Bundesministerium
Inneres

Nationale CVD-Policy

Leitfaden

Nationale CVD-Policy

Leitfaden

Wien, 2024

Bundeskanzleramt

CERT.at

Bundesministerium
Inneres

dsb
Republik Österreich
Datenschutz
behörde

Impressum

Medieninhaberin, Verlegerin und Herausgeberin:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
bmi.gv.at
Fotonachweis: Adobe
Layout: Referat I/C/10/a – Strategische Kommunikation und Kreation
Druck: Digitalprintcenter des BMI
Wien, 2024

Inhalt

Abkürzungsverzeichnis

C

CRA.....Cyber Resilience Act (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung, KOM (2022) 454 endg)

CSAF.....Common Security Advisory Framework

CSIRT.....Computer Security Incident Response Team

CVD.....Coordinated Vulnerability Disclosure (Koordinierte Offenlegung von Schwachstellen)

CVE.....Common Vulnerabilities and Exposures

CVSS.....Common Vulnerability Scoring System

D

DSG.....Datenschutzgesetz: Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF 70/2024

DSGVO.....Datenschutzgrundverordnung: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 2016/119, 1 idF L 2021/74, 35

E

EMRK..... Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl 210/1958

ENISA.....Agentur der Europäischen Union für Cybersicherheit

H

HSchG.....HinweisgeberInnenschutzgesetz: Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen, BGBl I 6/2023

I

IKT.....Informations- und Kommunikationstechnologie

N

NIS-2-Richtlinie ..... Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, ABl 2022/333

O

OWASP ..... Open Web Application Security Project

P

PaaS ..... Platform-as-a-Service

PGP ..... Pretty Good Privacy

S

S/MIME ..... Secure/Multipurpose Internet Mail Extensions

SaaS ..... Software-as-a-Service

StGB ..... Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), BGBl 60/1974 idF BGBl I 135/2023

StPO ..... Strafprozeßordnung 1975 (StPO), BGBl I 631/1975 idF BGBl I 96/2024

1 Einleitung

Unsere Welt wird immer vernetzter. Die Grenzen des analogen und digitalen Raums verschwimmen und ermöglichen einen rasanten Anstieg an Lebensqualität, Produktivität und Effizienz im Alltag. Doch diese Geschwindigkeit an technischen Weiterentwicklungen im digitalen Raum führt auch dazu, dass Produkte und Dienste mit digitalen Elementen komplexer werden und daher nicht frei von Schwachstellen sind. Diese Schwachstellen werden oft nicht rechtzeitig von den Anbieterinnen und Anbietern jener Produkte und Dienste entdeckt. Sogenannte *„Zero-Days"* haben folglich noch keinen Patch erhalten und können bei Ausnutzung dazu führen, dass Systeme lahmgelegt oder gekapert werden und in der Theorie immensen Schaden an der Lieferkette, der Infrastruktur und zuletzt am Menschen verursachen.

Aufgrund der Tatsache, dass Schwachstellen innerhalb von Unternehmen und Behörden unentdeckt bleiben können, hilft es, wenn auch Dritte Schwachstellen suchen, finden und melden. Die Schwachstellensuchenden müssen nicht zwingend von Anbieterinnen und Anbietern beauftragt werden. Sie können auch Außenstehende sein, denen die Sicherheit von Produkten und Diensten mit digitalen Elementen ein Anliegen ist.

Maßgeblich für den Erfolg dieses Prozesses ist die Koordinierte Offenlegung von Schwachstellen (CVD, nach dem Englischen *Coordinated Vulnerability Disclosure*). Die CVD beschreibt das Verfahren zur Offenlegung von Schwachstellen, in dem im Rahmen eines strukturierten Prozesses die Meldung einer Schwachstelle in einer Diagnose und Behebung des Sicherheitsproblems resultiert. Die CVD erlaubt Anbieterinnen und Anbietern in Folge, rasch zu handeln und Lösungen bzw. Patches für Schwachstellen zu entwickeln und diese strukturiert an ihre Nutzerinnen und Nutzer zu verteilen, um einen möglichen, potenziell großflächigen Schaden zu minimieren. Der vorgesehene Prozess wird meist im Zuge einer sogenannten CVD-Policy an Beteiligte kommuniziert.

Das primäre Ziel des CVD-Prozesses ist die Minimierung des Risikos einer böswilligen Ausnutzung von Schwachstellen.

