CERT.at

ZUKUNFT GESTALTEN
Industriellenvereinigung

iv

IT-SECURITY VORFÄLLE

VORBEREITUNG UND ANSPRECHSTELLEN

IT-SECURITY

Internetkriminalität und Cyberattacken haben in den vergangenen Jahren massiv zugenommen. Die Bedrohung für Unternehmen in Österreichs Industrie und den mit ihr verbundenen Sektoren ist real und richtet jährlich Schäden in Millionenhöhe an. Dabei richten sich Attacken vor allem gegen Betriebe, deren Produkte und Dienstleistungen zu den innovativsten und qualitativ höchstwertigsten zählen. Umso wichtiger ist es, den Industrie- und Wirtschaftsstandort stärker zu schützen sowie Unternehmen zu unterstützen.

Was sind Cyberattacken? Welche Leitlinien gibt es, um sich darauf vorzubereiten? Was ist im Fall konkreter Angriffssituationen zu beachten? Welche Stellen bieten im Fall der Fälle welche Unterstützungsleistungen an? Die Industriellenvereinigung hat sich mit Expertinnen und Experten sowie Unternehmen intensiv ausgetauscht – und Empfehlungen, wissenswerte Informationen und relevante Kontaktstellen zusammengetragen, die Sie hier bzw. unter www.iv.at/cybersicherheit vorfinden.

1. CYBERANGRIFF: VORBEREITUNG AUF DEN ERNSTFALL

Wenn von einem IT-Security oder einem Cybersecurity Vorfall oder Angriff die Rede ist, dann versteht man darunter in der Regel, dass ein IT-System (Computer, Server, Smartphone, Router, etc.) durch eine Schadsoftware oder einen menschlichen Angreifer bewusst und absichtlich gestört wird. Ob es sich nun um eine Schadsoftware handelt, die Daten löscht, verschlüsselt oder kopiert, oder um einen Hacker, der auf der Suche nach für ihn relevanten Information ist: es ist **ein absichtlicher Angriff und kein technischer Defekt**.

Der wesentliche Unterschied ist dabei, dass ein technischer Defekt nicht auf Gegenmaßnahmen reagieren wird. Ein menschlicher Angreifer wird Gegenmaßnahmen aber erkennen und darauf mit einem neuen Angriff, eventuell aus einer anderen Richtung, kontern. In diesem Sinne muss jede Vorbereitung auf einen Angriff immer berücksichtigen, dass eine **einzelne Schutzmaßnahme nicht ausreicht** und dass **jede offene Schwachstelle potentiell ausgenutzt** werden wird. Bei Cyberangriffen ist nicht der Zufall der Gegner, sondern ein menschliches Wesen mit kriminellen Absichten.

Vorbereitung auf die Abwehr eines Cyberangriff

Die Vorbereitung auf die Abwehr eines Cyberangriffs umfasst **rechtliche, technische und organisatorische Maßnahmen**.

- Die **technischen Maßnahmen** sollten von den in den Unternehmen tätigen IT-Abteilungen bzw. von externen Dienstleistern nach Stand der Technik umgesetzt werden (Detektionssysteme, Asset Management, Logging, Zugriffsregelungen, etc.). Wesentlich ist dabei, insbesondere mit Blick auf die aktuellen Erpressungen mit Ransomware, eine **robuste Datensicherungs- bzw. Backupstrategie**. Das beinhaltet beispielsweise, dass regelmäßig geprüft wird, ob **Datensicherungen auch wieder auf die Systeme zurückgespielt** werden können bzw. dass sie sicher sind vor **Verschlüsselungen bzw. Beschädigung durch Schadsoftware**.

