GovCERT Austria

CERT.at

Bericht

Internet-Sicherheit

Österreich 2025

Inhaltsverzeichnis

1 CERT.at **1**

1.1 CERT.at – Österreichs nationales CERT . . . 1

1.1.1 CERT-Beirat – Strategische Leitlinien schaffen . . . 2

1.1.2 Vernetzung . . . 3

1.1.3 Gesetzlicher Auftrag von CERT.at . . . 3

1.2 Kernaufgaben von CERT.at . . . 4

1.3 Zertifizierungen 2025 . . . 5

1.3.1 ISO 27001 Zertifizierung . . . 5

1.3.2 TI Zertifizierung . . . 6

2 Das IT-Sicherheitsjahr 2025 **7**

2.1 NIS Meldungen . . . 7

2.2 Incident Reports, Incidents und Investigations . . . 11

2.3 Taxonomie . . . 15

2.3.1 Reference Security Incident Taxonomy – ein kurzer Überblick . . . 15

2.4 2025 im Detail . . . 16

2.4.1 Überblick . . . 16

2.4.2 Kategorie “Vulnerable” . . . 17

2.4.3 Kategorie “Malicious Code´´ . . . 20

2.4.4 Warnings . . . 22

2.4.5 Aktuelles . . . 23

2.4.6 Weitere Informationsangebote . . . 24

2.5 Datenbasis . . . 25

2.5.1 Eigene Erhebungen . . . 25

2.5.2 Externe Quellen . . . 27

2.6 Tooling . . . 28

2.6.1 IntelMQ . . . 29

2.6.2 MISP . . . 30

2.7 Bedrohungen . . . 30

2.7.1 Angriffe gegen Lieferketten . . . 32

2.7.2 Regulatorische Entwicklungen . . . 32

2.7.3 Künstliche Intelligenz . . . 34

2.7.4 Angriffe auf kritische Infrastruktur . . . 35

2.7.5 Trends bei Ransomware und Phishing . . . 37

2.8 Hilfe bei Vorfällen . . . 38
2.8.1 Verhinderung der Ausnutzung von Schwachstellen . . . 38
2.8.2 DDoS gegen österreichische Ziele . . . 38
2.8.3 Unterstützung bei Ransomware-Vorfällen . . . 39
3 Kooperationen und Networking **40**
3.1 Vernetzung als Grundvoraussetzung für Vertrauensbildung . . . 40
3.2 Vernetzung auf nationaler Ebene . . . 41
3.2.1 Austrian Trust Circle (ATC) . . . 41
3.2.2 CERT-Verbund . . . 41
3.2.3 IKDOK/OpKoord . . . 42
3.2.4 Sektoren-CERTs . . . 43
3.2.5 Government CERT - GovCERT . . . 43
3.2.6 Austrian Energy CERT - AEC . . . 44
3.2.7 Austrian Health CERT - AHC . . . 44
3.2.8 Cybersicherheit Plattform - CSP . . . 45
3.3 Vernetzung auf internationaler Ebene . . . 45
3.3.1 Bilaterale Vernetzung . . . 45
3.3.2 Task Force CSIRT . . . 46
3.3.3 CSIRTs Network . . . 46
3.3.4 European GovCERT Group . . . 47
3.3.5 FIRST . . . 48
4 Drittmittelprojekte **49**
4.1 Digital Europe Program (DEP) . . . 49
4.1.1 ENSOC (101127660) . . . 49

Impressum

Medieninhaber und Verleger: CERT.at GmbH, Computer Emergency Response Team Austria, Karlsplatz 1/2/9, 1010 Wien.

Konzeption und Redaktion: CERT.at

Herstellungsort: Wien, Februar 2026.

Vorwort: Wolfgang Rosenkranz (CERT.at)

Sehr geehrte Leserinnen und Leser,

2025 war aus Sicht der Cybersicherheit ein Jahr, in dem vieles, über das wir seit Jahren gesprochen haben, langsam Realität geworden ist. Regulierung, künstliche Intelligenz, geopolitische Konflikte und die Abhängigkeit von digitalen Lieferketten sind keine Zukunftsthemen mehr. Sie bestimmen inzwischen ganz konkret, womit sich Unternehmen, Behörden und auch wir als CERT beschäftigen müssen.

Zumindest bei NIS 2 hat Österreich im vergangenen Jahr einen entscheidenden Schritt gemacht. Nachdem wir uns an dieser Stelle vor einem Jahr noch darüber gewundert haben, dass die europäische Umsetzungsfrist ohne österreichisches Gesetz verstrichen war, wurde das NISG 2026 Ende 2025 schließlich beschlossen. Damit wissen wir nun zumindest, wohin die Reise geht. Für CERT.at bedeutet sie allerdings deutlich mehr Aufgaben, mehr Organisationen, die wir unterstützen sollen, und neue Rollen – unter anderem bei der koordinierten Behandlung von Schwachstellen.

Gleichzeitig gilt DORA seit Jänner 2025 unmittelbar für den Finanzsektor und auch der Cyber Resilience Act wird zunehmend praktisch relevant. Regulierung alleine macht Systeme natürlich noch nicht sicher. Aber 2025 war wohl das Jahr, in dem endgültig klar wurde, dass Cybersicherheit in Europa nicht mehr nur als freiwillige technische Aufgabe betrachtet wird.

Technisch war das Jahr leider weniger überraschend. Wir mussten wiederholt vor kritischen und teilweise bereits aktiv ausgenutzten Schwachstellen warnen – auffallend oft in Firewalls, VPN-Gateways und anderen Produkten, die eigentlich zur Absicherung von Netzwerken eingesetzt werden. Besonders problematisch wird es, wenn ein Update alleine nicht mehr genügt, weil Angreifer eine Schwachstelle bereits ausgenutzt und sich dauerhaft im System eingenistet haben. Genau das haben wir 2025 etwa bei Angriffen auf Fortinet-Systeme gesehen. Die alte Regel „Patch einspielen und Problem erledigt“ funktioniert in solchen Fällen nicht mehr.

Auch Phishing und Ransomware sind nicht verschwunden. Im Gegenteil: Die Methoden entwickeln sich weiter, während künstliche Intelligenz es einfacher macht, überzeugende Texte, Stimmen oder andere Inhalte für Social Engineering zu erzeugen. Gleichzeitig sehen wir, dass Cyberangriffe immer stärker mit politischen und militärischen Konflikten verbunden sind. DDoS-Angriffe und Hacktivismus gehören inzwischen fast schon zum digitalen Begleitprogramm internationaler Krisen. Das macht unsere Arbeit nicht unbedingt einfacher, zeigt aber umso deutlicher, warum funktionierende nationale und internationale Netzwerke zwischen CERTs wichtig sind.

2026 wird für CERT.at daher ein besonderes Jahr. NISG 2026 und Cyber Resilience Act bringen neue Aufgaben und werden auch unsere eigene Organisation verändern. Dabei sollten wir aber nicht vergessen, was die wesentliche Aufgabe eines CERT bleibt: Informationen sammeln, einordnen und weitergeben, Menschen miteinander vernetzen und dort helfen, wo trotz aller Vorsichtsmaßnahmen etwas schiefgegangen ist. In diesem Sinne wünsche ich Ihnen viel Vergnügen bei der Lektüre unseres Rückblicks auf das IT-Sicherheitsjahr 2025!

Wolfgang Rosenkranz, Teamleiter CERT.at

Kapitel 1

CERT.at

CERT.at leistet in seiner Rolle als nationales Computer-Notfallteam 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. CERT.at fungiert seitdem als erste Anlaufstelle für IT-Sicherheitsfragen im nationalen Kontext. Zuständig ist das Team für alle Cybersicherheitsvorfälle, die nicht bereits durch andere spezialisierte Notfallteams, etwa Sektoren-CERTs wie das GovCERT, das Energy-CERT und 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, kritischen Infrastrukturen und relevanten staatlichen Einrichtungen weiter intensiviert worden. Dies stärkt die gemeinsame Reaktionsfähigkeit auf nationale und internationale Cybersicherheitsvorfälle und ermöglicht eine engere Abstimmung zwischen Wirtschaft, Wissenschaft, Behörden und anderen Sicherheitsteams.

CERT.at überwacht laufend die Cyber-Bedrohungslage, verbreitet sicherheitsrelevante Informationen, vernetzt sich aktiv mit neuen nationalen und internationalen Partnern und reagiert auf relevante Ereignisse. Darüber 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 Informationen in Österreich fungiert CERT.at als vertrauenswürdige Informationsdrehscheibe, die Wissen bündelt, verdichtet, aufwertet und zielgenau weitergibt.

CERT.at ist zudem ein zentrales Bindeglied zwischen anderen CERTs und CSIRTs (Computer Se-

curity Incident Response Teams), insbesondere in den Bereichen kritischer Infrastrukturen und staatlicher Zuständigkeiten. 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 bei Bedarf die Koordination der Lagebilderstellung und informiert Behörden, Netzbetreiber sowie Sicherheitsteams. Dabei liegt der Fokus auf der schnellen und effektiven Bewältigung von akuten Sicherheitsvorfällen.

Das Team besteht derzeit aus 16 Expertinnen und Experten und wird von Robert Schischka und Andreas Musielak als Geschäftsführer geleitet.

1.1.1 CERT-Beirat – Strategische Leitlinien schaffen

CERT.at wird in seiner strategischen Ausrichtung von einem eigens dafür eingerichteten Beirat begleitet. Dieses Gremium setzt sich aus Expertinnen und Experten zusammen, die einen repräsentativen Querschnitt der österreichischen Internetgemeinde abbilden - von Behörden, über die akadmische Welt bis zur Wirtschaft.

Die Mitglieder des Beirats stellen sicher, dass CERT.at seine Aufgaben im Sinne der gesamten Gesellschaft wahrnimmt und sie agieren nach außen als engagierte Botschafterinnen und Botschafter für CERT.at. Sie stellen sicher, dass die Maßnahmen und Strategien von CERT.at stets mit einem ganzheitlichen Blick auf die österreichische IT-Landschaft entwickelt und umgesetzt werden.

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

Die Mitglieder des CERT-Beirats waren 2025:

- DI Philipp Blauensteiner (BMI)
- DI Michael Eichinger, BSc (BMI)
- Univ. Prof. Dr. Nikolaus Forgo (Universität Wien)
- Ing. Franz Hoheiser-Pförtner, MSc (MAG Wien, Vorsitzender)
- Dr. Andreas Koman (Internetstiftung)
- Ing. Thomas Mandl (CDCE, Stellvertretender Vorsitzender)
- DI (FH) Harald Michl (Univie/ACOnet/VIX)
- Ing. Clemens Möslinger, BA MSc (BKA)
- Christopher Ozvald, BSc MSc (Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz)
- Univ. Prof. Dr. Reinhard Posch (TU Graz)

- Ing. Robert Scharinger, BSc(Hons) MSc MBCS (Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz)
- Dipl.-HTL-Ing. Lambert Scharwitzl, MSc MA (BMLV)
- DI Dr. Andreas Schildberger (BOKU)
- Mag. Robert Schischka (nic.at)
- Ing. Dr. iur Christof Tschohl (Research Institute & Co. KG)
- Mag.(FH) Christian Zec, MSc (BKA)

1.1.2 Vernetzung

CERT.at ist keine isoliert arbeitende Einrichtung, sondern eine zentrale, national und international breit vernetzte Koordinations- und Informationsstelle, die aktiv zur Sicherstellung der IT-Sicherheit in Österreich beiträgt. Im Falle eines Angriffs auf IKT-Systeme nimmt das Expertinnen und Experten-Team Kontakt mit den jeweiligen Netzbetreibern 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, die wiederum allen anderen dabei helfen, diese Probleme gar nicht aufkommen zu lassen. Dabei handelt es sich um ein freiwilliges Angebot, das sich durch enge Zusammenarbeit mit der Cybersecurity-Community 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 Behörden 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 Internet. 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 ist seit mehr als einem Jahrzehnt einer der international maßgeblichsten Treiber einer koordinierten und gemeinsamen Gefahrenabwehr im Bereich der Cybersicherheit. Ein bedeutender Meilenstein in dieser Entwicklung war das Inkrafttreten der NIS-Richtlinie („Directive on Security of Network and Information Systems“) in 2016, gefolgt von NIS2 im Jahr 2023. Diese Richtlinie schafft einen EU-weit einheitlichen Rechtsrahmen, innerhalb dessen alle EU-Mitgliedstaaten ihre Kapazitäten zur Cybersicherheit ausbauen müssen. Sie definiert zudem verbindliche Mindestsicherheitsanforderungen, Risikomanagementmaßnahmen sowie Meldepflichten für Betreiber wichtiger bis wesentlicher Dienste.

