchange E-Mail-Servers, die es Angreifer:innen ermöglicht, beliebige Befehle mit Administrationsrechten über das Netzwerk auszuführen. Sie benötigen dafür nur Zugangsdaten mit beschränkten Rechten, da es bei der Schwachstelle auch zu einer Privilege-Escalation kommt.

TLS < 1.2 Seit März 2020 haben die führenden Browser (Chrome, Firefox, Safari, Microsoft Edge) die Untersützung für TLS-Versionen niedriger als 1.2 standardmäßig deaktiviert, d.h. seit diesem Zeitpunkt konnten Nutzer:innen Webseiten, die nicht mindestens TLSv1.2 unterstützen, nicht mehr besuchen. CERT.at testet alle öffentlich per HTTPS erreichbaren .at Domänen und in Österreich geolokalisierten IPv4-Adressen und infomiert deren BetreiberInnen, falls ihre Server über gängige Browser nicht mehr erreichbar sind.

Dazu kamen einige einmalige bzw. unregelmäßige Scans. Diese sind auf der oben verlinkten Webseite genauer beschrieben.

2.5.2 Externe Quellen

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

Researcher:innen und NPOs

Es gibt einige Non-Profit Organisationen, die Daten für die IT-Security-Community erheben und dieser gratis zur Verfügung stellen.

Die für CERT.at und GovCERT Austria wichtigste davon ist die Shadowserver Foundation, die überwiegend im Bereich der Analyse von Botnetzen und Malware arbeitet. Dazu wurde ein riesiges Netzwerk aus Honeypots[5] aufgebaut. Die Erkenntnisse daraus liefern wertvolle Analysedaten, um beispielsweise Botnetzen auf die Spur zu kommen und sie auszuschalten. Weiters scannt Shadowserver täglich das Internet nach diversen Kriterien ab: daraus ergeben sich viele der Informationen, die zu unseren Warnungen über verwundbare bzw. missbrauchbare Systeme (siehe Kapitel 2.4.1) führen.

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

Andere CERTs/CSIRTs

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

Kommerzielle IT-Firmen

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

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

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

Suchmaschinen

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

Ermittlungsbehörden

Wenn Ermittlungsbehörden ein Schlag gegen die Internetkriminalität gelingt, sammeln sie oft Daten aus der Beschlagnahmung von Domains oder Servern von Botnetzen.

Dabei werden die ursprünglich von den Angreifern eingesetzten Steuerserver der Botnetze (sog. “Command and Control Server”) durch Sensoren (diese werden “Sinkholes” genannt) ersetzt, die für die Strafverfolgungsbehörden mitprotokollieren, von welchen IP-Adressen infizierte Geräte neue Befehle abholen wollen. Diese ”Botnet drones” befinden sich meistens verteilt über mehrere Länder und daher werden die so erfassten Daten – sofern es der rechtliche Rahmen erlaubt – an die zuständigen nationale CERTs/CSIRTs weitergeleitet, die diese dann wiederum im eigenen Land an die Betroffenen weitergeben können.

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

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

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

2.6 Tooling

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

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

2.6.1 IntelMQ

Das Projekt

Gestartet wurde der Entwicklungsprozess von IntelMQ[7] bei einem Treffen mehrerer CERTs im Jahr 2014. Die damals verfügbaren Softwarelösungen zur Automatisierung und Verarbeitung von Daten im IT-Securitybereich waren zumeist teuer und/oder schwer zu bedienen. Einige Entwickler des portugiesischen CERT und von CERT.at beschlossen daher, selbst ein Tool zu entwickeln, das diese Probleme adressiert, da eine manuelle Bearbeitung aufgrund der (stetig wachsenden) Datenmenge nicht machbar war.

Dementsprechend sollte IntelMQ möglichst einfach zu nutzen und zu administrieren sein sowie problemlos weiterentwickelt und angepasst werden können. Um das zu erreichen, waren und sind Kompatibilität mit und Schnittstellen zu anderen Tools sowie eine Veröffentlichung als Open Source Software unerlässlich. Der Quellcode von IntelMQ findet sich auf GitHub.

Diese Designprinzipien – Ease-of-Use und Kompatibilität – sind bis heute unverändert und maßgeblich für den Erfolg des Programms verantwortlich. Auch die Umsetzung des Ziels, große Datenmengen automatisiert zu verarbeiten, erleichtert die Arbeit von CERTs/CSIRTs enorm. Bei CERT.at werden Dank IntelMQ täglich hunderte E-Mails verschickt, die BetreiberInnen von Internet-Diensten in Österreich auf Probleme in ihren Netzen hinweisen.

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

IntelMQ 2024

Im Jahr 2024 wurden die Entwicklungsarbeiten konsequent weitergeführt und führten zu mehreren Releases, die sowohl Stabilitätsverbesserungen als auch neue Funktionen mit sich brachten. Besonders hervorzuheben sind Erweiterungen zur besseren Integration in bestehende Systemlandschaften sowie Optimierungen der Performance bei hoher Last.

Darüber hinaus lag ein Schwerpunkt auf der weiteren Automatisierung von Abläufen und der Verbesserung der Benutzerfreundlichkeit. Die Dokumentation wurde erneut umfassend überarbeitet, um den Einstieg für neue Nutzer:innen zu erleichtern und die Nutzung bestehender Funktionen transparenter zu gestalten.

Einmalige Aussendungen a.k.a. “One-Shots”

IntelMQ ermöglicht es, über ein Web-Interface sog. “One-Shots” abzuwickeln. Dabei handelt es sich um Aussendungen, die anlassbezogen bei akuten Bedrohungen möglichst schnell alle Betroffenen erreichen müssen.

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

Ein Beispiel wäre die Veröffentlichung eines Exploit zu einer bekannten Sicherheitslücke, zu der es bereits einen Patch gibt: Sind Daten über dafür noch anfällige Geräte in Österreich, z.B. über die Suchmaschine shodan.io verfügbar, können diese in ein CSV-File umgewandelt werden, das dann bequem über das Web-Interface hochgeladen werden kann.

Anschließend muss noch ein Erklärungstext zum vorliegenden Problem inklusive Links zu Workarounds/Updates verfasst werden, um durch IntelMQ automatisch Mails an alle Betroffenen zu verschicken.

Dies ermöglicht CERT.at nicht nur, schnell auf aktuelle, aber einmalige Umstände zu reagieren, sondern eignet sich auch, um neue Feeds zu testen.

2024 wurde diese Funktion 26 Mal genutzt. Ausgesandt wurden unter anderem Informationen zu Sicherheitslücken in Firewalls und anderen Netzwerk-Appliances, gestohlenen Zugangsdaten und durch Angreifer:innen kompromittierte Systeme.

2.6.2 MISP

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

CERT.at und GovCERT Austria betreiben gemeinsam eine MISP-Instanz zu der Teilnehmer:innen aus der Forschung, staatlichen Institutionen und der Wirtschaft Zugriff haben.[9]

Mit wem die Inhalte geteilt werden, wird beim Upload festgelegt – MISP bietet hier eine Vielzahl an Optionen, die von eigens angelegten Gruppen, über eine Einschränkung auf die eigene Organisation bis zur Verbindung mit anderen MISP-Instanzen alles abdecken.

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

Das MISP-Projekt hat eine eigene Webseite, der Code wird in einem GitHub Repository zur Verfügung gestellt. MISP kristallisiert sich immer mehr als wesentliches Informations-Austauschwerkzeug der internationalen Security-Community heraus, weshalb CERT.at für interessierte Partner Schulungen und Unterstützung beim Einsatz anbietet.

2.7 Bedrohungen 2024

Das Gros der Probleme der IT-Sicherheit sind gut bekannt, nur in seltenen Fällen werden von Grund auf neue Angriffsmethoden entwickelt. Dennoch bringen die meisten Jahre einzelne Wei-

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

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

terentwicklungen oder neue Verhaltensweise von Bedrohungsakteuren mit sich, die aus der breiten Masse hervorstechen.

Wie bereits in den vergangenen Jahren nahmen Angreifer:innen auch 2024 wieder vermehrt Systeme und Software ins Visier, welche aufgrund ihrer Aufgabe direkt aus dem Internet erreichbar sein müssen. Dabei nutzten Bedrohungsakteure Schwachstellen in verbreiteten Softwarelösungen von Unternehmen wie beispielsweise Atlassian, Ivanti, Cisco, MOVEit, Citrix, Fortinet, Aruba, Nextcloud oder Microsoft.

Auch geopolitische Ereignisse hatten abseits ihrer geografischen Lage weitreichende Auswirkungen, von denen auch Österreich nicht verschont geblieben ist. Sowohl der anhaltende Angriffskrieg Russlands gegen die Ukraine als auch der Überfall der Hamas auf Israel sorgten dafür, dass österreichische Unternehmen und Institutionen Opfer politisch motivierter Angriffe wurden.

2.7.1 Angriffe gegen Lieferketten

Supply-Chain-Security bezeichnet die Sicherheit der gesamten Lieferkette digitaler Produkte und Dienstleistungen – von der Softwareentwicklung bis zur Auslieferung beim Endnutzer. Im Jahr 2024 ist dieses Thema nicht mehr nur in Fachkreisen, sondern auch in der breiten Öffentlichkeit angekommen, nachdem wiederholt spektakuläre Angriffe bekannt wurden, bei denen Firmen und Behörden über legitime Updates oder Erweiterungen unwissentlich Schadsoftware installierten.