- Eine **organisatorische Vorbereitungsmaßnahme** ist beispielsweise die **Schulung der Mitarbeiter:innen**, damit diese keine Schadsoftware aktivieren, die sie z.B. per Email erhalten haben. Diese Schulungen können **mit eigenem Personal** oder ebenfalls wieder **durch Dienstleister** durchgeführt werden. Als Trainingsmaßnahme bieten Dienstleister z.B. auch **„**Phishing-Tests**“** an, bei denen den Mitarbeiter:innen Nachrichten gesendet werden, die wie echte Phishing-Emails aussehen, die aber ungefährlich sind. Aber auch **Tests der Verwundbarkeit von technischen Systemen** (z.B. Penetration Tests) und **regelmäßige Übungen und Planspiele** verbessern die Vorbereitung und reduzieren die Wiederherstellungszeit nach einem Angriff.

- Eine **weitere organisatorische Maßnahme** ist die **Einrichtung eines Krisenstabes**, der im Fall eines schweren Cybervorfalls aktiviert werden kann. Im Rahmen der Vorbereitungsarbeiten können dabei auch bereits **Texte für Pressemeldungen für unterschiedliche Fälle** erstellt werden, auf die dann im Anlassfall rasch zurückgegriffen werden kann. Insbesondere bei der Vorbereitung auf Ransomware-Vorfälle muss berücksichtigt werden, dass **die wichtigen Unterlagen (Verträge, Support-Nummern, Telefonnummern, etc.) auch in Papierform vorhanden** sind, da digitale Unterlagen, Unterstützungssoftware und Kommunikationsmittel eventuell nicht zu Verfügung stehen, weil sie ebenfalls verschlüsselt wurden.

- Ebenfalls als Vorbereitungsmaßnahme kann der Abschluss einer Versicherung gegen IT-Störungen oder Cyberangriffe gesehen werden. Abhängig von den angebotenen Modellen kompensieren sie Schäden, stellen IT-Dienstleister zur Unterstützung bei Vorfällen bereit oder bezahlen die Rechtsfolgen.

Die aufgelisteten Themen bilden nur einen Teil der möglichen und oft verpflichtenden Maßnahmen ab. Viele dieser Maßnahmen werden mit der Einführung von NIS 2 und DORA (für den Finanzbereich) insbesondere für größere Unternehmen verpflichtend.

2. UNTERSTÜTZUNG IM FALL DER FÄLLE

Das **Knowhow**, das zur Eingrenzung oder Behebung eines solchen bereits laufenden Angriffs notwendig ist, ist sehr speziell und erfordert einerseits eine **entsprechende Fachausbildung** und andererseits (im Idealfall tiefergehendes) **Verständnis über das IT-System**, das gerade angegriffen wird. Damit grenzt sich die Gruppe jener Personen und Organisationen, die auf **solche Angriffe unterstützend reagieren** können von jenen ab, die sich auf die **vorbereitende Absicherung oder den Wiederaufbau nach einem Angriff** fokussieren.

- Die Erwartungshaltung ist sehr oft, dass ein IT-Security Angriff durch einen erfahrenen und gut ausgebildeten Experten innerhalb von kurzer Zeit (Minuten bis Stunden) behoben werden kann. Dieser Eindruck wird beispielsweise durch Spielfilme erweckt, in denen Hackerangriffe oft innerhalb von Minuten oder Sekunden durch rasche Eingabe von Befehlen in ein Terminal gelöst werden. Die Realität ist davon weit entfernt. Die **Prüfung von IT-Systemen** auf auffällige Spuren von Angreifern, das Analysieren von möglicher Schadsoftware oder das Aussperren eines Angreifers aus einem System erfordern (zusätzlich zu dem bereits angesprochenen Knowhow) **viel Zeit, Geduld, Personal und Vorsicht**, damit der Schaden nicht noch vergrößert wird.
- Die beste Unterstützung, die man im Falle eines IT-Security Vorfalls erhalten kann, kommt in der Regel von jemandem, der das **betroffene System sehr gut kennt**. Das ist meistens das **eigene IT-Personal bzw. ein Dienstleister, der im Vorfeld die Möglichkeit hatte, das System kennenzulernen**. Bzw. der es nicht nur kennt, sondern der auch an der **Absicherung des Systems gegen Angriffe und der Einrichtung von Wiederaufbaumaßnahmen** (Backups, Ersatz-Infrastruktur, etc.) beteiligt war.
- Ist ein solcher Dienstleister nicht bereits **vorab vertraglich zur Unterstützung verpflichtet** worden, so muss **auf andere Experten-Pools zugegriffen** werden. Zusätzlich zur individuellen Suche nach einem Dienstleister per Internetsuchmaschine, stehen **diverse Ansprechstellen bei Wirtschaft und Behörden** zu Verfügung, die aber **in unterschiedlichem Ausmaß unterstützen** können. Das betrifft sowohl die fachlichen