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 blieb 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.

Wichtig ist dabei eine klare Abgrenzung: CERT.at ist keine Behörde und hat keine Eingriffsrechte in die österreichische Netzwerkinfrastruktur, agiert aber mit den über das NIS-Gesetz definierten und ihm per Bescheid übertragenen Rechten und Pflichten.

1.2 Kernaufgaben von CERT.at

Die Bedeutung der von CERT.at 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 übernimmt in seinen Zuständigkeitsbereichen eine Vielzahl essenzieller Aufgaben, um diesen Herausforderungen wirksam zu begegnen. So stellen wir sicher, dass Cyberbedrohungen frühzeitig erkannt, analysiert und effektiv abgewehrt werden. Wir 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 unverzichtbar, um die Sicherheit und Stabilität der österreichischen IT-Infrastruktur nachhaltig zu gewährleisten. Ihr gemeinsames Ziel ist es, ein widerstandsfähiges, gut vernetztes und proaktives Cybersicherheitsumfeld zu schaffen, das den steigenden Bedrohungen wirkungsvoll entgegentreten kann.

Information in allen Bereichen: CERT.at verfolgt 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 stützt sich CERT.at neben eigener Sensorik auf Quellen[1] 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 unterstützt im Rahmen seiner 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, agiert CERT.at bei größeren Vorfällen als Koordinationsstelle und Schnittstelle zwischen den Betroffenen und anderen relevanten Akteurinnen und Akteuren 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.

1.3 Zertifizierungen 2025

1.3.1 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.

[1] Eine ausführliche Beschreibung der verwendeten Quellen findet sich in 2.6 Tooling.

Ein wichtiger Qualitätsnachweis in diesem Bereich ist die Zertifizierung nach ISO 27001:2022. 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.

1.3.2 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 2025) eines von 15 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 2025

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 zur 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 können.

Aus all diesen technischen und nicht-technischen Informationen entsteht der tägliche Blick auf das "Cybersecurity-Österreich". Im Folgenden wird beschrieben, wie diese Informationen gesammelt und ausgewertet wurden und was sie über das IT-Sicherheitsjahr 2025 aussagen.

2.1 NIS Meldungen

Das NIS Gesetz sieht vor, dass freiwillige Meldungen und Pflichtmeldungen an die jeweils zuständigen Computer-Notfallteams übermittelt werden. Sollte ein Sektor kein eigenes sektorenspezifisches CERT zur Verfügung haben, ist an das nationale Computernotfallteam zu melden. 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.

Über alle CERTs (nationales, GovCERT, Energie-CERT und Health-CERT[1]) zusammengefasst zeigt

[1] Wir danken dem AHC für die Bereitstellung der Daten aus dem Gesundheitsbereich.

Abbildung 2.1 folgende Entwicklung der NIS-Meldungen.

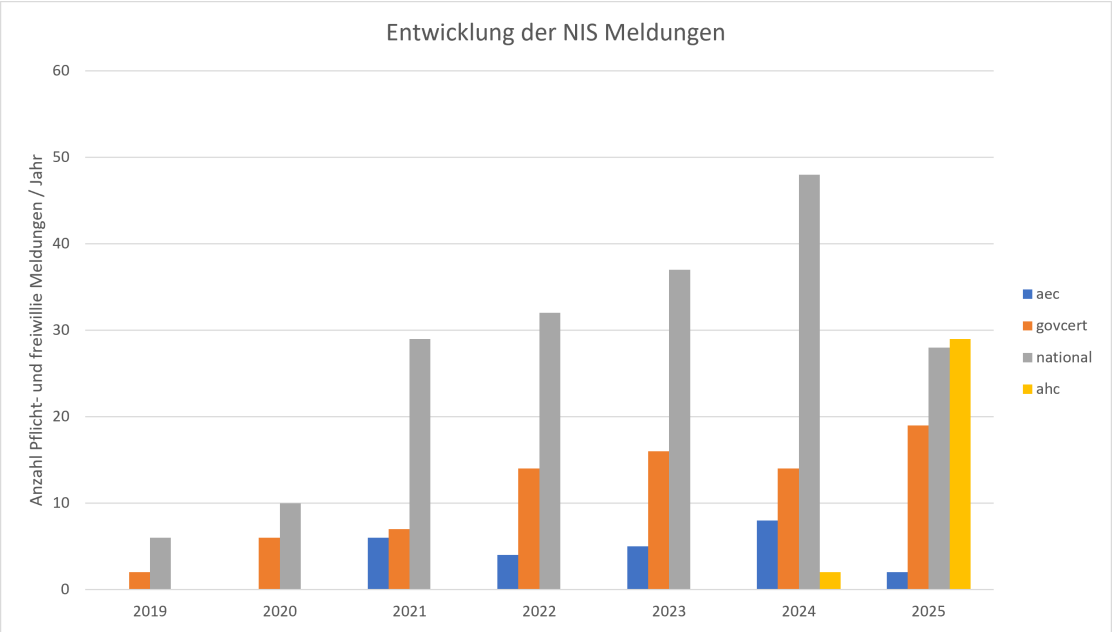


Abbildung 2.1: Entwicklung der NIS-Meldungen seit 2019 (nach CERT)

Abbildung 2.2 stellt die Entwicklung nach dem Typ der Meldung aufgeschlüsselt dar. 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.

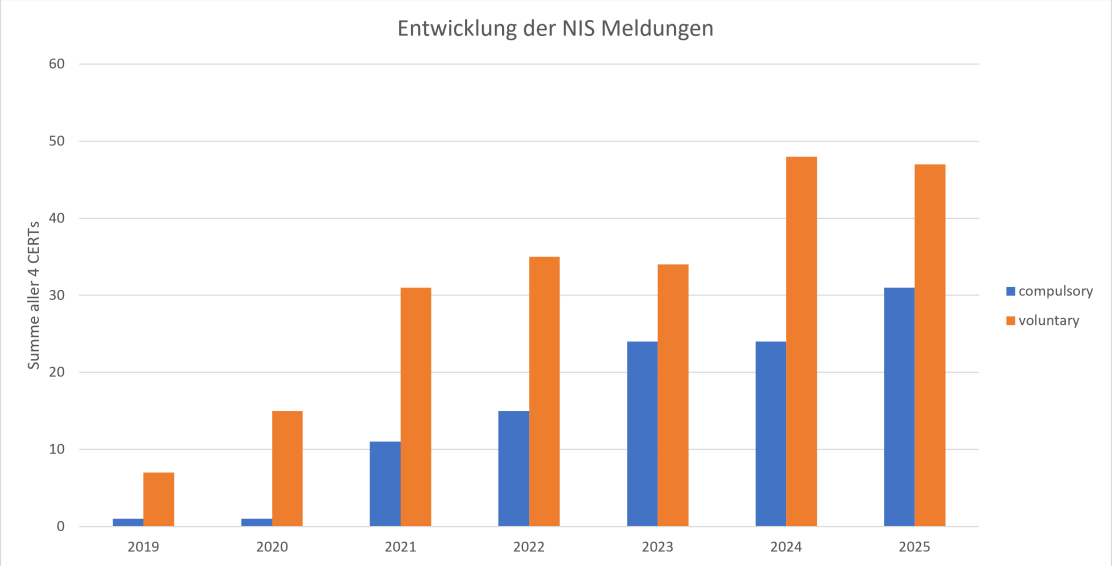


Abbildung 2.2: Entwicklung der NIS-Meldungen seit 2019 (nach Meldungstyp)

Anfang 2023 wurde das Meldeformular so erweitert, dass auch ”Art” und ”Herkunft” des Vorfalls abgefragt werden. Damit werden gezielt die Attribute der Vorfälle erfasst, die in der EU-weiten Präsentation der Meldedaten durch die ENISA dargestellt werden. Für 2025 sind diese Daten nicht immer konsistent, da die ENISA schon auf NIS2 umgestellt hat, Österreich aber noch nach NIS1-Schema berichtet hat.

Die Art des Vorfalls zeigt massive Differenzen zwischen freiwilligen und Pflichtmeldungen wie Abbildung 2.3 für das Jahr 2025 zeigt. Bei den Pflichtmeldungen zeigt sich, dass der Serviceausfall fast immer der Grund für die Meldung war, während bei freiwilligen Meldungen das Bild differenzierter ist.

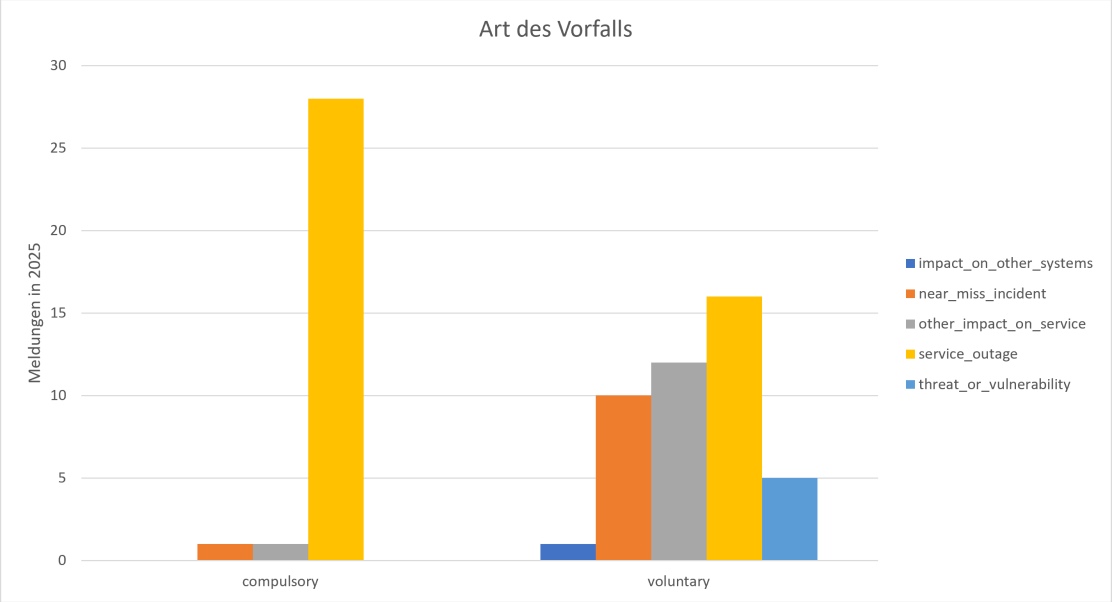


Abbildung 2.3: Art des Vorfalls einer NIS-Meldung 2025

Bei der Herkunft des Vorfalls geht es um den Auslöser (im CIRAS der ENISA wird das ”Root Cause” genannt) des Vofalls. Auch hier gibt es klare Unterschiede zwischen freiwilligen und Pflichtmeldungen. Abbildung 2.4 stellt diese für 2025 dar.

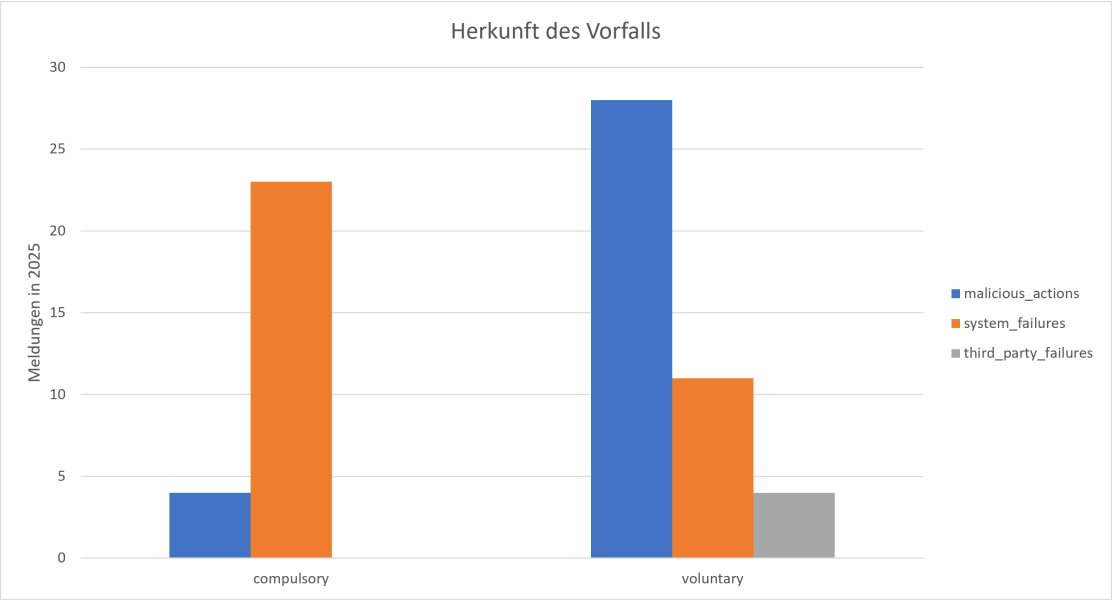


Abbildung 2.4: NIS-Meldungen 2025: Herkunft

Aus dem Blickwinkel Sektor betrachtet sieht man, dass der Gesundheitssektor die Pflichtmeldungen dominiert, wie Abbildung 2.5 zeigt. Wichtig zu betonen ist hier, dass fast alle diese Pflichtmeldungen technische Störungen betreffen und keine Cyberangriffe.