Klassische Beispiele sind Attacken auf Software-Repositories oder Update-Server. Sobald Kriminelle hier eindringen, können sie Manipulationen an weit verbreiteten Programmbestandteilen vornehmen, die in vielen Unternehmen und öffentlichen Einrichtungen im Einsatz sind. Dies ermöglicht es, verdeckt Hintertüren (Backdoors) oder Trojaner zu platzieren. Besonders kritisch sind Attacken auf beliebte Open-Source-Projekte, denn eine einzige kompromittierte Bibliothek kann weltweit hunderte oder tausende Produkte beeinflussen.

Im Jahr 2024 rücken auch Hardware-Lieferketten stärker in den Fokus. Der Einsatz von Bauteilen aus unterschiedlichen Ländern und mit oft undurchsichtigen Lieferketten erhöht das Risiko, dass Komponenten bereits vor Auslieferung manipuliert wurden. Diese Sorge treibt inzwischen nicht nur Unternehmen, sondern auch Politik und Militär um, da die Infrastruktur eines Landes durch versteckte Hardware-Implantate sabotiert oder ausspioniert werden könnte.

Angesichts dieser Gefahren werden verstärkt Sicherheitsstandards und gesetzliche Vorgaben diskutiert. Auf EU-Ebene sind hier u. a. die NIS2-Richtlinie und der Cyber Resilience Act von Bedeutung, welche verpflichtende Sicherheitsmaßnahmen und Dokumentationspflichten für Hersteller und Dienstleister vorsehen. Darüber hinaus gewinnt die Idee eines Software Bill of Materials (SBOM) an Bedeutung: Dabei soll jedes Softwareprodukt eine detaillierte „Zutatenliste“ mitführen, die Auskunft über alle verwendeten Bibliotheken und Versionen gibt. So könnten Unternehmen schneller auf bekannte Schwachstellen in Zulieferkomponenten reagieren.

Zudem etabliert sich in vielen Organisationen ein DevSecOps-Ansatz: Sicherheitsmechanismen werden bereits in die Entwicklungs- und Lieferprozesse integriert, um Manipulationen früh zu erkennen und Risiken zu minimieren. Automatisierte Tests auf Malware, Signaturprüfungen und

fest definierte Vertrauensmodelle zwischen Softwarekomponenten sind Beispiele dafür, wie ein durchgehendes Sicherheitskonzept die Lieferkette schützen kann.

Die große Herausforderung bleibt, dass Supply-Chain-Angriffe zwar vergleichsweise selten sind, aber bei Erfolg verheerende Konsequenzen haben. Sie betreffen nicht nur ein einzelnes Ziel, sondern potenziell eine ganze Reihe von Kunden oder Partnern. 2024 hat einmal mehr gezeigt, wie wichtig transparente Lieferketten und ein Zusammenspiel verschiedener Abwehrstrategien sind, um das Risiko für alle Beteiligten zu reduzieren.

2.7.2 Regulatorische Entwicklungen

Im Jahr 2024 sind wesentliche regulatorische Neuausrichtungen in Kraft getreten oder vorbereitet worden, welche die Cybersicherheit in Europa nachhaltig prägen. Zu den wichtigsten zählen die NIS2-Richtlinie, die Digital Operational Resilience Act (DORA) sowie der Cyber Resilience Act (CRA). Gemeinsam zielen sie darauf ab, das Sicherheitsniveau in kritischen Sektoren zu erhöhen und zugleich die Resilienz digitaler Produkte und Dienstleistungen im Binnenmarkt zu stärke

NIS2-Richtlinie

Die NIS2-Richtlinie baut auf der früheren NIS-Richtlinie (Network and Information Security) auf und zieht nun einen größeren Kreis von Unternehmen und Organisationen in die Pflicht. Während die ursprüngliche NIS-Richtlinie lediglich für „betreiberkritische“ Sektoren galt, deckt die neue Fassung deutlich mehr Branchen ab, darunter öffentliche Verwaltungen, digitale Dienste, Abfallwirtschaft oder Herstellung von Medikamenten. Ziel ist es, ein einheitliches Mindestmaß an Cybersicherheit in möglichst vielen Bereichen zu etablieren, die für das Funktionieren des Gemeinwesens essenziell sind.

Eine wesentliche Neuerung sind verschärfte Meldepflichten. Unternehmen müssen sicherheitsrelevante Vorfälle binnen strenger Fristen melden und können bei Verstößen gegen die Richtlinie mit hohen Bußgeldern rechnen. Darüber hinaus verpflichtet NIS2 alle betroffenen Akteure zu einem Risiko-Management-Ansatz, der präventive Maßnahmen wie Sicherheitsaudits, Mitarbeiterschulungen und Krisenübungen einschließt.

Die Umsetzung dieser Vorgaben auf nationaler Ebene ist noch nicht erfolgt, relevante Stellen arbeiten jedoch bereits mit Hochdruck daran dies zu ändern. Nichtsdestotrotz setzt NIS2 einen europaweit gültigen Rahmen, der die Zusammenarbeit und den Austausch von Informationen verbessern soll.

Digital Operational Resilience Act (DORA)

Der DORA zielt speziell auf den Finanzsektor ab und adressiert Banken, Versicherungen, Zahlungsdienstleister sowie andere Finanzinstitute. Hintergrund ist die zunehmende Vernetzung und Digitalisierung des Finanzwesens, die einerseits Effizienzgewinne bringt, andererseits jedoch erhebliche Risiken birgt, wenn IT-Infrastrukturen Angriffen oder Ausfällen ausgesetzt sind.

Kernanliegen von DORA ist es, die digitale Betriebsresilienz zu erhöhen. Finanzunternehmen müssen sicherstellen, dass sie Ausfälle in ihrer IT-Infrastruktur ohne gravierende Auswirkungen auf den Geschäftsbetrieb überstehen können. Zu diesem Zweck werden Mindeststandards für Business Continuity, Disaster Recovery und Risikoanalysen festgelegt.

Außerdem schreibt DORA vor, dass externe Dienstleister – beispielsweise Cloud-Anbieter – gründlich geprüft und überwacht werden müssen. Auf diese Weise soll eine zu große Abhängigkeit von einzelnen IT-Providern verhindert und die Lieferkettenresilienz gestärkt werden.

Cyber Resilience Act (CRA)

Der Cyber Resilience Act (CRA) weitet die regulatorische Perspektive auf sämtliche vernetzte Produkte aus, also sowohl Hardware als auch Software mit digitalen Funktionen. Hersteller sind verpflichtet, ihre Produkte bereits während der Entwicklung nach dem Security-by-Design-Prinzip abzusichern. Zudem müssen sie für einen definierten Zeitraum Sicherheitsupdates bereitstellen.

Mit dem CRA will die EU-Kommission durchgängige Sicherheitsstandards schaffen, um Manipulationen oder Datenabflüsse über vernetzte Geräte zu verhindern. Angesichts der rasanten Ausbreitung des Internets der Dinge (IoT) und immer anspruchsvollerer Cyberangriffe hat sich gezeigt, dass ein Flickenteppich nationaler Regeln nicht ausreicht. Der CRA sieht deshalb EU-weit einheitliche Vorgaben vor, die bei Zuwiderhandlungen empfindliche Strafen vorsehen können.

Ausblick und Herausforderungen

Gemeinsam zeichnen NIS2, DORA und der Cyber Resilience Act ein neues Regelungsumfeld für IT-Sicherheit in Europa. Während DORA vor allem den Finanzsektor fest im Blick hat und mit NIS2 weitere kritische und wichtige Einrichtungen abgedeckt werden, wird mit dem CRA eine breitere Basis für Cybersicherheit im Binnenmarkt geschaffen.

In der Praxis erfordert dies eine enge Zusammenarbeit zwischen Unternehmen, Behörden und Verbänden sowie erhebliche Investitionen in Technologie, Prozesse und Personal. Gleichzeitig ist zu erwarten, dass die rechtlichen Anforderungen weiter zunehmen werden, da die EU ihre Digitalstrategie kontinuierlich ausbaut und dabei verstärkt die Themen Datenschutz, Resilienz und Verbrauchersicherheit berücksichtigt.

2.7.3 Künstliche Intelligenz

Große Sprachmodelle, auch LLMs (Large Language Models) genannt, haben im Jahr 2024 immer mehr an Bedeutung gewonnen und beeinflussen inzwischen nahezu alle Bereiche der IT-Branche – einschließlich der Cybersicherheit. Ein Grund dafür ist die Fähigkeit dieser Modelle, riesige Datenmengen in kurzer Zeit zu analysieren und verständliche Texte zu generieren. Während das in vielen Unternehmensbereichen nützlich ist (z.B. zur Kundenkommunikation oder für automatisierte Übersetzungen), entstehen in der IT-Sicherheit sowohl Chancen als auch Risiken.