Fähigkeiten also auch die zeitliche Verfügbarkeit. Es ist daher in jedem Fall sinnvoll, bereits **vor einem IT-Sicherheitsvorfall Dienstleister zu identifizieren, zu prüfen und ihre Unterstützung vertraglich zu sichern**. Insbesondere wenn mehrere Organisationen gleichzeitig von einem Vorfall betroffen sein sollten, kann es ansonsten sehr schwer werden, geeignete Unterstützung zu finden.

3. ÜBERSICHT: RELEVANTE KONTAKTSTELLEN

Polizei und Bundesministerium für Inneres

- Das Innenministerium hat 2011 im Bundeskriminalamt den Fachbereich **„Cybercrime-Competence-Center C4“** eingerichtet, der sich mit den kriminalpolizeilichen **Aufgaben in der Bekämpfung und Aufklärung von Cybercrime** beschäftigt. Die Expert:innen des C4 kommen aus den Bereichen Ermittlung, Forensik und Technik, sie bilden eine Zentralstelle für die **elektronische Beweismittelsicherung und -auswertung und koordinieren Aktionen im Kampf gegen Cybercrime**. Über eine eMail-Adresse (against-cybercrime@bmi.gv.at) kann die BMI-Meldestelle zur Bekämpfung von Internetkriminalität in einem 24/7-Betrieb erreicht werden. Es können aber **derzeit noch keine Anzeigen** darüber erstattet werden.
- Die Aufgabe des C4 ist die kriminalpolizeiliche Arbeit nach einer Internetstraftat. Das C4 hat damit nicht die Rolle der technischen Unterstützungseinheit vor Ort vor, während oder nach einem IT-Security Vorfall. Es kann aber beispielsweise über seine nationalen und internationalen Kontakte bei der Einschätzung von Tätergruppen helfen (beispielsweise bei der Frage, ob eine bestimmte Gruppe dafür bekannt ist, dass sie bei Erpressungen trotz Zahlung von Lösegeld die verschlüsselten Daten nicht wieder freigibt) oder ob Ermittlungskräfte in anderen Ländern bei vergleichbaren Fällen erfolgreiche Lösungen gefunden haben.
- Das Innenministerium empfiehlt bei IT-Security Vorfällen auch das **Erstatten einer Anzeige bei einer Polizeidienststelle**. Dadurch wird es ermöglicht bzw. erleichtert, dass die **Polizei im Sinne des Betroffenen aktiv werden kann, wenn der Täter gefasst werden sollte bzw. kann**, wie auch bei einer Meldung an das C4, eventuell bei der Schadensbehebung geholfen werden. Zusätzlich kann dadurch ein Lagebild krimineller Cyberaktivitäten erstellt werden, das für strategische Entscheidungen notwendig ist.
- Das Innenministerium hat weiters im Bereich der Direktion für Staatsschutz und Nachrichtendienst (DSN) eine Kontaktstelle für kritische Infrastrukturen, verfassungsmäßige Einrichtungen und internationale Organisationen aufgebaut: das **“Cyber Security Center“** (CSC; csc@dsn.gv.at).
- Das Ziel des CSC ist es, im Zuge von Beratungen und/oder bilateralen Hilfestellungen Firmen oder Organisationen beim Threat Modelling zu unterstützen und mit Hilfe der eigenen strategischen und technischen Erkenntnisse zur Verbesserung der Abwehrmaßnahmen beizutragen.