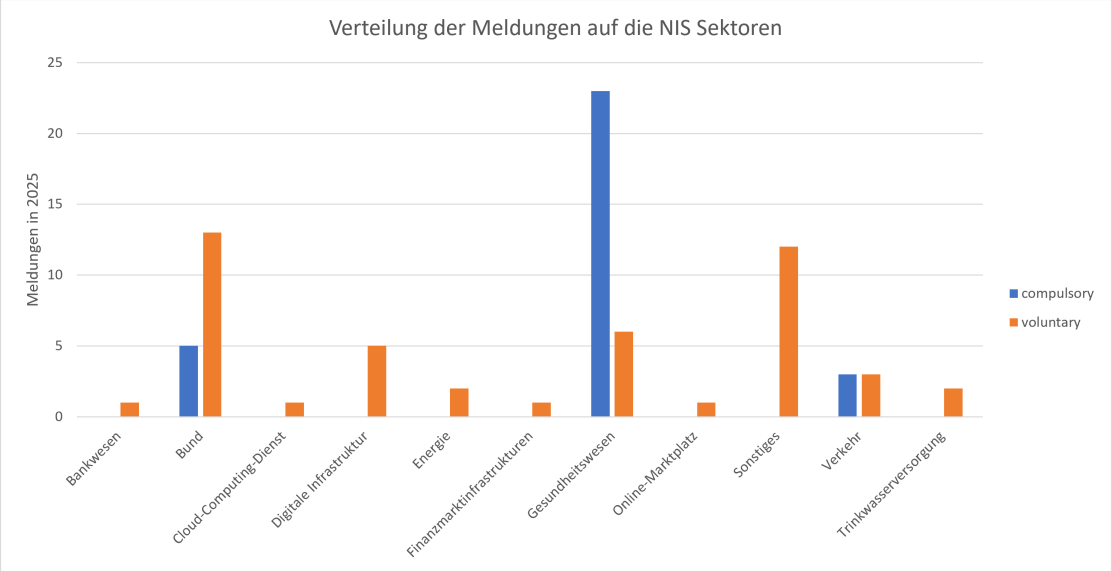


Abbildung 2.5: NIS-Meldungen 2025: Sektorenverteilung

2.2 Incident Reports, Incidents und Investigations

Eingehende und ausgehende Informationen werden bei CERT.at in Incident Reports, Incidents und Investigations getrennt:

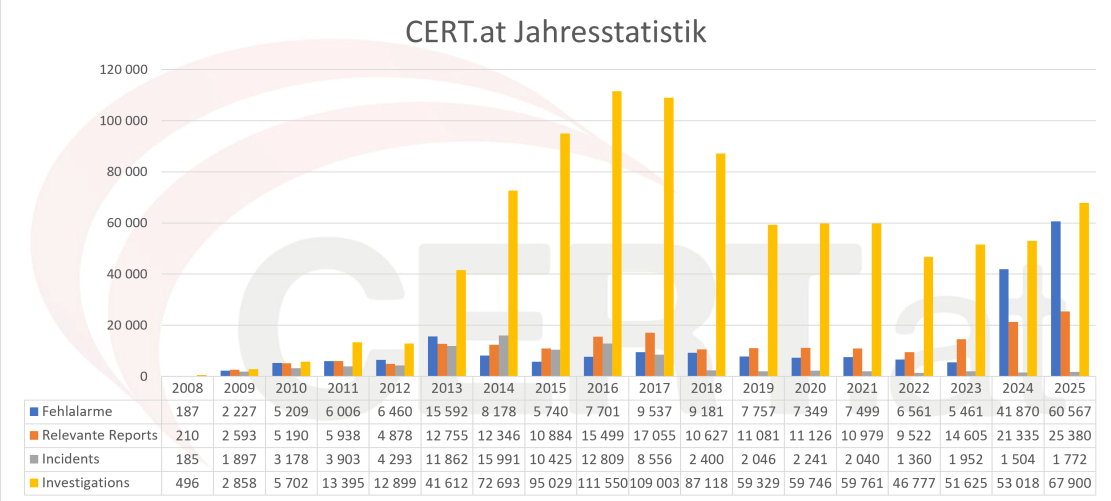
Incident Reports sind Meldungen über Sicherheitsprobleme oder -vorfälle, die bei CERT.at eingehen. Diese werden anschließend als relevant, informativ oder als Fehlalarm kategorisiert. Als "informativ" sieht CERT.at Meldungen an, bei denen eine Weiterverarbeitung aufgrund verschiedener Faktoren nicht 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-verschlüsselter E-Mail übermittelt werden.[2] In vielen Fällen sind die Reports in Datenfeeds rein informativ, weil sie etwa die erreichbaren Services in Netzblöcken beschreiben. Daher ist ein hoher Anteil an Reports, die nicht zu Incidents geführt haben, normal und für sich genommen kein Zeichen für eine schlechte Datenquelle.

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.

[2] 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	2025
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	60 567
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	25 380
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	1 772
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	53 018	67 900

Abbildung 2.6: Incident Reports, Incidents und Investigations im Überblick

Die Abwicklung der Vorfallsbehandlung erfolgt – wo immer möglich – automatisiert. Eine 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.

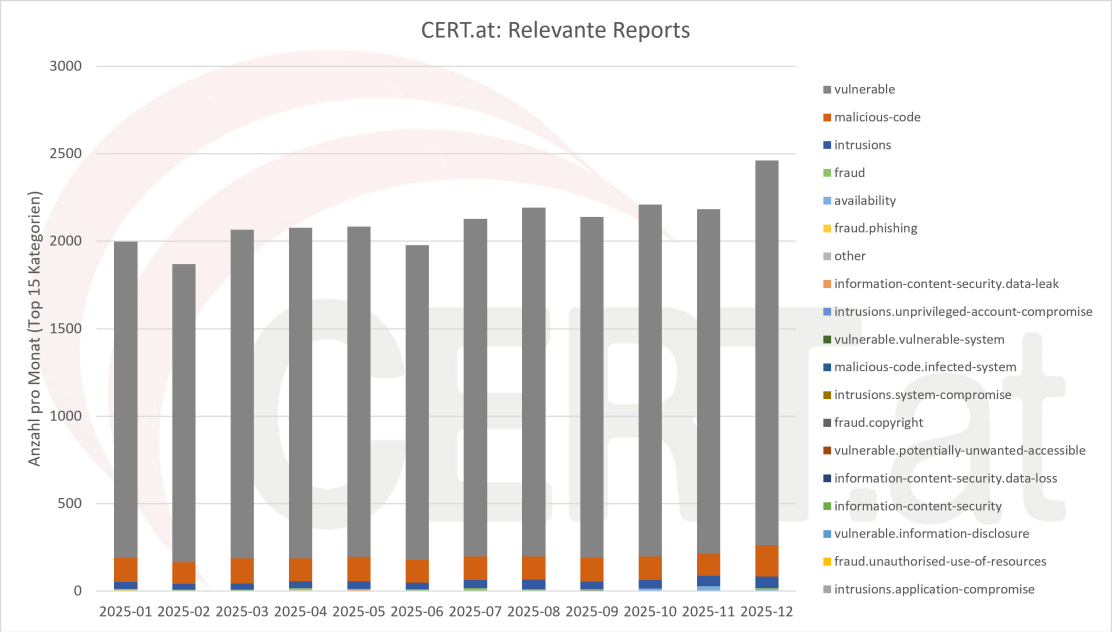


Abbildung 2.7: Incident Reports

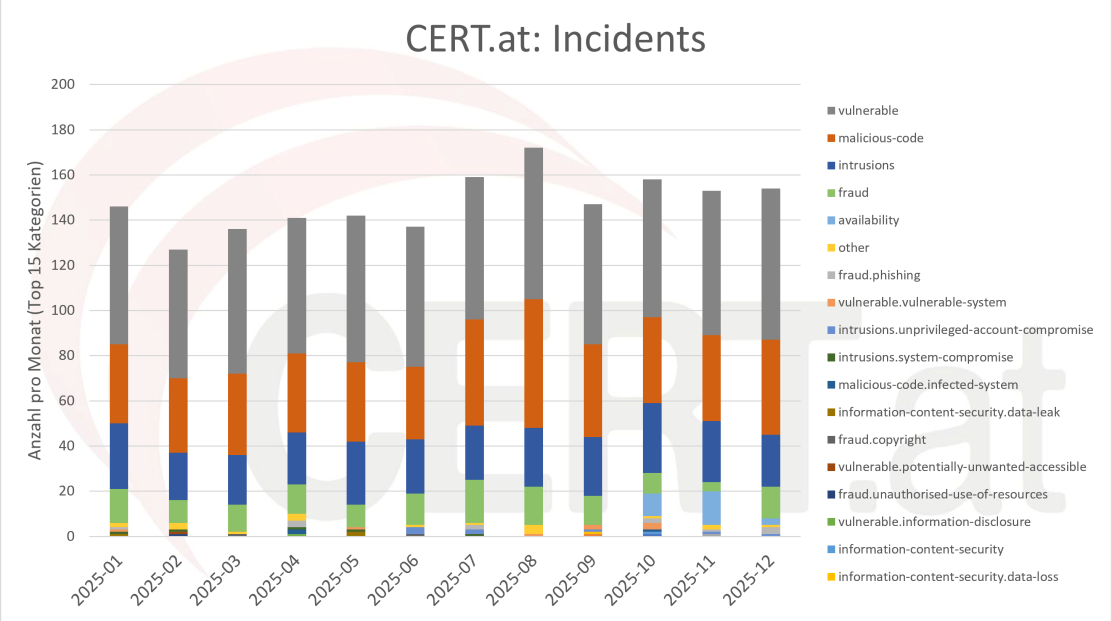


Abbildung 2.8: Incidents

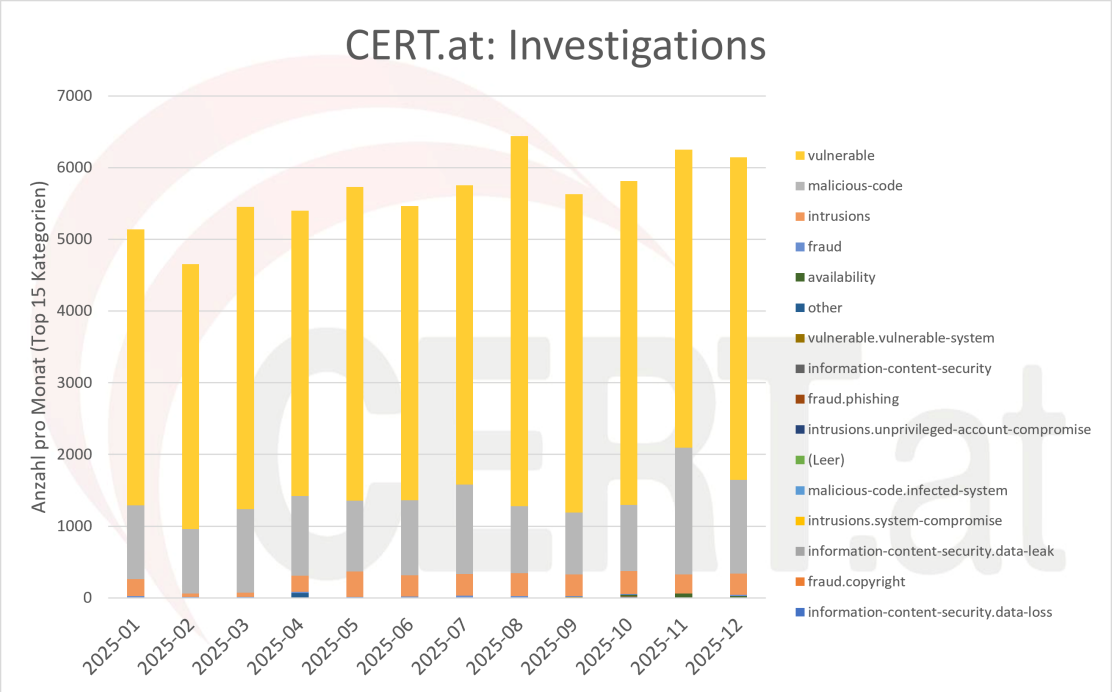


Abbildung 2.9: Investigations

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 SicherheitsforscherInnen müssen sich auf gemeinsame Richtlinien zum Austausch von Informationen einigen, um im Notfall schnell eingreifen zu können. Auch eine automatisierte Verarbeitung von Reports ist nur möglich, wenn sich alle einer einheitlichen Sprache bedienen.