Einerseits können Unternehmen LLMs nutzen, um gezielt Bedrohungen zu erkennen und präventiv abzuwehren. Beispielsweise lassen sich Protokolldaten aus Sicherheitsinfrastrukturen mithilfe sprachbasierter Analysetools schneller und detaillierter auswerten. Verdächtige Muster in Netzwerklogs, E-Mails oder Applikationen können automatisiert erkannt werden, was Security Operations Center (SOC) entlastet und zu einer schnelleren Reaktion führt. Zudem erlauben LLMs die verbesserte Dokumentation von Sicherheitsvorfällen und das rasche Verfassen von technischen Berichten für Entscheidungsträger, was die Zusammenarbeit zwischen IT-Fachleuten und Management erleichtert.

Andererseits eröffnen LLMs Angreifern neue Angriffsmethoden. So können Kriminelle mit vergleichsweise geringem Aufwand täuschend echte Phishing-E-Mails oder Social-Engineering-Kampagnen erstellen. Moderne Modelle analysieren Kontexte, verwenden passgenaue Formulierungen und täuschen damit besser als je zuvor eine vertrauenswürdige Identität vor. Zusätzlich können sie schädlichen Code generieren oder vorhandenen schädlichen Code verbessern, indem sie mögliche Schwachstellen aufzeigen und effizientere Exploits vorschlagen. Dadurch steigt das Niveau der Angriffe spürbar und stellt Unternehmen vor immer raffiniertere Attacken.

Ein weiterer Aspekt ist die Datenverarbeitung: LLMs benötigen zum Training riesige Datenmengen, darunter oft vertrauliche Dokumente. Werden solche Modelle nicht sorgfältig abgesichert, besteht die Gefahr, dass sensible Informationen in falsche Hände gelangen oder von den Modellen ungewollt wieder ausgespuckt werden. Zusätzlich sind sogenannte Prompt-Injection-Angriffe in den Fokus geraten, bei denen Angreifer gezielt versuchen, ein Modell „umzuprogrammieren“, indem sie manipulierte Eingaben verwenden.

Insgesamt hat das Jahr 2024 deutlich gemacht, dass der Umgang mit LLMs verantwortungsvolle Sicherheitsmaßnahmen erfordert. Während sie auf der Verteidigungsseite sehr hilfreich sein können, zeigen erste Angriffe, wie mächtig die Technik auch für die Gegenseite ist. In vielen Unternehmen laufen deshalb bereits Initiativen, um Richtlinien zum Umgang mit LLMs zu entwickeln und sicherzustellen, dass sowohl Datenschutz als auch IT-Sicherheit gewährleistet bleiben. Parallel wird an KI-gestützten Abwehrmechanismen geforscht, um mögliche Gefahren zeitnah zu erkennen und zu neutralisieren.

2.7.4 Angriffe auf kritische Infrastruktur

Unter kritischer Infrastruktur versteht man all jene Einrichtungen und Anlagen, die essenziell für das Funktionieren einer Gesellschaft sind, z. B. die Energieversorgung, das Gesundheitswesen, die Wasserversorgung oder das Finanzsystem. Im Jahr 2024 hat sich der Trend der vergangenen Jahre fortgesetzt: Solche Infrastrukturen standen international vermehrt im Fokus von Cyberangriffen. Gründe dafür sind einerseits die zunehmende Abhängigkeit von digitalisierten Prozessen und andererseits die potenziell große Wirkung eines erfolgreichen Angriffs.

Ein markantes Beispiel aus 2024 ist die gezielte Attacke auf ein europäisches Pipeline-Netzwerk, bei der es Hackern gelang, kurzzeitig die Steuerungs- und Überwachungssysteme lahmzulegen. Auch wenn es zu keiner langfristigen Versorgungsunterbrechung kam, zeigte dieser Vorfall, wie leicht sich Versorgungsengpässe erzeugen lassen und wie verwundbar hochvernetzte Steuerungstechnik sein kann.

Viele dieser Angriffe werden entweder staatlichen Akteuren zugeschrieben oder zumindest von

diesen unterstützt. Häufig dient Cyber-Kriegsführung dazu, politische oder ökonomische Ziele zu erreichen, ohne direkt militärisch eingreifen zu müssen. Durch die Verschleierung im Cyberspace ist eine eindeutige Attribution jedoch oft schwierig – das heißt, es ist nicht immer klar, wer tatsächlich hinter einem Angriff steckt.

Ein weiterer Aspekt ist die zunehmende Vernetzung und Digitalisierung im Rahmen von Smart-City-Konzepten oder Industrie-4.0-Projekten. Systeme, die bisher isoliert liefen, sind heute häufig via Internet erreichbar. Das erleichtert zwar die Fernwartung, öffnet aber auch neue Angriffsvektoren. Sensoren und Aktoren in Leitstellen, Wasserkraftwerken oder Umspannwerken müssen nicht nur funktional zuverlässig sein, sondern auch sicher vor Manipulation.

Um dieser Entwicklung entgegenzuwirken, haben viele Staaten – darunter Österreich – ihre Cyber-Abwehrstrukturen ausgebaut. Das umfasst neben technischen Verbesserungen, wie Segmentierung der Netzwerke und strengen Zugriffsberechtigungen, auch eine engere internationale Zusammenarbeit. So unterstützen sich europäische CERTs (Computer Emergency Response Teams) zunehmend gegenseitig, um in Krisensituationen schnell reagieren zu können und Informationen über Bedrohungen auszutauschen.

Nicht zuletzt tragen regulatorische Vorgaben wie die NIS2-Richtlinie der EU dazu bei, dass Betreiber kritischer Infrastruktur verpflichtet werden, ein höheres Schutzniveau einzuhalten. Trotzdem bleibt die Bedrohungslage akut: Ein erfolgreicher Cyberangriff auf eine zentralisierte Steuerungsanlage kann nicht nur wirtschaftliche Schäden in Milliardenhöhe verursachen, sondern im schlimmsten Fall auch Menschenleben gefährden. 2024 hat eindringlich bewiesen, dass Cyberabwehr in kritischen Bereichen zu den wichtigsten Sicherheitsaufgaben überhaupt zählt.

2.7.5 Professionalisierung der Cyberkriminalität

Im Verlauf des Jahres 2024 zeigte sich, dass die Cyberkriminalität nochmals deutlich professioneller geworden ist. In den letzten Jahren war bereits ein Wandel erkennbar, bei dem kriminelle Akteure ausgefeilte Geschäftsmodelle einführten. Inzwischen kann man geradezu von einer eigenen „Industrie“ sprechen, die sich um den Verkauf von Hacker-Dienstleistungen, Schadsoftware und gestohlenen Daten dreht.

Bekannt ist etwa das Cybercrime-as-a-Service (CaaS)-Konzept: Erfahrene Kriminelle entwickeln spezialisierte Angriffswerkzeuge oder komplette „Angriffs-Kits“ und bieten diese gegen eine Gebühr im Darknet an. Dadurch benötigen Kunden – also potenzielle Täter – immer weniger eigene IT-Kenntnisse, um erfolgreiche Cyberangriffe durchzuführen. Diese Dienstleistung kann alle Facetten des kriminellen Geschäfts umfassen: von gefälschten Websites (Phishing-Kits) über DDoS-Attacken bis hin zu Ransomware.

Weiterhin populär sind Affiliate-Modelle. Dabei betreiben die Entwickler von Ransomware oder Trojanern eine Art Partnerprogramm. „Affiliate-Kunden“ bezahlen eine Startgebühr oder teilen sich einen Teil der Lösegelderlöse mit den Entwicklern. Als Gegenleistung erhalten sie Zugang zu fertigen Schadsoftware-Bausteinen und Unterstützungsleistungen wie technische Hilfestellung oder Anleitungen zum Geldwaschen. Diese „Arbeitsteilung“ führt zu einer schnelleren Verbreitung neuer Schadsoftware und macht es Ermittlungsbehörden schwieriger, den Ursprung zurückzuverfolgen.

Ein weiterer Grund für die Professionalisierung ist, dass immer mehr legitime Tools und Cloud-Dienste zu kriminellen Zwecken missbraucht werden. Beispielsweise nutzen Angreifer gehostete Server in gängigen Cloud-Umgebungen, um Angriffe zu starten. Das verschleiert ihre Spuren, da solche Server zunächst als vertrauenswürdig gelten. Darüber hinaus haben viele Hackergruppen eigene Strukturen für Personalmanagement, Forschung und Entwicklung etabliert, sodass sie auf neue Sicherheitslücken schneller reagieren können als manche Unternehmen.

Die Finanzierung krimineller Organisationen erfolgt zunehmend über Kryptowährungen, die eine gewisse Anonymität bieten. Trotzdem konnten Strafverfolgungsbehörden 2024 auch einige spektakuläre Erfolge erzielen: Europol und Interpol arbeiteten eng mit nationalen Cybercrime-Einheiten zusammen und konnten mehrere große Ransomware-Banden zerschlagen. Solche Fahndungserfolge unterstreichen jedoch nur die Tatsache, dass sich die Szene mehr und mehr in Schattenbereiche des Internets zurückzieht und ihre Machenschaften immer besser tarnt.