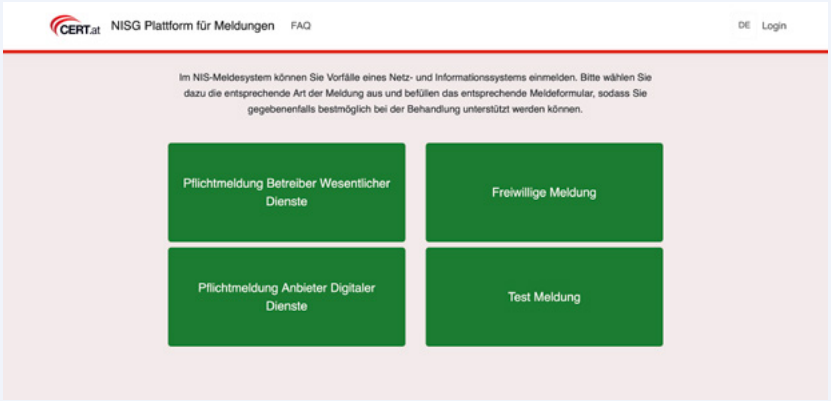
- Insbesondere bei zielgerichteten Cyberangriffen staatlicher Akteure (APTs) gehen diese Beratungen mit vor- oder nachgelagerten technischen Analysen einher. So können die Zuordnung eines Angriffs zu einer bekannten Tätergruppierung, die Analyse der verwendeten Techniken sowie die eingesetzte Infrastruktur einem Opfer helfen, die Bedrohungslage genauer einzuschätzen, Sicherheitslücken aufzudecken und geeignete Abwehrmaßnahmen zu setzen.

Bundesheer und Bundesministerium für Landesverteidigung

- Das Bundesheer hat Cyberexperten in mehreren Bereichen, unter anderem in seinen Nachrichtendiensten (Abwehramt und Heeres-Nachrichtenamt), in seinem IKT & Cybersicherheitszentrum und in den Streitkräften selbst. Diese Experten sind **primär für den Schutz militärischer Einrichtung** zuständig. Die **gesamtstaatliche Zuständigkeit für Cybersicherheit liegt beim Innenministerium**. Sie geht nur bei Krisen und nur, wenn diese souveränitätsgefährdend sind (Angriffe auf militärische IKT-Systeme sowie auf kritische Infrastrukturen und/oder verfassungsmäßige Einrichtungen), auf das Bundesheer über.
- Das Bundesheer kann im Rahmen von Amtshilfen oder Assistenzeinsätzen angefordert werden, wenn der Bund Unterstützung bei Gewährleistung von Cybersicherheit benötigt. **Es ist nicht vorgesehen, dass das Bundesheer bei IT-Sicherheitsvorfällen der Wirtschaft unterstützt, wenn diese nicht souveränitätsgefährdend sind**.

Computer Emergency Teams

- Bald nachdem die ersten EDV- oder IT-Abteilungen in Universitäten, der Wirtschaft oder bei Behörden eingerichtet wurden, waren diese mit IT-Sicherheitsvorfällen konfrontiert. Die als Antwort darauf eingerichteten IT-Security-Abteilungen wurden und werden in der Regel mit der **Tagesarbeit zur Absicherung** von Netzwerken und Infrastruktur beauftragt. Organisationen, die im Falle eines tatsächlichen Angriffes rasch und effektiv reagieren müssen, haben daher **zusätzlich eigene Notfallteams eingerichtet**.
- Neben vielen firmen- bzw. organisationsinternen Notfallteams gibt es ein als **gemeinnütziges Projekt betriebenes nationales Computernotfallteam** „CERT.at“. CERT.at vernetzt nationale CERTs und CSIRTs, ist **Ansprechpartner für IT-Security Themen und Informationsdrehscheibe für Informationen**, die bei der Erkennung und Bewältigung von Angriffen helfen sollen. Teil dieser Aufgabe und auch Auftrag aus dem NIS-Gesetz ist der Betrieb einer **Meldestelle für Sicherheitsvorfälle**. **CERT.at ist per eMail oder auch telefonisch erreichbar**.
- Die **NIS-Meldeplattform** kann auch für Testmeldungen genutzt werden, z.B. im Rahmen von Cyberangriffsübungen oder auch nur, um den Umgang mit der Plattform zu trainieren.