Die Taxonomie, auf die sich CERT.at stützt, ist die ”Reference Security Incident Taxonomy”, die auf der älteren eCSIRT II Taxonomy (PDF) basiert. Die Kategorien dieser Taxonomie sind nicht exklusiv, d.h. mehrere Kategorien können auf einen Vorfall zutreffen. In Bezug auf Probleme mit Webservern verwendet CERT.at eine noch genauere Aufspaltung der einzelnen Kategorien.

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 Passwörtern 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 autorisierte 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 2.4.2 Kategorie "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 2025 im Detail

Der größte Teil der Daten, die CERT.at ausschickt, kommt aus diversen automatischen Feeds.[3] 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, da die täglichen Werte in den täglichen Statistiken zu stark variieren.

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.

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 Überblick

Wie im Kapitel 2.3 erklärt, verwendet CERT.at eine dreistufige Taxonomie zur Einstufung von Vorfällen. Auch die automatisiert verarbeiteten Hinweise zu Sicherheitsproblemen in Österreich folgen diesem Schema.

[3] Für eine genauere Beschreibung siehe 2.5 Datenbasis.

Auf der obersten Ebene der Taxonomie verteilen sich die behandelten Events wie in Abbildung 2.10 dargestellt:

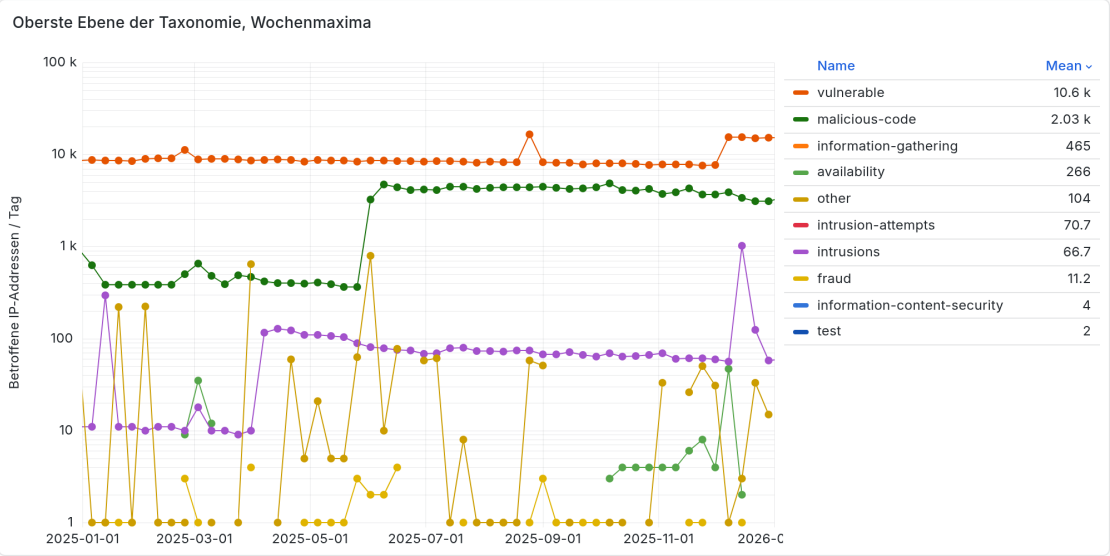


Abbildung 2.10: Alle Events nach oberster Ebene der Taxonomie

2.4.2 Kategorie “Vulnerable”

In den von CERT.at verarbeiteten Informationen zu IP-Adressen machen verwundbare Systeme die größte Teilmenge aus. Schränkt man die Datenbasis auf die Kategorie ein, und betrachtet man die Verteilung der IP-Adressen auf der zweiten Ebene der Taxonomie, dann erhält man Abbildung 2.11

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 und Nutzer das oft gar nicht bzw. verfügen nicht über das technische Know-How, um Änderungen vorzunehmen (sofern das überhaupt möglich ist).

(Vergessene) “Spielwiesen”: Technisch versierte Nutzerinnen und Nutzer 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.

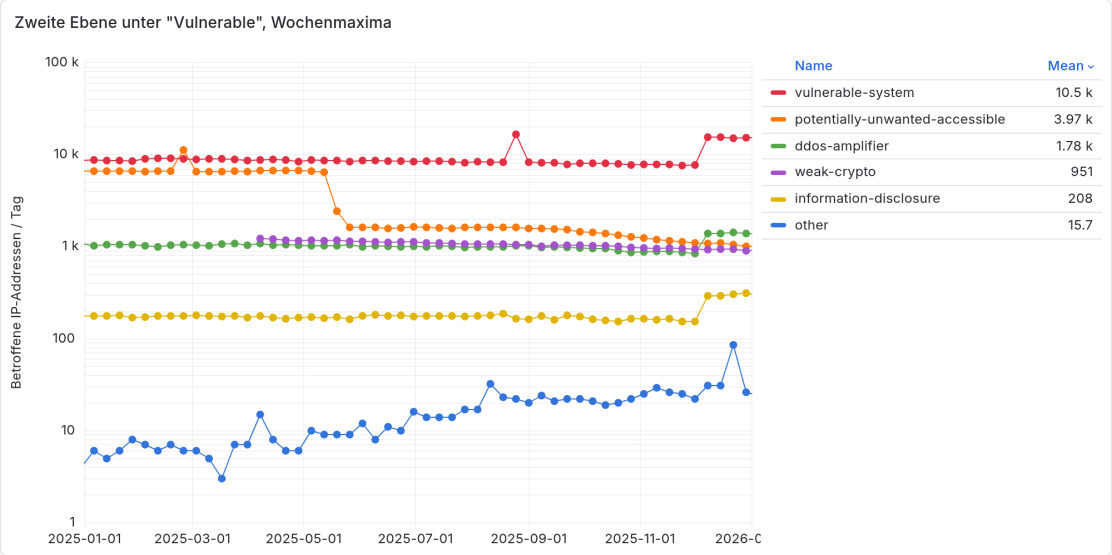


Abbildung 2.11: Verteilung der Events unter “Vulnerable”

Zoomt man weiter in die Daten hinein, ergeben sich folgende Erkenntnisse in der dritten Ebene der Taxonomie:

Dominiert wird die Untergruppe ”Vulnerable System” (Abbildung 2.12) durch CWMP und eine Woche, in der IKE mitgerechnet wurde. CWMP ist ein Management-Protokoll für Modems/Router auf Kundenseite, das eigentlich nicht offen im Netz erreichbar sein sollte.

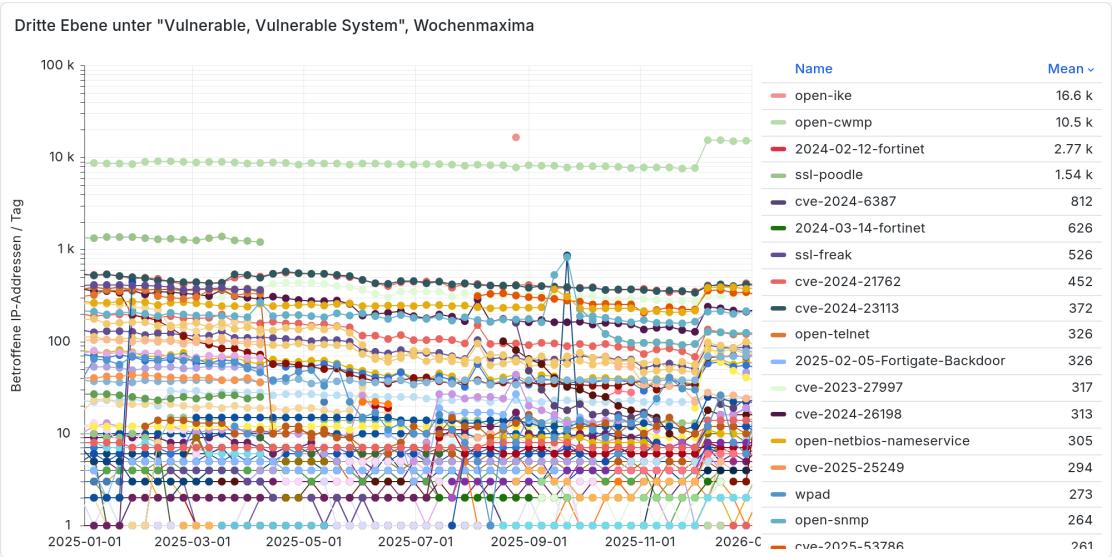


Abbildung 2.12: Verteilung der Events unter “Vulnerable / Vulnerable System”

TFTP, MSRPC, 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 abzusichern. So sind etwa Fernwartungszugänge direkt per RDP oft ein Faktor bei Ransomware-

vorfällen. (Abb. 2.13)

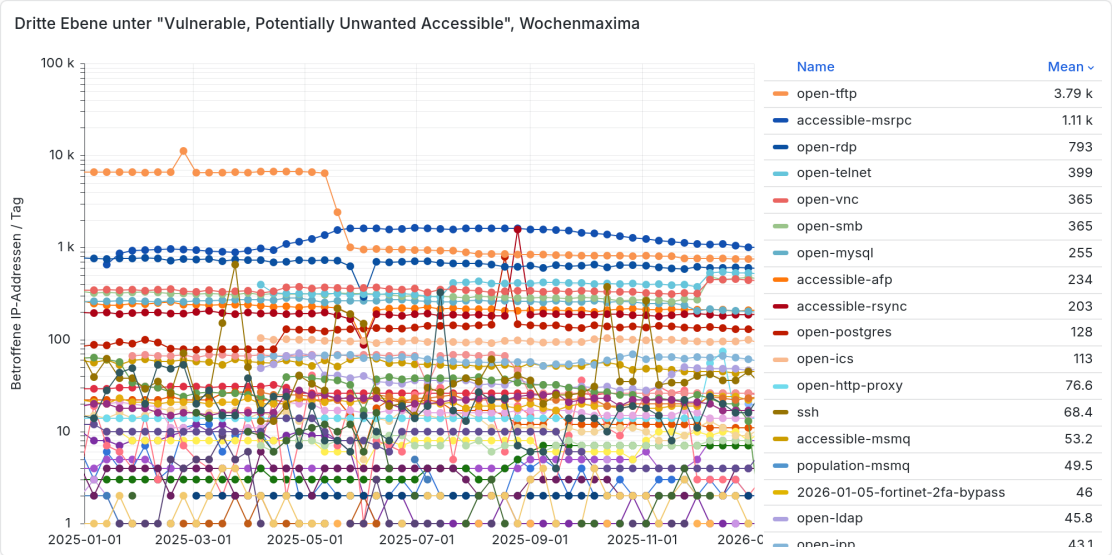


Abbildung 2.13: Ports, die nicht öffentlich erreichbar sein sollten

”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. 2.14)

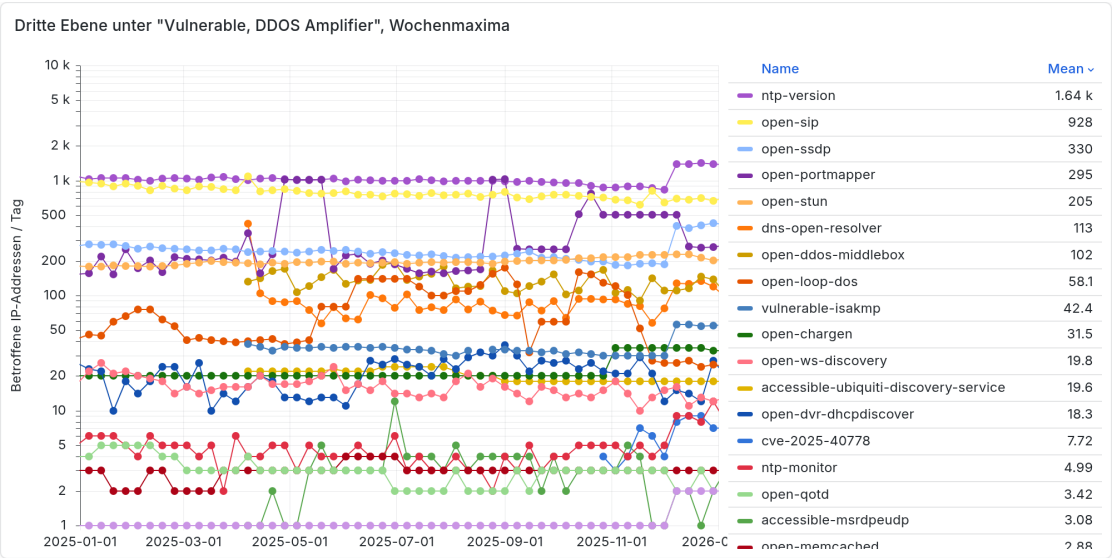


Abbildung 2.14: Geräte, die für UDP DDoS Amplifikation missbraucht werden können

Auch veraltete oder anfällige Kryptografie kann ein ein Problem für die betroffenen Systeme werden. Die CERT.at Datenbasis zu diesem Thema findet sich in Abbildung 2.15.