Aus nationaler sowie auch internationaler Perspektive sind digitale Resilienz und die Sicherstellung von Cybersicherheit zentral für den österreichischen Staat und die Europäische Union. Die koordinierte Offenlegung von Schwachstellen dient folglich der Stärkung der gesamtheitlichen Cybersicherheit, dem aktiven Cyberschutz, der Sicherheit von Produkten und Dienstleistungen sowie dem Schutz und der Gewährleistung der Privatsphäre der Nutzerinnen und Nutzer. Um die Ausnutzungswahrscheinlichkeit zu minimieren, ist eine Koordination zwischen Anbieterinnen und Anbietern sowie deren Lieferketten auf der einen Seite und Nutzerinnen und Nutzer auf der anderen Seite

nötig. Eine verfrühte öffentliche Offenlegung kann genauso gefährlich sein wie ein zu langes Zuwarten.

Die nationale CVD-Policy bietet als Leitfaden eine Übersicht darüber, wie ein Meldeprozess für Schwachstellen aussehen kann. Sie gibt einen Einblick in die Rechte und Pflichten aller Beteiligten in Österreich, um ausreichend Informationen zum Meldeprozess zu liefern und ein ordnungsgemäßes Verfahren sicherzustellen.

2 Wie sieht der CVD-Prozess aus?

2.1 Was ist eine Schwachstelle?

Unter einer Schwachstelle versteht man eine Schwäche, Anfälligkeit oder einen Fehler eines Produktes oder Dienstes mit digitalen Elementen, die durch eine Cyberbedrohung ausgenutzt werden kann.

Schwachstellenart und betroffene Systeme

Grundsätzlich können alle Arten von Schwachstellen in Produkten oder Diensten mit digitalen Elementen gemeldet werden. Dabei muss vor allem zwischen Schwachstellen in spezifischen Onlinediensten (Webseiten oder andere Server) und Schwachstellen in generischer Software, die kommerziell oder als Open Source vertrieben wird, unterschieden werden. Bei Schwachstellen in Onlinediensten (inkl. Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS)) muss bei der Suche zwangsläufig mit Systemen unter der Kontrolle von Anbieterinnen und Anbietern interagiert werden, während die Suche nach Schwachstellen in generischer Software auch im Labor der Schwachstellensuchenden erfolgen kann. Darüber hinaus können Schwachstellen auch in Protokollen und Hardwareelementen vorkommen.

Daher variieren je nach Art des betroffenen Systems das Prinzip der Proportionalität und der legale Rahmen.

2.2 Beteiligte des CVD-Prozesses

Hier finden Sie eine Aufschlüsselung der Beteiligten im CVD-Prozess:

Schwachstellensuchende

Es gibt verschiedene Personengruppen, die im Zuge dieses Leitfadens als „Schwachstellensuchende“ gelten. Dies können etwa die Nutzerinnen und Nutzer eines Produktes, IKT-Sicherheitsforschende oder Forschungseinrichtungen sein, unabhängig davon, ob die Schwachstelle durch gezielte Suche oder durch zufälligen Fund entdeckt wird. Schwachstellen können von natürlichen oder juristischen Personen[1] gemeldet werden. Grundsätzlich ist jede Person, die eine Schwachstelle meldet, als Schwachstellensuchende zu verstehen.

1 Siehe 3.1.

Anbieterinnen und Anbieter

Darunter fallen Einzelpersonen, aber auch Gruppen (wie z. B. Unternehmen, Behörden oder Organisationen), die Produkte oder Dienste mit digitalen Elementen erstellt haben und/oder diese bereitstellen.

Das können sowohl Herstellerinnen und Hersteller von Software als auch Betreiberinnen und Betreiber einer Webseite sein.

Koordinator (Koordinierende Stelle)

Die koordinierende Stelle, in Fachkreisen und zur internationalen Harmonisierung im Zuge dieses Dokuments als Koordinator bezeichnet, kann die Kommunikation zwischen Anbieterinnen und Anbietern sowie Schwachstellensuchenden bei dem CVD-Prozess übernehmen und koordiniert bei Bedarf die gewählte Vorgehensweise mit weiteren Beteiligten.

Wie jeder EU-Mitgliedstaat benennt Österreich ein „Computer Security Incident Response Team“ (CSIRT) als Koordinator für die Zwecke der CVD.[2] Dieses kann im Bedarfsfall als Vermittler zwischen den meldenden Personen (Schwachstellensuchenden) und den Anbieterinnen und Anbietern von Produkten oder Diensten mit digitalen Elementen, die von der Schwachstelle betroffen sind, fungieren. Sobald eine Schwachstelle mehr als einen EU-Mitgliedstaat betrifft (z.B.: Notwendigkeit einer grenzüberschreitenden Abstimmung vor der (möglichen) öffentlichen Offenlegung), kooperieren die jeweiligen CSIRT innerhalb des CSIRT-Netzwerks.