NIS-Meldeplattform

- Das NIS-Gesetz ermöglicht zusätzlich zu einem nationalen Computernotfallteam noch **sektorenspezifische Computernotfallteams**, von denen es aktuell nur eines für den Energiesektor (Austrian Energy CERT) und eines für die **öffentliche Verwaltung** (GovCERT) gibt. Ein weiteres CERT, das Austrian Health CERT für den Gesundheitssektor, ist im Aufbau. Diese sektorenspezifischen CERTs sind jeweils nur für ihren jeweiligen Sektor zuständig und erreichbar.
- Durch den gemeinnützigen Betrieb ist es auch CERT.at nur in einem **eingeschränkten Rahmen** möglich, **Unternehmen bei IT-Sicherheitsvorfällen direkt zu unterstützen**. CERT.at konnte aber bereits in vielen Fällen mit der **Vermittlung von Expertise (zu Angriffsarten, empfohlenen Schutzmaßnahmen, Meldungen über Datenleaks im Darknet, etc.) und Experten (eigene sowie nationale und internationale Partner) helfen, Vorfälle zu verhindern oder einzudämmen**. Über die von CERT.at erhältlichen Warnungen und Newsletter, seine Diskussionsbereiche für Experten oder den gemeinsam mit dem Bundeskanzleramt betriebenen „Austrian Trust Circle" betreibt und fördert CERT.at den fachlichen Austausch zwischen IT-Security Experten aus allen Bereichen von Wirtschaft und Behörden.

Angebote der Wirtschaftskammer

it-safe.at

- Auf it-safe.at finden Unternehmen praxisgerechte Informationen, Online-Ratgeber, Sicherheitshandbücher, Webinare, etc. zur Stärkung der Informationssicherheit im Unternehmen.
- Auf der Unterseite https://wko.at/basissicherheit stehen konkrete Vorlagen zur Verfügung, wie vor allem kleine und mittlere Unternehmen die grundlegenden Maßnahmen für Cybersicherheit im Unternehmen umsetzen können (z.B. Musterdokument Sicherheits-Richtlinie).

wko.at/nis2

- Auf wko.at/nis2 stehen Informationen rund um das Thema Cybersicherheitsgesetzgebung zu NIS2 zur Verfügung. Mit dem Onlineratgeber https://ratgeber.wko.at/nis2 kann in wenigen Schritten getestet werden, ob Unternehmen in den NIS2-Anwendungsbereich fallen.

WKO Firmen A-Z

- Das WKO Firmen A-Z ist das größte und aktuellste **Online-Firmenverzeichnis Österreichs**, es sind alle österreichischen Unternehmen auffindbar. Die Unternehmen können Ihr Profil selbstständig warten und sind daher auch unter den jeweils individuell gewählten Schlagworten (z.B. Cybersecurity) auffindbar. Zusätzlich kann die **Suche auf Branchen (z.B. IT-Dienstleister)** eingeschränkt werden.
- Über die Online-Suche zu IT-Sicherheits-Expertinnen und -Experten kann nach Firmen aus den Bereichen **„Allgemeine IT-Sicherheit", „Cybersecurity", „e-Health Security", „IKT-Security", „Open Source Security" und „IT-Sicherheit und Datenschutz"** gesucht werden. Die letzte Gruppe, „IT-Sicherheit und Datenschutz", umfasst Unternehmen, die eine eigens von der Experts Group IT-Security WKÖ mit der incite GmbH definierte und ISO-zertifizierte Prüfungsroutine durchlaufen haben und daher über entsprechende Qualifikationen im IT-Security Bereich verfügen.