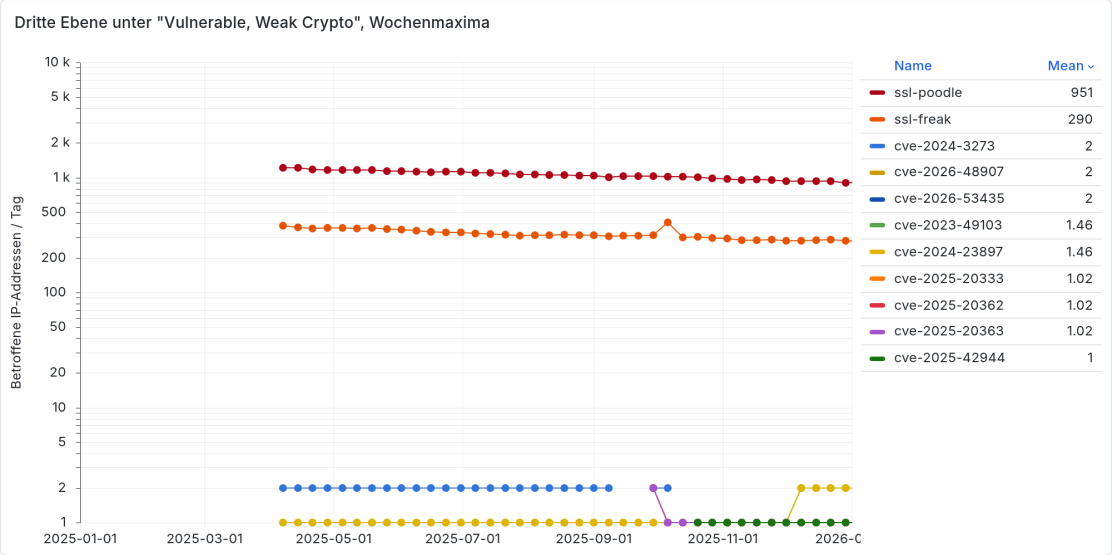


Abbildung 2.15: IP-Adressen, die verwundbare Verschlüsselungsverfahren einsetzen.

Shodan “Verified Vulnerabilities”

Die Suchmaschine Shodan hat sich zu einer etablierten Quelle für Schwachstellen und deren Analyse entwickelt, weshalb wir einen engen partnerschaftlichen Kontakt zu Shodan pflegen. Die “Verified Vulnerabilities” zeigen ihrem Namen nach entsprechend Schwachstellen an, die Shodan gefunden und verifiziert hat.[4] Diese Funktionalität ist nur für eine begrenzte Anzahl von IP Adressen anwendbar; im Falle von CERT.at sind das all jene, die in Österreich geolokalisiert sind. Diese Informationen werden automatisiert an ausgesuchte Netzverantwortliche geschickt, um diese bei der Erhaltung der ”Netzhygiene” zu unterstützen.

2.4.3 Kategorie “Malicious Code´´

Die zweitgrößte Kategorie an Problemen mit IP-Adressen in Österreich (siehe Abb. 2.10) behandelt Malware. Hier geht es nicht mehr nur um ”was passieren könnte”, sondern hier hat schon jemand Systeme übernommen und kontrolliert diese aus der Ferne.

Auf der zweiten Ebene der Taxonomie verteilen sich die betroffenen IP-Adressen wie in Abbildung 2.16 dargestellt:

[4] 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.

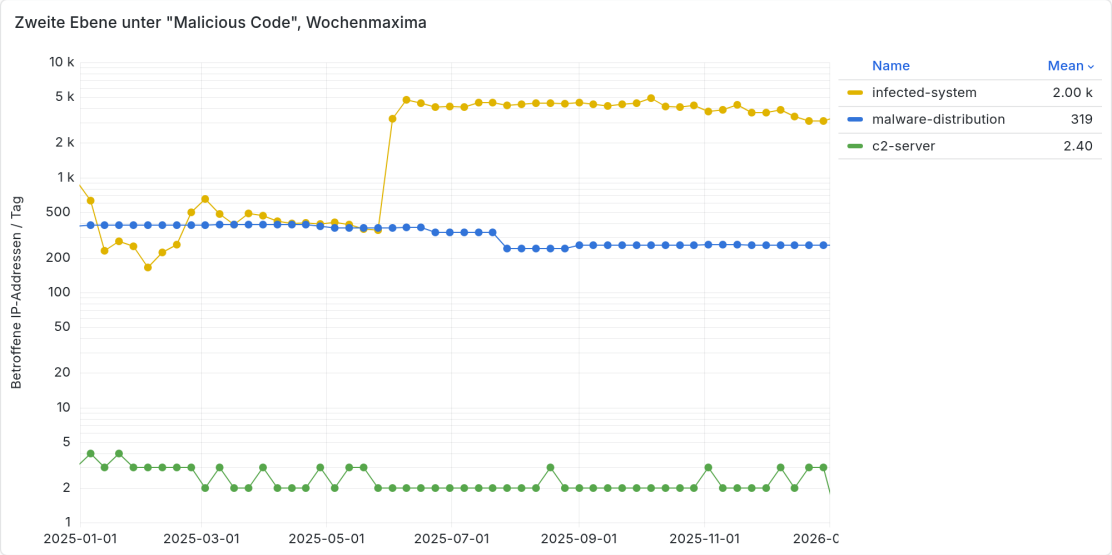


Abbildung 2.16: Zweite Taxonomieebene unter “Malicious Code´´

Betrachtet man die dritte Ebene der Taxonomie unter “Malicious Code´´ und “Infected System´´, so werden Detail zu den infizierten Systemen sichtbar. Bei der Interpretation der Daten muss man vorsichtig sein: diese Graphen zeigt, welche Infektionen in den Datenquellen von CERT.at sichtbar sind, haben daher potentiell eine starke Verzerrung gegenüber der Wirklichkeit. Auch ist nicht jede Malware-Infektion gleich zu bewerten: Android/Avalanche Infektionen, wo die Steuerungsserver schon längst von der Polizei übernommen wurden sind super gut sichtbar – aber stellen nur noch eine sehr kleine Bedrohung für die Eigentümer der Systeme dar. Andersherum tauchen Infektionen, die zu Ransomware geführt haben, in diesen Daten selten auf, weil hier der Einblick der Sicherheitsforscher in die Botnetze deutlich schlechter ist, und eine Infektion oft durch die Verschlüsselung der betroffenen Systeme beendet wird. Die Datenbasis von CERT.at wird in Abbildung 2.17 dargestellt.

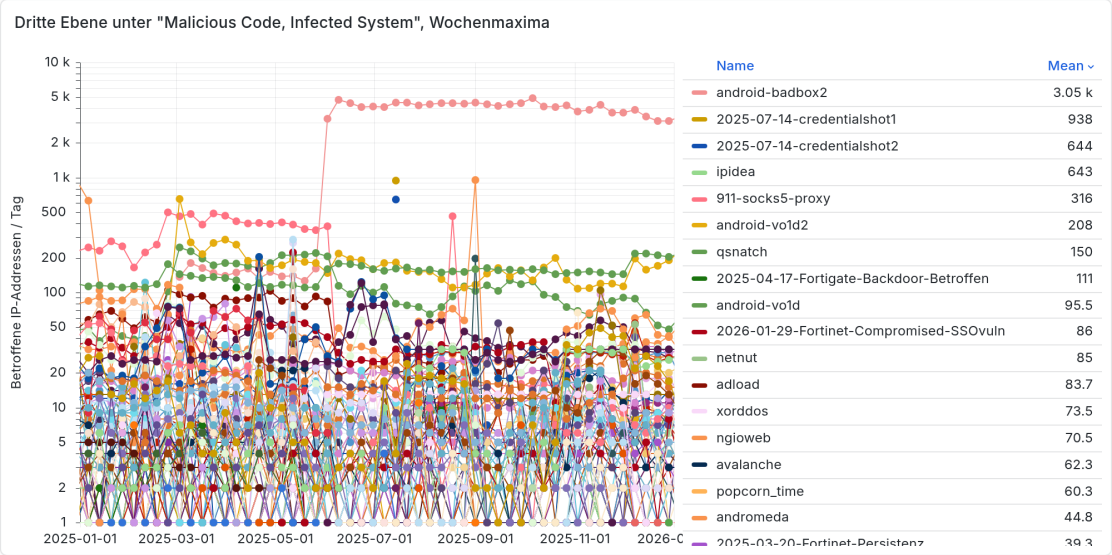


Abbildung 2.17: Verteilung der betroffenen Systeme unter“Infected Systems´´

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 2025 ausgesendet wurden, aufgelistet. Detailbeschreibungen finden sich auf der(CERT.at-Website).

- 7. Jänner 2025: Schwerwiegende Sicherheitslücken in Sonicwall SSL-VPN - aktiv ausgenutzt
- 23. Jänner 2025: Kritische Sicherheitslücke in SonicWall SMA1000 - aktiv ausgenutzt - Update verfügbar
- 4. März 2025: Kritische Sicherheitslücken in VMware ESXi, Workstation und Fusion - aktiv ausgenutzt - Updates verfügba

- 20. März 2025: Ransomware-Gruppen nutzen weiterhin kritische Fortinet-Schwachstellen - Warnung vor gepatchten, aber bereits kompromittierten Geräten
- 26. März 2025: Kritische Sicherheitslücken in Kubernetes Ingress NGINX Controller - Updates verfügbar
- 14. Mai 2025: Ivanti EPMM: Remote Code Execution Schwachstellen (CVE-2025-4427, CVE-2025-4428) - Updates verfügbar
- 12. Juni 2025: Phishing-Angriffe mit manipulierten SVG-Dateien - Vorsicht geboten
- 9. Juli 2025: Kritische Sicherheitslücke CVE-2025-47981 in Windows SPNEGO - Update dringend empfohlen
- 21. Juli 2025: Kritische Sicherheitslücke in Microsoft SharePoint - aktiv ausgenützt, Updates verfügbar
- 5. August 2025: Erhöhte Bedrohungsaktivität gegen SonicWall Gen 7 Firewalls mit SSLVPN - Sofortmaßnahmen empfohlen
- 26. August 2025: Mehrere (teils kritische) Schwachstellen in NetScaler ADC and NetScaler Gateway
- 6. Oktober 2025: Schwerwiegende Sicherheitslücke in Oracle E-Business Suite - aktiv ausgenutzt - Updates verfügbar
- 24. Oktober 2025: Angriffe gegen Microsoft WSUS Installationen - Update verfügbar
- 5. Dezember 2025: React2Shell - Angriffe gegen verwundbare Anwendungen auf Basis React.JS und weiterer Frameworks
- 19. Dezember 2025: Kritische Sicherheitslücken in mehreren Fortinet-Produkten (FortiCloud SSO) - aktiv ausgenutzt - 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 2025 als ”Aktuelles” ausgesendet wurden, aufgelistet. Detailbeschreibungen finden sich auf der(CERT.at-Website).