Ein Ende dieser Entwicklung ist nicht in Sicht. Im Gegenteil, im Jahr 2024 haben wir erlebt, wie Kriminelle immer stärker von neuen Technologien – etwa KI und automatisierten Angriffswerkzeugen – Gebrauch machen. Gleichzeitig wächst die Bereitschaft, Angriffe über den internationalen Handel mit Hacker-Dienstleistungen zu finanzieren. Es gilt daher, auf Unternehmensseite wie auch auf staatlicher Ebene, gezielt dagegenzuhalten, etwa durch konsequente Strafverfolgung, bessere Aufklärung und den Ausbau von IT-Sicherheitsmaßnahmen.

2.7.6 Trends bei Ransomware und Phishing

Ransomware hat sich in den letzten Jahren zu einer der lukrativsten und gleichzeitig bedrohlichsten Methoden der Cyberkriminalität entwickelt. Auch 2024 hat sich dieser Trend fortgesetzt. Unter Ransomware versteht man Schadprogramme, die Daten eines Opfers verschlüsseln und für die Entschlüsselung ein Lösegeld verlangen. Neuerdings kombiniert diese Angriffsform verschiedene Methoden, um den Druck auf die Opfer zu erhöhen.

Einer der auffälligsten Trends ist die sogenannte Double Extortion. Dabei verschlüsseln die Täter nicht nur die Daten, sondern kopieren sie zusätzlich auf ihre Server. Im Fall einer Weigerung, das Lösegeld zu zahlen, drohen sie mit der Veröffentlichung sensibler Informationen – was Datenschutzverstöße, Reputationsverluste und teure Rechtsfolgen nach sich ziehen kann. Sogar eine Triple Extortion, bei der zusätzlich gezielt Kunden oder Lieferanten eines betroffenen Unternehmens unter Druck gesetzt werden, kommt zunehmend vor. Dieser mehrstufige Erpressungsansatz erhöht die Erfolgschancen der Angreifer erheblich.

Auch Phishing hat im Jahr 2024 weiter an Raffinesse gewonnen. Neben klassischen E-Mail-Kampagnen setzen Angreifer verstärkt auf Spear-Phishing, bei dem gezielt einzelne Personen oder Abteilungen angegangen werden. Die E-Mails sind dann so echt und personalisiert gestaltet, dass selbst versierte Nutzer oft erst bei genauem Hinsehen misstrauisch werden. Besonders gefährlich ist, dass Kriminelle mittlerweile KI-Modelle nutzen, um natürliche Sprache zu erzeugen oder gefälschte Chat-Verläufe zu erstellen. So wirkt der Betrug noch glaubwürdiger.

Ein weiteres Phänomen sind Smishing (Phishing via SMS) und Vishing (Phishing via Telefonanrufe). Durch die Nutzung mehrerer Kommunikationskanäle gelingt es Angreifern, eine größere Anzahl von potenziellen Opfern zu erreichen. Zudem werden sie kreativer, was die Tarnung angeht. Oft werden seriöse Namen oder Nummern nachgeahmt, etwa die einer Bank oder Behör-

de, sodass die Hemmschwelle für das Opfer sinkt, persönliche Daten preiszugeben.

Aufgrund dieser Entwicklungen investieren Unternehmen wie Privatpersonen zunehmend in bessere Schutzmaßnahmen. Awareness-Schulungen haben an Bedeutung gewonnen, um Mitarbeitende für Tricks und Täuschungen zu sensibilisieren. Unternehmen führen zudem häufiger Simulationen durch, bei denen gefälschte Phishing-Mails intern verschickt werden, um das Erkennungsvermögen zu steigern. Technisch können mehrstufige Authentifizierungsverfahren (MFA) und Anti-Phishing-Filter helfen, Angriffe abzuwehren. Dennoch zeigt das Jahr 2024, dass weder Ransomware noch Phishing so schnell verschwinden werden – sie passen sich stets den neuen Gegebenheiten an und lassen sich immer neue Methoden einfallen, um Nutzer auszutricksen.

2.7.7 Hacktivismus

Im Zuge globaler Spannungen haben sich 2024 verschiedene Formen von Hacktivismus herausgebildet, bei denen politische, soziale oder ideologische Ziele im Vordergrund stehen. Unter Hacktivismus versteht man die Nutzung von Hacking-Methoden – etwa das Eindringen in fremde IT-Systeme, das Lahmlegen von Websites oder das Veröffentlichen vertraulicher Daten –, um eine Botschaft zu verbreiten oder auf Missstände aufmerksam zu machen. Dabei kann es sich durchaus um unabhängige Aktivisten handeln, zunehmend aber auch um Angriffe, die von staatlichen Stellen unterstützt werden und unter dem Deckmantel des Hacktivismus operieren.

Ein typisches Instrument in diesem Kontext sind DDoS-Angriffe (Distributed Denial of Service). Hierbei werden Server oder Netzwerke mit einer derart hohen Zahl von Anfragen überflutet, dass sie legitime Anfragen nicht mehr bearbeiten können und faktisch „zusammenbrechen“. DDoS-Angriffe können Webseiten über Stunden oder Tage lahmlegen und so wirtschaftlichen Schaden verursachen oder ein politisches Statement setzen. Besonders kritisch wird es, wenn solche Angriffe gezielt auf kritische Infrastruktur zielen, wie etwa Energieversorger, Telekommunikationsunternehmen oder öffentliche Behörden.

2024 haben mehrere Gruppen öffentlichkeitswirksam DDoS-Attacken auf Regierungsportale und Medienunternehmen gestartet, um gegen bestimmte politische Entscheidungen zu protestieren oder Einfluss auf Debatten zu nehmen. Gleichzeitig ist nicht immer eindeutig, ob es sich wirklich um unabhängige Hacktivisten handelt, oder ob staatliche Akteure diese Gruppen im Hintergrund finanzieren oder lenken, um bestimmte geopolitische Ziele zu verfolgen. Das Verschleiern der Urheberschaft ist im Cyberspace relativ einfach, was eine klare Zuschreibung (Attribution) erschwert.

Auch die Informationsbeschaffung (beispielsweise durch Datendiebstahl und anschließende Veröffentlichung) ist ein beliebtes Mittel, um Regierungen oder Großunternehmen zu diskreditieren. In manchen Fällen werden erbeutete Dokumente selektiv veröffentlicht, um bestimmte Narrative zu untermauern und die öffentliche Meinung zu beeinflussen. Hier verschwimmen die Grenzen zwischen klassischer Spionage, Hacktivismus und Desinformationskampagnen.

Regierungen reagieren auf diese Bedrohung, indem sie ihre Cyberabwehr und Gesetzgebung anpassen. So werden Sicherheitsstandards für kritische Einrichtungen angehoben und grenzüberschreitende Kooperationen intensiviert, um gegen großangelegte DDoS-Attacken gemeinsam vorzugehen. Dennoch bleibt das Problem bestehen, dass Hacktivismus – ob echt oder staatlich

gelenkt – viele Sympathisanten finden kann, wenn er eine populäre Idee oder Protestbewegung vertritt. Gerade deshalb werden DDoS-Angriffe und zielgerichtete Datenlecks wohl auch in Zukunft ein beliebtes Mittel sein, um politisch Druck auszuüben oder für Aufmerksamkeit zu sorgen.

2.8 Hilfe bei Vorfällen

Auch wenn die Hauptaufgabe von CERT.at und GovCERT Austria darin besteht, koordinierend zu unterstützen, gibt es Fälle, die dabei herausstechen und wesentlich mehr Zeit erfordern als das normale Tagesgeschäft. In solchen Fällen unterstützen wir Betroffene sowohl mit unserem Fachwissen und unserer Erfahrung als auch bei der Koordination mit den relevanten staatlichen Stellen.

2.8.1 DDoS gegen österreichische Ziele

Ähnlich wie bereits in den vergangenen Jahren kam es auch 2024 zu einer Reihe von DDoS-Angriffen, bei denen erneut eine breite Palette von österreichischen Organisationen betroffen war, darunter öffentliche Einrichtungen und Betreiber kritischer Infrastrukturen, die ins Visier genommen wurden. Auch die Infrastruktur von CERT.at war zeitweise Ziel der Angreifer:innen. Es kam aber im Zusammenhang mit den Nationalratswahlen im September 2024 auch zu DDoS-Angriffen auf die Webseiten wahlwerbernder Parteien, die für öffentliche Aufmerksamkeit sorgten.

Dank der im Vorjahr gewonnenen Erfahrung konnten viele Betroffene jedoch ihre Schutzmaßnahmen und internen Abläufe rechtzeitig verbessern. Die umgehende Weitergabe von Informationen und die bereits etablierten Notfallpläne trugen maßgeblich dazu bei, dass sich die Auswirkungen auf die angegriffenen Systeme in Grenzen hielten. Die meisten betroffenen Organisationen konnten ihre Dienste rasch stabilisieren oder auf Ausweichinfrastrukturen zurückgreifen, wodurch großflächige Ausfälle vermieden wurden.

Insgesamt lässt sich festhalten, dass die verbesserten Vorbereitungsschritte und das enge Zusammenspiel zwischen CERT.at und den betroffenen Einrichtungen wesentlich dazu beitrugen, den Schaden zu minimieren. Die Angriffe wurden durch den Misserfolg, ernsthaften Schaden anzurichten, relativ schnell eingestellt – ein Beleg dafür, wie wichtig effektive Abwehrmaßnahmen und eine schnelle, gemeinsame Reaktion im Ernstfall sind.