Cyber-Security-Hotline

- Für Notfälle hat die WKO eine Cyber-Security-Hotline (telefonisch erreichbar unter 0800 888 133) eingerichtet, über die in einem 24/7-Betrieb eine kostenlose Erstinformation und danach bei Bedarf die Vermittlung eines IT-Security Unternehmens erfolgen kann.

4. LINKSAMMLUNG

- Übersichtseite der Industriellenvereinigung: www.iv.at/cybersicherheit
- Österreichisches Informationssicherheits-handbuch: www.sicherheitshandbuch.gv.at/siha.php
- Cyber-Kriminalität & Cyber-Versicherungen, WKO: www.wko.at/it-sicherheit/cyber-versicherungen-das-risiko-einfach-auslagern
- Netz- und Informationssicherheitsgesetz: www.nis.gv.at
- Digital Operational Resilience Act (DORA): www.fma.gv.at/querschnittsthemen/digital-operational-resilience-act-dora/
- BMI-Meldestelle zur Bekämpfung von Internetkriminalität: against-cybercrime@bmi.gv.at
- Cyber Security Center (CSC) im Bereich der Direktion für Staatsschutz und Nachrichtendienst (DSN) / BMI: csc@dsn.gv.at
- Nationales Computernotfallteam „CERT.at“: cert.at bzw. team@cert.at; Telefonische Erreichbarkeit: +43 1 5056416 78 (Mo–Fr 8.00–18 Uhr)
- Austrian Energy CERT: www.energy-cert.at/de/
- GovCERT: www.govcert.gv.at
- Cybercrime-Competence-Center C4, Meldestelle BMI: against-cybercrime@bmi.gv.at
- It-safe.at, WKO: it-safe.at; wko.at/basissicherheit
- wko.at/nis2: https://wko.at/nis2; wko.at/basis-sicherheit
- WKO Firmen A-Z: firmen.wko.at
- IT-Sicherheits-Expertinnen und -Experten, WKO: www.wko.at/it-sicherheit/it-sicherheits-expertinnen-und-experten
- Cyber-Security-Hotline, WKO: cys.at
- Wikipedia: de.wikipedia.org/wiki/Ransomware; (de.wikipedia.org/wiki/Phishing); de.wikipedia.org/wiki/Penetrationstest_(Informatik)

www.iv.at

IMPRESSUM

Vereinigung der Österreichischen Industrie (Industriellenvereinigung)
Schwarzenbergplatz 4, 1031 Wien
Tel.: +43 1 711 35 - 0

zvr.: 806801248, livr-n.: 00160, EU-Transparenzregister Nr.: 89093924456-06
Vereinszweck gemäß § 2 Statuten: Die Industriellenvereinigung (IV) bezweckt, in Österreich tätige industrielle und im Zusammenhang mit der Industrie stehende Unternehmen sowie deren Eigentümer und Führungskräfte in freier und demokratischer Form zusammenzufassen, ihre Interessen besonders in beruflicher, betrieblicher und wirtschaftlicher Hinsicht auf nationaler, europäischer und internationaler Ebene zu vertreten und wahrzunehmen, industrielle Entwicklungen zu fördern, Rahmenbedingungen für Bestand und Entscheidungsfreiheit des Unternehmertums zu sichern und Verständnis für Fragen der Wirtschafts- und Gesellschaftsordnung zu verbreiten.

Die verwendeten Bezeichnungen beziehen sich auf alle Geschlechter gleichermaßen.

Für den Inhalt verantwortlich: Industriellenvereinigung
Grafik: Nicola Skalé
Fotocredits: AdobeStock

Wien, Mai 2024