- 9. Jänner 2025: Aktive Ausnutzung einer schwerwiegenden Sicherheitslücke in Ivanti Connect Secure VPN
- 18. Februar 2025: Ransomware nutzt Sicherheitslücke in FortiOS/FortiProxy Management-Interfaces

- 5. März 2025: Text-basiertes QR Code Phishing im Umlauf
- 9. April 2025: Microsoft-Patchday behebt aktiv ausgenutzte Sicherheitslücke
- 6. Juni 2025: DDoS-Angriffe auf österreichische Unternehmen und Organisationen
- 13. Juni 2025: Selenskyj kommt am 16. Juni nach Wien
- 23. Juni 2025: Auswirkungen des militärischen Konfliktes zwischen Israel und dem Iran auf Österreich
- 8. Juli 2025: Aktiv ausgenutzte Schwachstellen in Citrix NetScaler ADC und NetScaler Gateway
- 25. Juli 2025: Angriffe gegen Citrix Netscaler CVE-2025-6543
- 9. September 2025: Populäre JavaScript Pakete manipuliert
- 7. Oktober 2025: Kritische Redis Sicherheitslücke (CVE-2025-49844) erlaubt Authenticated Remote Code Execution
- 20. Oktober 2025: SAP behebt schwerwiegende Sicherheitslücken in mehreren Produkten
- 5. November 2025: Aktuelle Phishingwelle im Namen von FinanzOnline
- 17. November 2025: Kritische Sicherheitslücke in Fortinet FortiWeb wird aktiv ausgenutzt
- 3. Dezember 2025: Schwerwiegende Sicherheitslücke in React und Next.js
- 18. Dezember 2025: Kritische Zero-Day-Lücke in Cisco Secure Email-Lösungen aktiv ausgenutzt
- 29. Dezember 2025: Schwerwiegende Sicherheitslücke in MongoDB (”MongoBleed”)

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. Sie sind nicht nur notwenig, um einen Überblick zur Lage in Österreich und den staatlichen Institutionen zu haben, sondern dienen dem noch wichtigeren Zweck, Betroffene schnell über Probleme zu informieren, damit diese behoben werden können.

Die Daten werden einerseits von CERT.at 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,[5] 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.

2025 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

[5] 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.

Netgear Router mit kritischen Schwachstellen scannt mithilfe der Suchmaschine shodan.io nach Netgear Geräten in Österreich gesucht, die aus dem öffentlichen Internet erreichbar sind und über die Modell- und Versionsnummer versuchen, potentiell betroffene Geräte zu identifizieren.

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.

UPnP Devices auf Port 1900 ist ein Test auf Devices, die auf Port 1900 öffentlich erreichbar sind, auf eine noch nicht veröffentlichte Schwachstelle

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 informiert 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, erhält CERT.at 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 wichtigste davon ist die Shadowserver Foundation, die überwiegend im Bereich der Analyse von Botnetzen und Malware arbeitet. Dazu wurde ein riesiges Netzwerk aus Honeypots[6] 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 2.4.2) führen.

Zusätzlich arbeitet CERT.at 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[7] 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.

[6] 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 und Betreiber aufgezeichnet und anschließend analysiert.

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

Kommerzielle IT-Firmen

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

Suchmaschinen und Archive

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

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, Sicherheitsforscherinnen und -forscher 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 setzt 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[8] 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 und Betreiber 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 2025

Im Jahr 2025 wurden die Entwicklungsarbeiten konsequent weitergeführt und führten zu mehreren Releases, die sowohl Stabilitätsverbesserungen als auch neue Funktionen mit sich brachten. 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.

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

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

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.

2025 wurde diese Funktion 28 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[9] 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 betreibt eine MISP-Instanz welche auch durch die weiteren sektoralen CERTs (AHC, AEC, GovCERT) zum Informationsaustausch genutzt wird.[10] Darüber hinaus betreut CERT.at, als Betreiber des sektorspezifischen CERT für den Energiesektor (Austrian Energy CERT) eine geschlossene Instanz zum Austausch von Bedrohungsinformationen innerhalb der Energiebranche.

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

Im Jahr 2025 hat sich die Verflechtung von Geopolitik und Cybersicherheit weiter verstärkt. Der Cyberraum entwickelt sich zunehmend von einer primär technischen Domäne zu einem eigen-

[9] 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.

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

ständigen Handlungsfeld internationaler Machtpolitik. Damit stellt er nicht mehr ausschließlich eine technologische Herausforderung dar und Cyberangriffe sind längst nicht mehr ausschließlich als kriminelle Einzelphänomene zu verstehen. Vielmehr wird Cybersicherheit von vielen Staaten zunehmend als legitimer Bestandteil nationaler Sicherheits- und Verteidungsstrategien betrachtet.

Insbesondere geopolitische Rivalitäten und Konflikte zwischen Staaten haben die Bedrohung im Cyberraum maßgeblich beeinflusst. Der russische Angriffskrieg in der Ukraine verdeutlicht exemplarisch, wie Cyberoperationen als Bestandteil der Konfliktführung eingesetzt werden. Staatliche und staatlich unterstützte Akteure nutzen digitale Angriffe zur Spionage, zur Beeinträchtigung nationaler Infrastruktur sowie zur Unterstützung militärischer und politischer Zielsetzungen. Dementsprechend verschwimmen die Grenzen zwischen klassischer und kinetischer Kriegsführung, nachrichtendienstlicher Informationsgewinnung und Konflikten auf politischer Ebene immer weiter – wie Angriffe auf Einrichtungen der Europäischen Union sowie nationale Behörden und Betreiber kritischer Infrastrukturen außerhalb der Ukraine sehr deutlich zeigen.

Parallel dazu gewann das Thema der sogenannten digitalen Souveränität an strategischer Bedeutung, auch in Österreich. Die Abhängigkeit von ausländischen Technologieunternehmen, Cloud-Betreibern, Halbleiterherstellern und globalen Lieferketten wird von Staaten zunehmend als potentielles Risiko für die nationale Sicherheit wahrgenommen, da diese im Krisenfall potentiell als Hebel geopolitischer Einflussnahme genutzt werden könnten. Dies führte erstmalig zu ernsthaften Bemühungen, technologische Abhängigkeiten zu reduzieren und nationale beziehungsweise regionale Kapazitäten im Bereich der Informations- und Kommunikationstechnologien auf- oder auszubauen.

Darüber hinaus beeinflussen geopolitische Spannungen auch die Aktivitäten nichtstaatlicher Akteure. Hacktivistische Gruppierungen und cyberkriminelle Organisationen nutzten politische Konflikte als Rahmen oder Deckmantel zur Durchführung von Überlastungsangriffen, Erpressung durch Ransomware oder andere Formen der digitalen Einflussnahme, häufig mit explizitem Bezug zu internationalen Konflikten oder ideologischen Positionierungen.

Ebenfalls entwickelt sich die Attribuierung von Cyberangriffen im geopolitischen Kontext selbst zu einem politischen Instrument. Die öffentliche Zuschreibung von Angriffen an bestimmte Akteure oder Staaten dient nicht nur der technischen Aufklärung, sondern auch der diplomatischen Positionierung und Legitimation von Gegenmaßnahmen wie Sanktionen durch internationale Organisationen.

Insgesamt zeigt sich, dass Cybersicherheit als integraler Bestandteil geopolitischer Strategien verstanden werden muss, die Grenze zwischen technischer Cyberabwehr und klassischer Außenpolitik verschwimmt. Die fortschreitende Digitalisierung von Gesellschaften, wirtschaftlichen Prozessen und kritischen Infrastrukturen erhöht die strategische Bedeutung des Cyberraums wie nie zuvor. Auch Österreich steht daher vor der Herausforderung, technologische Resilienz, internationale Kooperation und nationale Sicherheitsinteressen miteinander zu verbinden.

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. Nachdem schon 2024 die Hardware-Lieferketten vermehrt in den Fokus geraten sind, hat sich der Trend 2025 weiter fortgesetzt. Nicht zuletzt durch den Ausblick auf regulatorische Vorgaben wie den Cyber Resilience Act und NIS 2 oder die bereits erfolgte Umsetzung von DORA. Dabei geht es nicht ausschließlich um Cyberangriffe auf Komponenten, sondern auch potentielle Mangellagen bei Hardware, wie z.B. bei Computerchips, die für KI-Anwendungen benötigt werden. Dies veränderte einerseits die strategische Planung aber auch die Bewertung von Risiken in Bezug auf Unterbrechungen der Lieferketten.

Attacken auf Software-Repositories oder Update-Server sind auch 2025 bedrohlich geblieben und zeigen die Verwundbarkeit unserer weltweit verteilten Arbeitsweise. 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.

Eine 2025 neue Bedrohung entstand durch die vermehrte Nutzung von KI für die Erstellung von Angriffswerkzeugen und die Manipulation von breit genutzter Software (siehe auch Kapitel 2.7.3). Die Nutzung von Informationen aus kompromittierten Lieferantenunternehmen, um deren Kunden mit Deep Fakes, Voice-Phishing und anderen, grundsätzlich bekannten Techniken anzugreifen, hat durch die KI zugenommen und wird immer schwieriger abwehrbar (siehe auch Kapitel 2.7.5).

Da mit Ende 2025 feststand, dass NIS 2 ab 1. Oktober 2026 in Österreich in Kraft treten wird, wird auch außerhalb des Finanzsektors (der mit DORA bereits Vorgaben in Bezug auf Lieferantensicherheit hat) der Druck erhöht. Gleichzeitig tritt mit 11. September 2026 der Cyber Resilience Act in Kraft, der Meldepflichten beim Fund von Schwachstellen mit sich bringt. In diesem Zusammenhang sollte es also spätestens 2027 möglich sein, die Wirksamkeit dieser Regularien auf Lieferketten zu bewerten.

Von CERT.at-Seite zeigt sich der Angriff auf Lieferketten primär aus der Schwachstellensicht. Und hier hatten wir auch wieder viel mit Schwachstellen bei Sicherheitsprodukten zu tun (siehe Kapitel 2.4.4). Die große Herausforderung bleibt, dass Supply-Chain-Angriffe zwar (bisher) 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.

2.7.2 Regulatorische Entwicklungen

2025 zeichnete sich regulatorisch insbesondere durch das Inkrafttreten von DORA mit 17. Jänner 2025 und den Beschluss des NISG 2026, der österreichischen Umsetzung von NIS 2, aus.

NISG 2026

Das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) wurde kurz vor Jahresende 2025 beschlossen und tritt damit ab 1. Oktober 2026 in Kraft. Es zielt auf einen größeren Kreis von Unternehmen und Organisationen ab als NIS 1, darunter öffentliche Verwaltungen, digitale Dienste, Abfallwirtschaft oder die Herstellung von Medikamenten. Eine wesentliche Neuerung sind verschärfte Meldepflichten. Unternehmen müssen sicherheitsrelevante Vorfälle binnen strenger Fristen melden und können bei Verstößen gegen die gesetzlichen Verpflichtungen mit hohen Bußgeldern rechnen.

Aus CERT.at-Sicht ergibt sich damit eine Vielzahl an Änderungen und neuen Aufgaben. Insbesondere das für NISG 2026 neu zu schaffende Bundesamt für Cybersicherheit (das auch Aufsichtsaufgaben über die CERTs erhält), erhöhte Berichtspflichten, eine wesentlich höhere Anzahl an betroffenen Unternehmen und die Rolle von CERT.at als Coordinated Vulnerability Coordinator (für NISG 2026 und CRA) machen eine teilweise Neustrukturierung, in jedem Fall aber eine Erweiterung von CERT.at notwendig.

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.

DORA ist mit 16. Jänner 2023 formal in Kraft getreten und nach einer zweijährigen Übergangsphase verbindlich seit 17. Jänner 2025 anzuwenden. Da es sich um eine Verordnung handelt, war es nicht notwendig, DORA in nationales Recht umzuwandeln. Für Finanzinstitute erhöhte sich seitdem u.a. die Verpflichtung zur Prüfung und Überwachung von Dienstleistern, die Pflicht zu regelmäßigen Penetration Tests und die Umsetzung von Mindeststandards für Business Continuity, Disaster Recovery und Risikoanalysen.

Aus DORA ergeben sich auch Meldepflichten bei Cybervorfällen, wobei die Meldungen an die Finanzmarktaufsicht erfolgen und damit nicht über das nationale CERT (CERT.at ist aber als nationales CERT - und weil es kein eigenes Finanz-CERT gibt - weiterhin auch das nationale CERT des Finanzsektors).