2.8.2 Unterstützung bei Ransomware-Vorfällen

Auch im Jahr 2024 ging die Anzahl an Ransomware-Angriffen gegen österreichische Unternehmen und Institutionen leider nicht zurück, eher im Gegenteil. Die Angreifer:innen nutzten dabei eine Kombination aus neu entdeckten Sicherheitslücken und bereits existierenden Hintertüren, um sich unbemerkt Zugriff zu verschaffen. Ihr letztendliches Ziel blieb stets dasselbe: die Verschlüsselung geschäftskritischer Daten, um Druck auf die betroffenen Organisationen auszuüben und hohe Lösegeldsummen zu fordern.

Durch gezielte Hinweise durch CERT.at zu potenziell gefährdeten Systemen konnten viele österreichische Organisationen ihre Infrastruktur rechtzeitig absichern und Softwareupdates einspielen. In einer ganzen Reihe von Fällen wurden auf diesem Wege erfolgreiche Kompromittierungen verhindert, sodass sich der Schaden für die betroffenen Stellen deutlich in Grenzen hielt. Zusätzlich konnten durch internationale Partner zur Verfügung gestellte Informationen in mehreren Fällen genutzt werden, um beginnende Angriffe frühzeitig zu entdecken und zu verhindern, dass es schlussendlich zu einer Verschlüsselung von Daten kam.

Dennoch kam es zu Vorfällen, bei denen Ransomware in Netzwerken ausgerollt wurde, vor allem bei Klein- und mittelgroßen Unternehmen. Hier unterstützte CERT.at nach Möglichkeit die Betroffenen unter anderem bei der forensischen Analyse und der operativen Bewältigung der Vorfälle. Durch die enge Zusammenarbeit mit den betroffenen Organisationen, aber auch durch den Austausch mit internationalen Partnern, konnten oft wichtige Erkenntnisse zu den genutzten Angriffsmethoden gewonnen werden, die wiederum in neue Warnmeldungen einflossen.

Kapitel 3

Kooperationen und Networking

Ohne Zusammenarbeit ist die Arbeit eines CERTs/CSIRTs nicht möglich; keine Institution kann alle Bereiche der IT-Sicherheit im Alleingang abdecken. Dementsprechend haben CERT.at und GovCERT Austria über die Jahre viel Zeit in den Vertrauensaufbau und Vernetzung gesteckt.

3.1 Vernetzung als Grundvoraussetzung für Vertrauensbildung

CERT.at arbeitet nicht im Verborgenen an der Sicherheit des österreichischen Internets – im Gegenteil: Nur durch enge Zusammenarbeit und aktive Vernetzung mit nationalen und internationalen Akteur:innen der IT-Sicherheitsbranche können Bedrohungen frühzeitig erkannt und effektive Gegenmaßnahmen entwickelt werden. Der kontinuierliche Austausch von Erfahrungen, neuen Lösungen und Best Practices ist essenziell, um der dynamischen Bedrohungslage stets einen Schritt voraus zu sein. Eine starke Vernetzung, nationale wie internationale Sichtbarkeit und ein hohes Maß an gegenseitigem Vertrauen bilden die Grundlage der Arbeit von CERT.at.

CERT.at und GovCERT Austria verstehen ihre Aufgabe als Dienstleistung für die gesamte österreichische Gesellschaft. Jede Bürgerin und jeder Bürger profitiert letztlich von ihrer Arbeit – das „Produkt“, das sie bereitstellen, ist Sicherheit im Netz. Da es jedoch nicht möglich ist, jede einzelne Person direkt zu erreichen, setzen sie auf gezielte Interaktion mit Schlüsselakteuren der IT-Sicherheitsbranche. Dazu gehören Unternehmen, staatliche Institutionen, Forschungseinrichtungen und andere Organisationen, die sich mit Cybersicherheit befassen oder von ihr betroffen sind.

Ein wesentlicher Bestandteil ihrer Arbeit ist aktives Community-Management. CERT.at und GovCERT Austria pflegen den Austausch sowohl offline – durch die Organisation und Teilnahme an Konferenzen, Fachtreffen und Workshops – als auch online über Mailinglisten, soziale Medien und Instant-Messaging-Plattformen. Die Pandemie hat viele dieser Interaktionen in hybride Formate verlagert, doch seit 2023 finden vermehrt wieder physische Treffen statt, um den persönlichen Austausch weiter zu intensivieren.

Durch diese kontinuierliche Vernetzungsarbeit stärken CERT.at und GovCERT Austria die Zusam-

menarbeit zwischen relevanten Akteur:innen aus Wirtschaft, Forschung und Verwaltung in Österreich. Gleichzeitig sind sie international gut vernetzte und anerkannte Partner für ausländische CERTs und CSIRTs. Der Austausch mit internationalen Expert:innen ermöglicht es, globale Trends in der Cybersicherheit frühzeitig zu erkennen und gemeinsam Lösungen zu entwickeln.

GovCERT Austria nimmt dabei eine besondere Rolle ein: Als offizieller Ansprechpartner für vergleichbare staatliche Einrichtungen und internationale Organisationen vertritt es Österreich in Fragen der IKT-Sicherheit auf globaler Ebene. Diese internationale Zusammenarbeit stellt sicher, dass Österreich von weltweiten Sicherheitsinitiativen profitiert und aktiv zur Stärkung der globalen Cybersicherheitslandschaft beiträgt.

3.2 Vernetzung auf nationaler Ebene

3.2.1 Austrian Trust Circle (ATC)

Der Austrian Trust Circle (ATC) ist eine gemeinsame Initiative von CERT.at und dem österreichischen Bundeskanzleramt, die den sicheren und vertrauensvollen Austausch von sicherheitsrelevanten Informationen zwischen Unternehmen und Organisationen fördert. Er besteht aus ”Security Information Exchanges”, die gezielt auf verschiedene Bereiche der ”strategischen Informationsinfrastruktur (CIIP)” ausgerichtet sind und so eine enge Vernetzung innerhalb und zwischen kritischen Sektoren ermöglichen.

Durch den Austrian Trust Circle wird ein formeller Rahmen für den praxisnahen Informationsaustausch geschaffen, in dem Unternehmen nicht nur wertvolle Einblicke in aktuelle Bedrohungslagen erhalten, sondern auch voneinander lernen können. Er bietet eine Plattform für gemeinsame Sicherheitsprojekte und unterstützt österreichische Unternehmen dabei, Hilfe zur Selbsthilfe im Bereich der IKT-Sicherheit zu leisten. Gleichzeitig erhält CERT.at durch den ATC Zugang zu operativen Kontakten in verschiedenen Organisationen und kann so besser nachvollziehen, wie Sicherheitsvorfälle behandelt und bewältigt werden.

Der Austrian Trust Circle ist damit ein zentrales Netzwerk der österreichischen IKT-Sicherheit. Er stärkt das gegenseitige Vertrauen zwischen Akteur:innen der kritischen Infrastruktur und stellt sicher, dass im Ernstfall eine effektive und koordinierte Reaktion möglich ist. Durch den regelmäßigen Austausch entstehen wertvolle Synergien, die helfen, Bedrohungen frühzeitig zu erkennen und gemeinsam Gegenmaßnahmen zu entwickeln.

Die Gründung des ATC im Jahr 2011 erwies sich als vorausschauende Maßnahme. Als 2018 das Netz- und Informationssystemsicherheitsgesetz (NISG) in Kraft trat, waren viele Unternehmen, die nun offiziell als Betreiber wesentlicher Dienste eingestuft wurden, bereits an den offenen Austausch über Sicherheitsprobleme gewöhnt. Dadurch konnte eine Kultur der Transparenz und Zusammenarbeit etabliert werden, in der sich Unternehmen nicht scheuen, über Vorfälle zu berichten. Statt Vorfälle aus Angst vor Reputationsverlust zu verschweigen, wurde der bewährte Austausch im ATC genutzt, um Bedrohungen schneller zu identifizieren und gemeinsam Lösungen zu entwickeln.

Mit dieser starken Vertrauensbasis trägt der Austrian Trust Circle wesentlich zur Resilienz der österreichischen digitalen Infrastruktur bei und bleibt eine zentrale Säule der nationalen Cyber-

sicherheitsstrategie.

3.2.2 CERT-Verbund

Der nationale österreichische CERT-Verbund hat es sich zur Aufgabe gemacht, die Zusammenarbeit zwischen den österreichischen CERTs zu stärken und die CERT-Aktivitäten im Land gezielt zu fördern. Eine enge Vernetzung und Kooperation dieser Sicherheitsteams ist eine der wirkungsvollsten Strategien, um die vernetzten Informations- und Kommunikationssysteme gegen Bedrohungen abzusichern. Die steigende Anzahl an CERTs und CSIRTs in Österreich bestätigt diesen Ansatz und zeigt, dass koordinierte Cybersicherheitsmaßnahmen zunehmend an Bedeutung gewinnen.

Gegründet wurde der CERT-Verbund im Jahr 2011 als Zusammenschluss der damals bestehenden CERTs aus dem öffentlichen und privaten Sektor. Ziel dieser Kooperation war es, vorhandene Ressourcen und Fachkenntnisse zu bündeln, um die nationale Cybersicherheitslandschaft zu stärken und gemeinsam eine möglichst hohe IT-Sicherheit zu gewährleisten.

Durch den regelmäßigen Austausch profitieren die Mitglieder des Verbunds von gemeinsamem Wissen, bewährten Sicherheitsstrategien und schnellen Reaktionsmöglichkeiten im Ernstfall. Die enge Zusammenarbeit ermöglicht es, Synergien zu nutzen, Bedrohungen frühzeitig zu erkennen und effektive Schutzmaßnahmen zu ergreifen.

Heute ist der CERT-Verbund ein wesentliches Element der österreichischen Cybersicherheitsinfrastruktur. Er unterstützt nicht nur den Wissenstransfer zwischen Organisationen, sondern trägt auch dazu bei, Sicherheitsstrukturen kontinuierlich weiterzuentwickeln. Damit spielt er eine entscheidende Rolle in der Resilienz der digitalen Infrastruktur des Landes und sorgt dafür, dass Österreich auf aktuelle und zukünftige Herausforderungen in der IT-Sicherheit vorbereitet ist.

Die Teilnahme am CERT-Verbund ist freiwillig und kann jederzeit beendet werden. Alle Mitglieder verpflichten sich, folgende Ziele im Sinne eines gemeinschaftlich geführten und auf Kooperation basierenden CERT-Verbundes zu verfolgen:

1. Regelmäßiger Informations- und Erfahrungsaustausch
2. Identifikation und Bekanntmachung von Kernkompetenzen
3. Förderung nationaler CERTs in allen Sektoren

Im Lauf des Jahres 2023 fanden 6 Treffen physisch statt. Mit Stand Ende 2023 nehmen 17 Teams am österreichischen CERT-Verbund teil. Genauere Informationen finden Sie online.

3.2.3 IKDOK/OpKoord

Die “Struktur zur Koordination auf der operativen Ebene” (auch “Operative Koordinierungsstruktur” oder kurz “OpKoord” genannt) und der “Innere Kreis der operativen Koordinations-

struktur" (IKDOK) wurde erstmals in der im März 2013 herausgegebenen "Österreichische Strategie für Cyber Sicherheit" (ÖSCS 2013) beschrieben. Im Jahr 2016 nahmen beide Strukturen ihre Arbeit auf. Sowohl der IKDOK als die OpKoord bekamnen mit Inkrafttreten des NIS-Gesetzes Ende 2018 einen klaren rechtlichen Rahmen. Die Ende 2021 erschienene neue Version der "Österreichische Strategie für Cybersicherheit´´ (ÖSCS 2021) hat diese Strukturen nicht verändert.

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

Der IKDOK besteht (Siehe §3(4) NISG) aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für europäische und internationale Angelegenheiten. Die operative NIS Behörde (Abteilung IV/S/2 des BMI) hat die Aufgabe, die Koordinationsstrukturen zu leiten.

Damit sind die folgenden Akteure im IKDOK aktiv: Die operative NIS Behörde im Innenministerium (BMI IV/S/2), die strategische NIS Behörde im Bundeskanzleramt (BKA I/8) plus dem GovCERT, die Direktion für Staatsschutz und Nachrichtendienst (BMI/DSN), das Cybercrime Competence Center (BMI/BK), das das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) sowie das Abwehramt, das Heeres-Nachrichtenamt und das IKT & Cybersicherheitszentrum (alle BMLV).

3.2.4 Austrian Energy CERT – AEC

Gemäß der NIS-Richtlinie der Europäischen Union sind Betreiber kritischer Infrastrukturen dazu verpflichtet, sicherheitsrelevante Vorfälle wie Hacking-Angriffe oder schwerwiegende Softwareprobleme an eine zuständige Meldestelle weiterzuleiten. Um dieser Anforderung effizient nachzukommen, hat sich die gesamte österreichische Energiewirtschaft – einschließlich der Sektoren Strom, Gas und Öl – in einer bislang einzigartigen Initiative zusammengeschlossen.

In Form der Arbeitsgemeinschaft E-CERT wurde eine Public-Private-Partnership ins Leben gerufen, die das Austrian Energy Computer Emergency Response Team (AEC) aufgebaut hat. Diese Kooperation ermöglicht es, sicherheitsrelevante Informationen innerhalb der Branche gezielt auszutauschen, Bedrohungen frühzeitig zu erkennen und gemeinsame Maßnahmen zur Risikominimierung zu entwickeln.

Das AEC fungiert als zentrale Anlaufstelle für IT-Sicherheitsfragen in der österreichischen Energiewirtschaft und unterstützt Unternehmen dabei, ihre digitale Resilienz zu stärken. Durch die enge Zusammenarbeit zwischen öffentlichen Institutionen und privaten Energieunternehmen wird nicht nur ein effektives Meldewesen sichergestellt, sondern auch eine koordinierte Reaktion auf Cyberbedrohungen ermöglicht. Dieses Modell zeigt, wie durch sektorübergreifende Kooperationen ein hoher Sicherheitsstandard in einer der wichtigsten kritischen Infrastrukturen des Landes gewährleistet werden kann.

Mehr Informationen über das AEC finden Sie auf deren Webseite unter https://www.energy-cert.at/.

3.2.5 Cybersicherheit Plattform - CSP

Im Jahr 2015 wurde vom Bundeskanzleramt (BKA) die österreichische "Cyber Sicherheit Plattform" (CSP) als Public-Private-Partnership (PPP) ins Leben gerufen. Die CSP ist die zentrale Plattform Österreichs für die Kooperation zwischen dem privaten und öffentlichen Sektor in Sachen Cybersicherheit und dem Schutz kritischer Infrastrukturen.

Die CSP erfüllt mit allen Stakeholdern aus Verwaltung, Wirtschaft und Wissenschaft in Form einer Public-Private-Partnership folgende Aufgaben:

- Informationsaustausch zu wesentlichen Fragen der Cybersicherheit zwischen allen Mitgliedern der Plattform
- Initiierung von Kooperationen zwischen den beteiligten Partnern in den Bereichen Sensibilisierung und Ausbildung sowie Forschung und Entwicklung
- Beratung und Unterstützung der "Cyber Sicherheit Steuerungsgruppe"
- Förderung der Errichtung von Sektor-spezifischen Computer Emergency Response Teams (CERTs)
- Dachorganisation für bereits bestehende Kooperationsformate (unter anderem: Kompetenzzentrum Sicheres Österreich (KSÖ), Austrian Trust Circle (ATC), Cybersicherheitforum, A-SIT - Zentrum für sichere Informationstechnologie - Austria, Cyber Security Austria, CERT Verbund Austria)

CERT.at ist aktiver Partner der CSP und bringt unter anderem das Cyberlagebild in die Arbeit der CSP ein. Im Jahr 2024 wurde beispielsweise die "Nationale Coordinated Vulnerability Disclosure-Policy", die unter anderem die Rolle von CERT.at bei der Veröffentlichung von Schwachstelleninformationen regel soll, mit der CSP abgestimmt.

3.3 Vernetzung auf internationaler Ebene

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

3.3.1 Bilaterale Vernetzung

CERT.at pflegt eine enge Zusammenarbeit mit zahlreichen CERTs und CSIRTs aus benachbarten und Partnerländern, um den grenzüberschreitenden Austausch zu fördern und gemeinsame Sicherheitsstrategien zu entwickeln. Besonders intensiv ist die Kooperation mit dem Deutschen CERT-Verbund, mit dem ein regelmäßiger Dialog über aktuelle Entwicklungen und Bedrohungslagen stattfindet.

Ein wichtiger Bestandteil dieser Zusammenarbeit sind Konferenzen und Fachtreffen, zu denen CERT.at regelmäßig vom Deutschen CERT-Verbund eingeladen wird. Diese Veranstaltungen bieten eine Plattform für den direkten Erfahrungsaustausch, ermöglichen gegenseitige Updates zu neuen Sicherheitsherausforderungen und fördern die gemeinsame Erarbeitung von Lösungen.

Durch diesen grenzüberschreitenden Austausch wird nicht nur das Wissen über aktuelle Bedrohungen erweitert, sondern auch die Reaktionsfähigkeit auf internationale Cyberangriffe verbessert. Die enge Vernetzung mit Partnerländern trägt dazu bei, Synergien zu nutzen und die Sicherheit der digitalen Infrastruktur über nationale Grenzen hinweg zu stärken.

3.3.2 Task Force CSIRT

Die Task Force CSIRT (TF-CSIRT) dient in erster Linie als kontinuierliche und vertrauensbasierte Vernetzungsplattform für Computer Security Incident Response Teams. Ursprünglich entstand sie aus dem europäischen akademischen Netzwerk GÉANT und hat sich seither als wichtige Anlaufstelle für den Austausch von Wissen und Best Practices im Bereich der Cybersicherheit etabliert.