Mit Jahresende 2025 zeigte sich, dass der Finanzsektor DORA erfolgreich umsetzen konnte und dass bereits einige Lektionen aus dieser Umsetzung in die Diskussionen rund um NISG 2026 eingeflossen sind.

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 be-

reitstellen.

Mit dem CRA will die EU-Kommission durchgängige Sicherheitsstandards schaffen, um Manipulationen oder Datenabflüsse über vernetzte Geräte zu verhindern. Angesichts der rasanten Ausbreitung des Internet 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.

Für CERT.at bedeutet die Umsetzung des CRA ab 11. September 2026, dass Meldungen über ausgenutzte Schwachstellen von den betroffenen Unternehmen über eine Single Reporting Platfom der ENISA an die nationalen CERTs (CSIRTs) gesendet werden müssen, die diese wiederum als Warnungen oder im Rahmen einer Coordinated Vulnerability Disclosure an relevante Akteure weitergeben. Wie die Umsetzung auf technischer Ebene erfolgen wird, war Ende 2025 noch nicht absehbar.

Ausblick und Herausforderungen

Der Ausblick auf 2026 zeichnet sich vor allem durch die Umsetzung von NIS 2 und CRA aus, die voraussichtlich auch bis 2026 noch nicht alle Effekte dieser Regulierung zeigen werden. Erst 2027 wird sich wirklich zeigen, was von diesen Vorgaben die Cybersicherheit tatsächlich erhöht und vor allem, wie die jeweiligen EU-Mitgliedsstaaten diese Regularien tatsächlich umsetzen. Für CERT.at wird 2026 in jedem Fall ein sehr entscheidendes Jahr, da insbesondere NISG 2026 viele neue Aufgaben bringt, während gleichzeitig unklar ist, wie viele Unternehmen diese auch tatsächlich abrufen werden.

2.7.3 Künstliche Intelligenz

Große Sprachmodelle (LLMs, Large Language Models) haben sich im Jahr 2025 von reinen Text- und Analysewerkzeugen zu sogenannten agentischen Systemen weiterentwickelt: KI-Agenten, die selbstständig Werkzeuge bedienen, Code ausführen, im Web recherchieren und mehrstufige Aufgaben über längere Zeiträume hinweg abarbeiten. Standardisierte Schnittstellen wie das Model Context Protocol (MCP) haben die Anbindung solcher Agenten an E-Mail-Systeme, Ticketsysteme, Entwicklungsumgebungen und Fachanwendungen massiv vereinfacht. Damit ist KI endgültig in den operativen IT-Betrieb eingezogen – und mit ihr eine neue Angriffsfläche. Regulatorisch relevant ist, dass seit August 2025 die Pflichten des EU AI Act für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (GPAI) gelten.

Auf der Verteidigungsseite halten LLMs zunehmend Einzug in Security Operations Center: Sie übernehmen die Vorqualifizierung von Alarmen, fassen Vorfälle zusammen, unterstützen bei der Malware-Analyse und beschleunigen das Verfassen von Advisories und Berichten. Bemerkenswert sind die Fortschritte in der automatisierten Schwachstellensuche – KI-Systeme wie Googles ”Big Sleep” fanden 2025 erstmals reale, teils bereits von Angreifern ins Visier genommene Schwachstellen in weit verbreiteter Software, und KI-gestützte Pentesting-Plattformen erreichten Spitzenplätze in Bug-Bounty-Programmen. Für den Umgang mit sensiblen Daten setzen viele Organisationen zunehmend auf lokal betriebene Open-Weight-Modelle, um Vertraulichkeitsanforderungen zu erfüllen.

Auf der Angriffsseite markiert 2025 einen Wendepunkt: Erstmals wurden Kampagnen dokumentiert, in denen KI nicht nur einzelne Schritte unterstützte, sondern den Großteil des Angriffszyklus selbst durchführte. Im August 2025 beschrieb Anthropic eine Erpressungskampagne, bei der ein einzelner Akteur mithilfe eines agentischen Coding-Tools rund 17 Organisationen kompromittierte – von der Aufklärung über die Datenexfiltration bis zur Berechnung der Lösegeldforderungen. Im November 2025 folgte der Bericht über eine mutmaßlich staatlich unterstützte chinesische Gruppe, die eine Spionagekampagne gegen rund 30 Ziele zu einem Großteil autonom von KI-Agenten ausführen ließ. Parallel tauchte Schadsoftware auf, die LLMs zur Laufzeit einbindet: Der Proof-of-Concept "PromptLock" demonstrierte KI-generierte Ransomware-Logik, und Google dokumentierte Malware-Familien, die über APIs dynamisch neuen Schadcode generieren oder sich selbst umschreiben, um Erkennung zu erschweren. Phishing-Mails, Deepfake-Audio und -Video in täuschend echter Qualität sind inzwischen Massenware und in praktisch jeder Sprache verfügbar.

Mit der Verbreitung von KI-Agenten ist zugleich eine neue Schwachstellenklasse in den Mittelpunkt gerückt: die indirekte Prompt Injection. Dabei werden Anweisungen nicht vom Benutzer, sondern in verarbeiteten Inhalten – etwa E-Mails, Dokumenten oder Webseiten – versteckt und vom Modell ausgeführt. Dass dies keine theoretische Gefahr ist, zeigte die Zero-Click-Schwachstelle "EchoLeak" (CVE-2025-32711) in Microsoft 365 Copilot, über die allein durch den Empfang einer präparierten E-Mail Daten abfließen konnten. Je mehr Berechtigungen und Werkzeugzugriffe ein Agent besitzt, desto größer der potenzielle Schaden. Hinzu kommen Lieferkettenrisiken durch unzureichend geprüfte MCP-Server und Erweiterungen sowie das anhaltende Problem der "Schatten-KI": Beschäftigte, die vertrauliche Unternehmensdaten in nicht freigegebene KI-Dienste eingeben.

Insgesamt hat sich die Schere zwischen Chancen und Risiken 2025 weiter geöffnet – vor allem aber hat sich das Tempo erhöht. Die Zeitspanne zwischen Veröffentlichung einer Schwachstelle und ihrer Ausnutzung schrumpft, wenn Angreifer Exploits KI-gestützt entwickeln; umgekehrt können Verteidiger Erkennung, Analyse und Patching nur dann Schritt halten lassen, wenn sie dieselben Werkzeuge einsetzen. Organisationen sind daher gut beraten, KI-Nutzung nicht nur über Richtlinien, sondern über technische Kontrollen abzusichern: klare Berechtigungskonzepte für Agenten, Absicherung gegen Prompt Injection, Protokollierung von KI-Interaktionen und die Bewertung von KI-Komponenten als Teil der eigenen Angriffsfläche. Frameworks wie die OWASP Top 10 für LLM-Anwendungen sowie die schrittweise greifenden Vorgaben des AI Act bieten dafür erste Orientierung.

2.7.4 Angriffe auf kritische Infrastruktur

Kritische Infrastrukturen und wesentliche Dienste blieben auch 2025 ein attraktives Ziel für unterschiedliche Bedrohungsakteure. Dabei zeigte sich erneut, dass sich die Motivation der Angreifer stark unterscheidet: Neben finanziell motivierter Cyberkriminalität spielen staatliche und staatsnahe Akteure sowie hacktivistische Gruppen eine wichtige Rolle. Insbesondere geopolitische Konflikte wirken sich zunehmend unmittelbar auf die Auswahl von Angriffszielen im Cyberraum aus.

Die europäische Bedrohungslage bestätigt dieses Bild. ENISA analysierte für seinen Threat Landscape 2025 insgesamt 4.875 Vorfälle aus dem Zeitraum Juli 2024 bis Juni 2025. Besonders häufig

betroffen war die öffentliche Verwaltung, die 38 Prozent der erfassten Vorfälle ausmachte. Bei staatlich beziehungsweise staatsnah ausgerichteten Aktivitäten gehörten neben der öffentlichen Verwaltung insbesondere Verkehr, digitale Infrastruktur, Energie und Gesundheit zu den am häufigsten adressierten Sektoren. Fast alle EU-Mitgliedstaaten waren von solchen Aktivitäten betroffen.

Ein wesentliches Angriffsmittel blieben 2025 Distributed-Denial-of-Service-Angriffe (DDoS). Dabei geht es den Täterinnen und Tätern häufig weniger darum, dauerhaft in Systeme einzudringen, sondern öffentlich sichtbare Dienste vorübergehend unerreichbar zu machen. Solche Angriffe eignen sich daher besonders für hacktivistische Gruppen, die mit vergleichsweise geringem Aufwand Aufmerksamkeit erzeugen oder politische Botschaften transportieren wollen. ENISA stellte 2025 insbesondere bei Angriffen gegen öffentliche Verwaltungen einen starken Zusammenhang zwischen geopolitischen Entwicklungen, Hacktivismus und DDoS-Aktivitäten fest.

Auch Österreich war davon betroffen. Im Juni 2025 erreichten CERT.at vermehrt Meldungen über DDoS-Angriffe gegen österreichische Unternehmen und Organisationen. Die Ziele stammten aus unterschiedlichen Bereichen und Sektoren; ein eindeutiger Schwerpunkt war nicht erkennbar. Bei einem Teil der Angriffe gab es Hinweise auf finanzielle Motivation, gleichzeitig waren offenbar mehrere Tätergruppen aktiv. CERT.at empfahl den betroffenen Organisationen insbesondere, die Wirksamkeit bestehender DDoS-Schutzmaßnahmen und die Zusammenarbeit mit ihren Internet Service Providern zu überprüfen.

Wie eng Cyberangriffe inzwischen mit geopolitischen Ereignissen verbunden sind, zeigte sich auch während des militärischen Konflikts zwischen Israel und dem Iran im Juni 2025. Internationale Beobachtungen zeigten eine deutliche Zunahme hacktivistischer Aktivitäten, insbesondere DDoS-Angriffe und Webseiten-Defacements. Für Österreich waren zu diesem Zeitpunkt zwar keine direkten Auswirkungen bekannt, CERT.at wies jedoch darauf hin, dass eine Ausweitung auf europäische oder österreichische Ziele ebenso möglich war wie indirekte Auswirkungen über Geschäftspartner und digitale Abhängigkeiten.

Dass die Auswirkungen von Störungen in kritischen Infrastrukturen weit über das unmittelbar betroffene System hinausreichen können, bleibt dabei eine zentrale Herausforderung. Digitale Abhängigkeiten zwischen Unternehmen, Dienstleistern und Infrastrukturen führen dazu, dass ein erfolgreicher Angriff auf einen einzelnen Anbieter auch andere Organisationen oder ganze Sektoren beeinträchtigen kann. ENISA hob 2025 ausdrücklich hervor, dass solche Abhängigkeiten die Auswirkungen von Cyberangriffen verstärken und damit die Resilienz kritischer Dienste zu einer sektorübergreifenden Aufgabe machen.

Aus Sicht von CERT.at bedeutet dies, dass sich der Schutz kritischer Infrastruktur nicht auf einzelne technische Systeme beschränken darf. Neben klassischen Maßnahmen wie Netzwerksegmentierung, sicherer Administration und zeitnahem Patchen internetexponierter Systeme werden belastbare Notfallprozesse, DDoS-Mitigation, Monitoring und vor allem funktionierende Kommunikationswege zwischen Betreibern, Behörden und CERTs zunehmend entscheidend. Gerade bei politisch motivierten Angriffen kann die Vorwarnzeit sehr kurz sein. Die Erfahrungen aus 2025 zeigen daher einmal mehr, dass technische Resilienz und vertrauensbasierte Zusammenarbeit gleichermaßen notwendig sind.

2.7.5 Trends bei Ransomware und Phishing

Ransomware hat sich in den letzten Jahren zu einer der lukrativsten und gleichzeitig bedrohlichsten Formen der Cyberkriminalität entwickelt. Auch 2025 blieb sie eine bedeutende Bedrohung für Unternehmen und öffentliche Einrichtungen. Dabei hat sich die Angriffsmethodik zunehmend von einem klassischen Szenario der Datenverschlüsselung hin zu einer mehrstufigen Angriffskette entwickelt. Neben der Verschlüsselung stehen insbesondere der schnelle Initial Access, die Kompromittierung von Benutzerkonten mit erhöhten Rechten und die Exfiltration sensibler Daten im Mittelpunkt.