Mit der Einführung des CSIRTs Network, das speziell für die Zusammenarbeit zwischen nationalen und sektoralen CERTs innerhalb der EU geschaffen wurde, hat die Bedeutung der TF-CSIRT für CERT.at jedoch abgenommen. Während sie weiterhin eine wertvolle Plattform für internationale Vernetzung bleibt, hat sich der Fokus zunehmend auf direktere und strategisch ausgerichtete Kooperationsstrukturen verlagert.

Ein bedeutendes Ergebnis der TF-CSIRT ist die Entwicklung von Trusted Introducer (TI) – einer zentralen Datenbank, die eine wichtige Rolle bei der Bewertung der Vertrauenswürdigkeit und Seriosität von Akteur:innen im europäischen IT-Sicherheitsbereich spielt. Diese Plattform dient als Verzeichnis anerkannter CSIRTs und CERTs, erleichtert die Zusammenarbeit zwischen verschiedenen Sicherheitsorganisationen und stärkt das Vertrauen innerhalb der Cybersicherheits-Community.

3.3.3 CSIRTs Network

Im Jahr 2017 wurde auf Initiative der Europäischen Union und auf Basis der NIS-Richtlinie ein neues Netzwerk auf EU-Ebene eingeführt, mit dem ein Zusammenschluss aller europäischer nationalen CERTs und Branchen-CERTs erfolgen soll.

Mitglieder im CSIRTs Network (CNW) sind alle nationalen CERTs (in diesem Kontext: CSIRTs, die laut Artikel 9 der ersten NIS-Direktive, bzw. Artikel 10 der NIS2-Direktive akkreditiert sind) der EU-Mitgliedsländer, wobei es sich größtenteils um staatliche Stellen handelt. Dazu kommt noch CERT-EU, das CERT der EU-Organe, Einrichtungen und sonstige Stellen (EUIBAs). Das Netzwerk ist sehr divers, die Teamgröße reicht von sehr klein (etwa die CSIRTs aus Zypern oder Österreich) bis zu großen nationalen Cybersicherheitszentren wie NCSC-NL, ANSSI (Frankreich) oder dem CERT-Bund im deutschen BSI. Manche haben eher akademischen Hintergrund (CERT.LV, CERT.PL, CSIRT.CZ), andere hingegen sind sehr eng an den Nachrichtendienst (CFCS DK) angekoppelt. Für Österreich nimmt CERT.at, das GovCERT und das AEC am CSIRTs Network teil.

Das Netzwerk trifft sich mehrmals pro Jahr, online wird per Mailinglisten und vor allem über ein Instant Messaging System kooperiert. Letzteres hat sich seit seiner Einführung als wichtigstes Medium herausgestellt, da die niederschwellige Erreichbarkeit quer über die ganze Europäische Union die Zusammenarbeit zwischen Teams aller Mitgliedsstaaten deutlich verstärkt hat.

Die Phase des Vertrauensaufbaus hat das Netzwerk hinter sich gebracht, jetzt geht es um eine vertiefte Zusammenarbeit, sowohl im Tagesgeschäft als auch während größerer Vorfälle. Letzteres wird im Netzwerk regelmäßig geübt. Dadurch soll gewährleistet werden, dass bei Vorfällen, egal ob grenzübergreifend oder nicht, gegenseitige Unterstützung schnell und effizient erfolgen kann.

Um diese übergeordneten Ziele zu erreichen wird beispielsweise auf gleiche technische Lösungen[1] gesetzt, es gibt auch Versuche, eine gemeinsame Taxonomie (siehe 2.3: Taxonomie) zu etablieren.

3.3.4 European GovCERT Group

Die European GovCERT Group (EGC) ist ein gewachsenes Netzwerk, das sich aus den GovCERTs von zwölf europäischen Staaten sowie CERT-EU zusammensetzt. Während CERT-EU für die IT-Sicherheit der EU-Institutionen zuständig ist, dient die EGC als informelle Plattform für den länderübergreifenden Austausch und die koordinierte Reaktion auf Sicherheitsvorfälle. Im Gegensatz zum CSIRTs Network basiert die EGC nicht auf einer gesetzlichen Grundlage, sondern ist eine eigenständige Initiative der beteiligten CERTs, die auf freiwilliger Zusammenarbeit und gegenseitigem Vertrauen aufbaut.

Der Fokus der EGC liegt auf dem kontinuierlichen Austausch zwischen den Sicherheitsteams der teilnehmenden Länder. Dabei werden Informationen zu aktuellen Bedrohungen, Sicherheitsvorfällen und potenziellen Gefahren ebenso geteilt wie Erkenntnisse zu neuen Projekten und Werkzeugen. Neben regelmäßigen Treffen der GovCERT-Vertreterinnen und -Vertreter findet auch eine laufende und unkomplizierte Kommunikation zwischen den Teams statt, um einen schnellen und effizienten Informationsfluss sicherzustellen.

Ein entscheidender Vorteil dieses Netzwerks ist seine Unabhängigkeit von politischen Einflussnahmen, wodurch ein offener und vertrauensvoller Dialog zwischen den Mitgliedern gewährleistet wird. Diese enge Zusammenarbeit trägt dazu bei, länderübergreifende Cybersicherheitsrisiken besser zu verstehen und koordinierte Maßnahmen zu ergreifen.

Neben EU-Mitgliedstaaten umfasst die EGC auch CERTs aus Norwegen, der Schweiz und dem Vereinigten Königreich. Dies ermöglicht eine direkte Zusammenarbeit mit Organisationen, die nicht Teil des CSIRTs Network der Europäischen Union sind, und erweitert das Spektrum an Sicherheitsakteuren, mit denen ein vertrauensvoller Austausch gepflegt wird.

[1] Konkret unter anderem MISP und IntelMQ.

3.3.5 FIRST

Das Forum of Incident Response and Security Teams (FIRST) ist der weltweit anerkannte Verband von CERTs und Incident Response Teams. Die Mitgliedschaft in FIRST ermöglicht den Zugang zu einem globalen Netzwerk von Expertinnen und Experten sowie einer umfangreichen Wissensbasis, was eine effizientere und koordinierte Reaktion auf Sicherheitsvorfälle erleichtert.

Aufgrund der Größe des Netzwerks, das mittlerweile mehr als 800 Mitglieder umfasst, liegt der Fokus von FIRST nicht mehr auf der Bearbeitung einzelner Sicherheitsvorfälle. Stattdessen stehen der Erfahrungsaustausch, das gemeinsame Entwickeln von Sicherheitsstandards und Lobbying für bessere Cybersicherheitspraktiken im Mittelpunkt.

FIRST betreut zentrale Standards, die weltweit in der IT-Sicherheit genutzt werden. Dazu gehört das Traffic Light Protocol (TLP), ein System zur Klassifizierung und Weitergabe sensibler Informationen, das den sicheren Austausch innerhalb von Organisationen erleichtert. Ebenso entwickelt und pflegt FIRST das Common Vulnerability Scoring System (CVSS), eine Metrik zur standardisierten Bewertung von Schwachstellen, die weltweit genutzt wird, um Sicherheitslücken nach ihrer Kritikalität einzuordnen.

Durch diese Arbeit trägt FIRST maßgeblich zur Weiterentwicklung internationaler Sicherheitsrichtlinien bei und stärkt die Zusammenarbeit zwischen CERTs und Incident Response Teams über Länder- und Branchengrenzen hinweg.

Kapitel 4

Drittmittelprojekte

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

4.1 Connecting Europe Facilities (CEF)

Co-financed by the European Union
Connecting Europe Facility

4.1.1 AWAKE (2020-AT-IA-0254)

Im CEF-kofinanzierten Projekt AWAKE ("Cyber situational awareness for collaborative knowledge and joint preparedness") arbeiteten wir von September 2021 bis August 2024 gemeinsam mit dem Austrian Institute of Technology (AIT) als Koordinator, dem Bundesministerium für Inneres (BMI) sowie dem Bundeskanzleramt (BKA) an Werkzeugen für die kooperative Erstellung eines Lagebildes. Primär ging es hier um zwei der drei Ebenen in der Cybersicherheitsstrategie der EU (technisch: CERTs, operativ: CyCLONe; die dritte wäre die strategische), die sich in Österreich gut abbilden lassen.

Bei uns im CERT, auf der technische Ebene, geht es um die Details, was die (technischen) Bedrohungen sind, was aktuell ausgenutzt wird und was wo verwundbar ist. In Österreich ist die operative Ebene die entsprechende NIS Behörde im Innenministerium (das NIS Büro in der Sektion IV), wo es primär um die Auswirkungsdimension geht. Wir tauschen uns fallbezogen und laufend im Rahmen der OpKoord (siehe 5.1 NIS-Gesetz) aus. Das wollten wir mit diesem Projekt verbessern.

Einerseits ging es um eine Verbesserung des OSINT Prozesses: Mitarbeiter von CERT.at beobachten jeden Arbeitstag, was sich in der Welt zum Thema Cybersecurity tut: werden neue Schwachstellen bekannt, was gibt es Neues bei Werkzeugen, Taktiken und Prozeduren; welche Neuerun-

gen haben sich die Tätergruppen ausgedacht und was haben sich die Verteidiger an Verbesserungen einfallen lassen. Aktuell wird von CERT.at noch Taranis 3 (von GovCERT NL, später NCSC-NL entwickelt) für diesen Workflow benutzt; das Ergebnis kann man am Ende jeden Arbeitstages in der Tageszusammenfassung sehen.

In AWAKE setzten wir auf Taranis NG auf, was eine Neuimplementierung des Taranis Konzeptes mit einem aktuellen Softwarestack ist. Auf dieser Basis implementierte AWAKE neue Features, primär ein Clustering der Nachrichtenartikel in Stories. Wegen einiger grundlegender Umbauten und Verzögerungen bei der Annahme von Pull-Requests durch das Taranis NG Projekt war ein Code-Fork leider unvermeidlich, die AWAKE-Version heißt jetzt Taranis_AI. Einige der initial geplanten Neuerungen konten leider nicht mehr in der Projektlaufzeit umgesetzt werden; wir hoffen, dass wir das in Nachfolgeprojekte (etwa ENSOC, siehe 4.2.1) unterbringen können.

Andererseits ging es auch um das aktive Einholen von Statusberichten durch Umfragen. Hier konnten wir stark auf die Vorarbeiten aus dem ACCSA Projekt zurückgreifen. Das dort entwickelte Koord-Tool kann genau das: eine dauerhaft laufende Webumfrage, bei der sich die Fragen und Antworten mit der Zeit ändern dürfen, und wo jeweils eine aktuelle Zusammenfassung der Ergebnisse angezeigt wird. Im Nachhinein kann man sich auch anzeigen lassen, was der Wissensstand zu bestimmten Zeitpunkt war.

Beiden Modi gemeinsam ist die theoretische Möglichkeit, das System nicht nur als Brücke zwischen Layern, sondern auch im gleichen Layer zwischen geografischen Einheiten zu verwenden. Wir denken an, dass damit auch eine Aggregation der Information von EU-Mitgliedstaaten auf EU Ebene möglich sein sollte.

Den Projektfortschritt konnte man in den Repositories auf Github verfolgen: Taranis_AI und KoordTool.

4.1.2 JTAN (2020-EU-IA-0260)

Das Joint Threat Analysis Network (JTAN) Projekt war eine Kooperation mehrerer CERTs in der EU und lief von Juli 2021 bis Juli 2024. Für uns war primär die R&D Abteilung der nic.at (CERT.at Mutterfirma) eingebunden. Es ging für uns darum, Risikofaktoren für Domains zu finden und diese auf Basis der Daten, die in der Registry vorhanden sind, für konkrete Domains zu ermitteln. Die Vorgabe aus der NIS2 Direktive, dass die Identitäten von Domaininhabern validiert werden müssen, gab dem Projekt auch auf Seite der nic.at Druck, denn wenn in diesem Vorgang eine Risikoeinschätzung einer Domainregistrierung einfließen könnte, sind Prozessoptimierungen möglich.

Es wurden viele Rohdaten (aus Cyber Threat Informationen, dem Verhalten von Registranten und Registraren, sowie dem Volumen des DNS-Verkehrs) zu Risikobewertungen von Domains gesammelt, um dann daraus mit Hilfe von Machine Learning (ML) Methoden ein Modell zu entwickeln, damit wir für neue Domains gute Risikoabschätzungen geben können.

Gemeinsam mit den Kollegen von NASK, dem Betreiber von .pl und dem CERT-PL, arbeiteten wir auch an einer Berechnung vergleichbarer Risikofaktoren für Domains der TLD .at und .pl sowie an der statistischen Analyse der Ergebnisse.

Eine Vorstellung von JTAN im Rahmen einer Präsentation durch unsere Projektpartner CERT-PL und CIRCL auf der 36th annual FIRST Conference im Juni 2024 in Fukoaka kann man hier (https://www.youtube.com/watch?v=lcSO6O-9YRk) nachsehen.

4.2 Digital Europe Program (DEP)

Bisher war CEF das für CERT.at relevante Förderprogramm der EU, mit 2023 kam es hier zu Änderungen. Mit der Etablierung des ECCC (European Cybersecurity Competence Centre) und des Netzwerkes der nationalen Gegenstücke (bei uns Nationales Koordinierungszentrum Cybersicherheit (NCC-AT)) wurde das Digital Europe Program (DEP) das zentrale Förderinstrument für Cybersicherheit der Europäischen Union.

4.2.1 ENSOC (101127660)

Die EU-Kommission fördert im Rahmen des Digital Europe Programms Initiativen in Mitgliedsstaaten, die die Cybersicherheit der EU verbessern. Im Call DIGITAL-ECCC-2022-CYBER-03 werden insbesondere Projekte kofinanziert, die eine grenzüberschreitenden Zusammenarbeit von Security Operations Centres (SOCs) etablieren.

Die so gebildeten Konsortien können einerseits um Grants ansuchen, durch die eigene Kosten (Personal, Reisen, Hardware) zu 50% erstattet werden, andererseits können die Konsortien im Rahmen eines gemeinsamen Einkaufs mit dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung (ECCC) nötige Ausgaben im Bereich Hardware, Informationsquellen (etwa Cyber Threat Intelligence Feeds) oder Software(-Entwicklung) zu 75% ersetzt bekommen.

Der EU Cyber Solidarity Act, der dieses Schema gesetzlich verankert und langfristig finanziert, wurde am 19. Dezember 2024 verabschiedet und trat im Jänner 2025 inkraft.

ENSOC ist ein Konsortium von Cybersicherheitsagenturen aus mehreren EU-Mitgliedstaaten unter der Leitung von CCN-CERT, dem für die öffentliche Verwaltung zuständigem spanischen CERT. Als Mitglieder werden folgende Einrichtungen genannt:

- Directoratul National de Securitate Cibernetica (DNSC, Rumänien)
- Computer Incident Response Center Luxembourg (CIRCL,Luxemburg)
- Agenzia per la Cybersicurezza Nationale (ACN, Italien)
- Centro National de Ciberseguranca (CERT.PT, Portugal)

- Centro Criptológico Nacional (CCN-CERT, Spanien)
- NIS Büro Innenministerium (BMI, Österreich)
- NCSC-NL (Niederlande)

In der Ausschreibung waren die Teilnehmer auf ”public bodies” eingeschränkt, was eine direkte Teilnahme von CERT.at an diesem Projekt verhindert hat. Daher ist das offizielles Mitglied Österreichs das Innenministerium und CERT.at tritt nur als Subcontractor auf.

Das Konsortium definiert seine Ziele so:

> Through the ENSOC Crossborder Platform we aim at improving the collective security of EU stakeholders and support CSIRTs and SOCs by overlapping defensive capabilities.
>
> - Cyber Intelligence sharing: for continuous improvement of detection.
> - Incident Coordination: to limit the impact and scope of incidents. Necessary for incident visibility.
> - Automation: sharing anonymized information of an anomaly from minute 0.
> - Situation Awareness: to map the European cybersecurity situation. Based on:
>   - Incidents (LUCIA)
>   - Alerts (SIEM)
>   - Suspicious events (MISP)
>   - Vulnerabilities, social tension (PANORAMA)

Die Projektfortschritte 2024 waren leider überschaubar: der gemeinsame Einkauf (”Joint Procurement”) von 6 Lots durch sieben Staaten gemeinsam mit der EU (wobei hier die Verantwortung von der Kommission auf das ECCC überging) hatte zur Folge, dass man sich zuerst auf das Ausschreibungsprozedere, und dann auf die Ausschreibungstexte einigen musste. Das hat leider zu signifikanten Verzögerungen geführt.

4.2.2 Mitarbeit an Forschungsprojekten

SHIFT (KIRAS)

Das Austrian Energy CERT (AEC) nahm am Projekt SHIFT teil. Es ging um sichere Simulationstechnologien für cyber-physische Systeme und wurde nach Verlängerung im Sepember 2024 abgeschlossen.

Kapitel 5

Rechtsgrundlage

5.1 Netz- und Informationssicherheitsgesetz (NISG)

Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Um dies zu gewährleisten, wurde mit der Richtlinie (EU) 2016/1148 (“NIS-Richtlinie”) der erste EU-weite Rechtsakt über Cybersicherheit verabschiedet. Die NIS-Richtlinie wurde in Österreich mit dem am 29. Dezember 2018 in Kraft getretenen“NIS-Gesetz” umgesetzt.

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

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

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

5.1.1 NIS 2

Nachdem die NIS-2-Richtlinie auf EU-Ebene 2022 verabschiedet wurde, erfolgte in den EU-Mitgliedsstaaten die jeweilige Umsetzung in lokales Recht. In Österreich wurde bis zum Ende der Legislaturperiode im Juni 2024 an einer Gesetzesvorlage gearbeitet, die aber nicht mehr vor den Neuwahlen im September 2024 verabschiedet werden konnte, da es parlamentarisch insbesondere keine Mehrheit für die Ansiedlung des Themas im Innenministerium gab.

Die Einhaltung einer EU-Frist, die allen Mitgliedsstaaten bis Oktober 2024 Zeit zur Umsetzung gab, war damit nicht mehr möglich. Allerdings hatten zum Zeitpunkt Oktober insgesamt 23 Mitgliedsstaaten die Umsetzung noch nicht abgeschlossen.