Auch der Trend der Double-Extortion nimmt nicht ab. Dabei verschlüsseln die Täter nicht nur die Daten des Opfers, sondern kopieren sie zusätzlich auf eigene Systeme und drohen im Falle einer Zahlungsverweigerung mit deren Veröffentlichung. Neben der Betriebsunterbrechung entstehen dadurch weitere Risiken wie Datenschutzverstöße, Reputationsschäden und rechtliche Konsequenzen. 2025 war Datendiebstahl in einem großen Teil der beobachteten Ransomware-Angriffe Bestandteil der Angriffskette, weshalb die Exfiltration gegenüber der reinen Verschlüsselung weiter an Bedeutung gewinnt.

Eine wesentliche Veränderung betrifft den Initial Access. Die Ausnutzung von Schwachstellen gehörte 2025 zu den wichtigsten Zugangsmethoden. Besonders attraktiv waren öffentlich erreichbare VPNs, Firewalls und andere Edge-Systeme, da deren Kompromittierung einen direkten Zugang zu internen Netzwerken ermöglichen kann. Dabei wurden nicht ausschließlich neue Zero-Day-Schwachstellen verwendet. Auch bereits länger bekannte Sicherheitslücken wurden weiterhin ausgenutzt, wenn Systeme nicht rechtzeitig aktualisiert wurden. Entscheidend ist daher zunehmend die Geschwindigkeit, mit der ein verfügbarer Exploit nach Bekanntwerden einer Schwachstelle eingesetzt wird. Teilweise beginnen Angriffe bereits sehr kurze Zeit nach der öffentlichen Bekanntmachung, wodurch insbesondere für internetexponierte Systeme schnelle Patch-Prozesse erforderlich sind.

Nach dem Initial Access setzen Angreifer verstärkt auf legitime Administrationswerkzeuge und vorhandene Funktionen der Zielsysteme. Dazu gehören unter anderem PowerShell, WMI, Windows-Dienste, Scheduled Tasks, Active Directory und Remote-Management-Software. Diese sogenannte ”Living-off-the-Land”-Vorgehensweise erschwert die Erkennung, da sich die Aktivitäten teilweise kaum von regulären Administrationsvorgängen unterscheiden. Gleichzeitig werden gestohlene Zugangsdaten für den initialen Zugriff, Privilege Escalation und Lateral Movement eingesetzt.

Auch Virtualisierungsplattformen wie VMware ESXi sind attraktiv, da ihre Kompromittierung zahlreiche virtuelle Maschinen gleichzeitig beeinträchtigen kann. Weiterhin versuchen Angreifer, neben Active Directory auch Backup-Systeme zu kompromittieren oder Wiederherstellungsmöglichkeiten zu beseitigen. Zwischen Initial Access, Ausbreitung im Firmennetzwerk, Datendiebstahl und Verschlüsselung können dabei teilweise nur noch wenige Stunden liegen. Ransomware ist daher zunehmend als Teil einer auf Geschwindigkeit und Automatisierung optimierten Angriffskette zu verstehen.

Auch Phishing hat 2025 weiter an Raffinesse gewonnen. Neben klassischen E-Mail-Kampagnen werden gezielte Spear-Phishing-Angriffe, sogenannte ”Adversary-in-the-Middle” (AiTM)-Angriffe und Device-Code-Phishing eingesetzt. Diese Verfahren zielen unter anderem darauf ab, Zugangsdaten und Session-Tokens zu stehlen und dadurch herkömmliche Multifaktor-Authentifizierung

zu umgehen. Zusätzlich erleichtert generative KI die Erstellung glaubwürdiger und personalisierter Nachrichten. Auch Smishing und Vishing bleiben relevante Angriffsformen.

Aufgrund dieser Entwicklungen müssen Unternehmen ihre Schutzmaßnahmen stärker auf die gesamte Angriffskette ausrichten. Insbesondere ein schnelles Vulnerability Management für internetexponierte Systeme, der Schutz privilegierter Benutzerkonten sowie die Überwachung von VPN-, Active-Directory- und Virtualisierungsinfrastrukturen sind daher zu priorisieren. Phishingresistente Authentifizierungsverfahren können zusätzlich dazu beitragen, moderne Phishing-Techniken abzuwehren.

Das Jahr 2025 zeigt damit vor allem eine weiterhin steigende Professionalisierung von Ransomware und Phishing. Bekannte ”Tactics, Techniques, and Procedures” (TTPs) werden effizienter kombiniert, automatisiert und schneller eingesetzt. Entscheidend ist daher nicht erst die Erkennung der eigentlichen Ransomware, sondern die möglichst frühe Unterbrechung der Angriffskette.

2.8 Hilfe bei Vorfällen

Auch wenn die Hauptaufgabe von CERT.at darin besteht, als Informationsdrehscheibe potentiell Betroffene vor Angriffswellen zu warnen, bevor diese aufschlagen, gibt es Fälle, die eine speziellere Behandlung erfordern. In solchen Fällen unterstützen wir Betroffene sowohl mit unserem Fachwissen und unserer Erfahrung, als auch bei der Koordination der Zusammenarbeit mit den relevanten staatlichen Stellen.

2.8.1 Verhinderung der Ausnutzung von Schwachstellen

Der arbeitsintensivste Teil der CERT.at-Tätigkeiten ist die Warnung vor Gefahren und Bedrohungen durch Schwachstellen. CERT.at erhält täglich eine Vielzahl an Datensätzen nationaler und internationaler Partner sowie durch eigene Scans, die auf mögliche oder bereits ausgenutzte Schwachstellen hinweisen. Durch direkte (wo Kontaktdaten bekannt sind) und indirekte (meistens über ISPs) Kontaktaufnahmen werden die betroffenen Organisationen sehr oft noch vor einem tatsächlichen Angriff gewarnt. Wenn ein Angriff bereits im Gange ist, versucht CERT.at die Organisation auch telefonisch zu kontaktieren - eine nicht immer einfache Aufgabe, insbesondere wenn dies am Wochenende oder an Feiertagen notwendig ist.

2.8.2 DDoS gegen österreichische Ziele

Ähnlich wie bereits in den vergangenen Jahren kam es auch 2025 zu einer Reihe von DDoS-Angriffen (siehe Kapitel 2.4.5 die Aussendung vom 6. Juni 2025), bei denen erneut eine breite Palette von österreichischen Organisationen betroffen war, darunter öffentliche Einrichtungen und Betreiber kritischer Infrastrukturen, die ins Visier genommen wurden. Die tatsächliche Bedrohung durch solche Angriffe nimmt aber zumindest auf der gesamtstaatlichen Ebene ab, da viele Organisationen bereits Gegenmaßnahmen ergriffen haben. Die meisten betroffenen Or-

ganisationen 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. Wo möglich beobachtet CERT.at Drohungen gegen Unternehmen und erste Anzeichen für DDoS-Angriffe, um die betroffenen Organisationen zu warnen. 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.

2.8.3 Unterstützung bei Ransomware-Vorfällen

Ransomware war auch 2025 ein für die Angreifer erfolgreiches Geschäftsmodell. Das Ziel bleibt stets dasselbe: die Verschlüsselung geschäftskritischer Daten, um Druck auf die betroffenen Organisationen auszuüben und hohe Lösegeldsummen zu fordern. Der Trend, dass größere Unternehmen weniger oft Opfer von Ransomwareangriffen werden, setzte sich auch 2025 fort: die CERT.at gemeldeten Vorfälle betrafen meistens kleine und mittelgroße Unternehmen, die keine oder unzureichende Schutzmaßnahmen gegen Ransomwareangriffe getroffen hatten.

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 hat CERT.at 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 versteht seine Aufgabe als Dienstleistung für die gesamte österreichische Gesellschaft. Jede Bürgerin und jeder Bürger profitiert letztlich von dieser Arbeit – das „Produkt“ ist Sicherheit im Netz. Da es jedoch nicht möglich ist, jede einzelne Person direkt zu erreichen, setzen wir 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 der täglichen Arbeit ist aktives Community-Management. Wir 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. Durch diese kontinuierliche Vernetzungsarbeit wird die Zusammenarbeit zwischen relevanten Akteurinnen und Akteuren aus Wirtschaft, Forschung und Verwaltung in Österreich gestärkt.

Gleichzeitig sind wir international gut vernetzte und anerkannte Partner für ausländische CERTs und CSIRTs. Der Austausch mit internationalen Expertinnen und Experten ermöglicht es, globale

Trends in der Cybersicherheit frühzeitig zu erkennen und gemeinsam Lösungen zu entwickeln.

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 Innenministerium, die den sicheren und vertrauensvollen Austausch von sicherheitsrelevanten Informationen zwischen Unternehmen und Behörden fördert. Er besteht aus sieben ”Security Information Exchanges”: Industry, Energy, Health, Transportation, ISP, Finance und Government. Primäres Ziel ist es, eine enge Vernetzung innerhalb und zwischen kritischen Sektoren zu ermöglichen.

Durch den Austrian Trust Circle entstand eine Veranstaltungsreihe, in der Unternehmen nicht nur wertvolle Einblicke in aktuelle Bedrohungslagen erhalten, sondern auch voneinander lernen können. Gleichzeitig baut CERT.at durch den ATC Verbindungen zu operativen Kontakten in verschiedenen Organisationen auf und kann so besser nachvollziehen, wie und durch wen reale Sicherheitsvorfälle behandelt und bewältigt werden.

Der Austrian Trust Circle ist damit ein zentrales Netzwerk der österreichischen IKT-Sicherheit. Er stärkt das gegenseitige Vertrauen zwischen Akteurinnen und Akteuren 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 und Behörden 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 Cybersicherheitsstrategie.

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 Laufe des Jahres 2025 fanden 6 Treffen physisch statt. Mit Stand Ende 2025 nehmen 19 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 Koordinationsstruktur” (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 bekamen 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.

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

3.2.4 Sektoren-CERTs

3.2.5 Government CERT - GovCERT

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 seit April 2025 vom Bundesministerium für Inneres (BMI) verantwortet[1] 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

[1] Bis April 2025 wurde das GovCERT durch das Bundeskanzleramt betrieben. Durch eine Neuordnung der ministeriellen Zuständigkeiten nach der Nationalratswahl 2024 wurden die meisten Cybersecurity-Aufgaben des Bundes im BMI zusammengefasst. CERT.at unterstützt das GovCERT bei operativen Tätigkeiten und mit Infrastruktur.

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.

3.2.6 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/.

3.2.7 Austrian Health CERT - AHC

Das Austrian HealthCERT, kurz AHC, wurde durch einen Beschluss der Bundes-Zielsteuerungskommission, einem Gremium aus Vertreter:innen des Bundes, der Sozialversicherung und der Länder, zur Stärkung der IT-Sicherheitskompetenzen im Gesundheitssektor gegründet und als sektorenspezifisches CERT gemäß § 14 NISG benannt.

Durch eine intensive Vernetzung und die Funktion als Informationsdrehscheibe für Stakeholder aus dem Gesundheitsbereich stärkt es die Resilienz der Informations- und Kommunikations-Systeme im Gesundheitssektor. Informationen werden in Form von Lagebildern, Warnungen und Alarmierungen sowie davon abgeleiteten Handlungsempfehlungen und Best-Practice Ansätzen zur Verfügung gestellt.

Als sektorenspezifisches CERT wurde das Austrian HealthCERT zudem als Single Point of Contact (SPoC) für Betreiber wesentlicher Dienste und kritischer Infrastruktur aus dem Gesundheitssektor eingerichtet.

3.2.8 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.

3.3 Vernetzung auf internationaler Ebene

Neben der Zusammenarbeit innerhalb Österreichs, kooperiert CERT.at 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[2] 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.

[2] 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 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.

4.1.1 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. Diese Idee wurde im EU Cyber Solidarity Act formalisiert, dieser trat im Jänner 2025 in Kraft.

ENSOC ist ein Konsortium von Cybersicherheitsagenturen aus mehreren EU Mitgliedstaaten unter der Leitung von CCN-CERT, dem für die öffentliche Verwaltung zuständigen 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 offizielle Mitglied Österreichs das Innenministerium und CERT.at tritt nur als Subcontractor auf.

Die Finanzierung der EU für dieses Projekt ist zum Teil als gemeinsamer Einkauf des Konsortiums mit dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung (ECCC) organisiert. Der daraus folgende Formalismus (Ausschreibung mit zweistuftigem Verfahren) über sechs Staaten und einer EU-Agentur mit all den rechtlichen Rahmenbedingungen hat dazu geführt, dass sich 2025 der Beitrag von CERT.at auf geringfügige Hilfestellungen bei der Abwicklung dieses Einkaufs beschränkt hat.