Damit die Verteilung der Rollen und Aufgaben im Zuge dieses Leitfadens klar ersichtlich ist, werden allfällige Tipps und Hinweise für Anbieterinnen und Anbieter **BLAU** markiert, jene für Schwachstellensuchende **GRÜN**.

2 Siehe 3.1.

2.3 Grundprinzipien

Um im Zuge eines CVD-Prozesses einen ordnungsgemäßen Ablauf zu garantieren, sollten alle Beteiligten im Zuge des CVD-Prozesses die folgenden Grundprinzipien berücksichtigen:

1. **Verantwortliches Handeln und gute Absichten**

Gute Absichten sind Voraussetzung für ein ordnungsgemäßes Handeln. Alle Beteiligten sollten die gefundenen Schwachstellen und die dazugehörigen Parameter mit Sorgfalt behandeln und im Zuge der Kommunikation Kooperationsbereitschaft demonstrieren. Dasselbe gilt auch für die Vorgehensweise bei der Schwachstellensuche.

> Um gute Absichten und Verantwortung zu demonstrieren, ist eine rasche Meldung der Schwachstelle nach Entdeckung vorteilhaft. Das sollte in einem Aktivitäts- und Kommunikationsprotokoll dokumentiert werden.

2. Subsidiarität

Schwachstellensuchende sind dazu angehalten, eine Problemlösung möglichst direkt zu adressieren. Das bedeutet, dass in den meisten Fällen als erster Schritt eine Kontaktaufnahme mit den Anbieterinnen und Anbietern zu empfehlen ist.

3. Proportionalität und Datenschutz

Schwachstellensuchende sollten sicherstellen, dass die angewendeten Mittel proportional in Anbetracht des Zieles der Schwachstellensuche und Schwachstellenverifikation bleiben.

Dabei ist darauf zu achten, dass die Schwachstellensuche die Operationalität von Anbieterinnen und Anbietern nicht einschränkt und Anbieterinnen und Anbietern kein finanzieller oder materieller Schaden entsteht. Das heißt insbesondere, dass kein Brute-Forcing, kein Denial of Service, kein Social Engineering, keine Veränderung von Systemen und Daten und kein Einbringen von Malware ohne eine schriftliche „Permission-to-Attack"-Vereinbarung mit den Anbieterinnen und Anbietern zulässig ist.

Schwachstellensuchende sollten sicherstellen, dass die gelindesten Mittel angewandt und nur die notwendigsten Informationen für die Schwachstellenmeldung erhoben werden.

Ermöglicht die gefundene Schwachstelle den Zugriff auf sensible Daten, so darf diese nur soweit ausgenutzt werden, wie es zur Erbringung des Nachweises des Problems nötig ist. So erhaltene Daten müssen von Schwachstellensuchenden vertraulich behandelt und möglichst bald gelöscht werden.[3]

Bei Fragen zum ordnungsgemäßen Ablauf kann der Koordinator in seiner Funktion als Vermittler von allen Beteiligten des CVD-Prozesses konsultiert werden.

> Trotz Vereinbarungen im Zuge des CVD-Prozesses sind Anbieterinnen und Anbieter von Produkten und Diensten mit digitalen Elementen jederzeit für die Integrität ihrer Produkte verantwortlich.

---

3 Siehe Kapitel 3.5.

4. **Einhalten des Zeitrahmens und Abstimmungen**

Um einen reibungslosen Ablauf sicherzustellen, sollten sich alle Beteiligten auf einen Zeitplan für die Erarbeitung und Verteilung eines Patches sowie die Offenlegung der Schwachstelle einigen und sich daran halten. Der Koordinator kann auch hier als Vermittler agieren.

Unkoordinierte öffentliche Offenlegungen sollten unterlassen werden.

5. **Kommunikation**

Zu einem ordnungsgemäßen Ablauf zählt auch eine sorgfältige, bedachte und niederschwellige Kommunikation. Alle Beteiligten sind dazu angehalten höflich und respektvoll zu kommunizieren und den CVD-Prozess so zu unterstützen.

> Ein höflicher und zuvorkommender Umgangston demonstriert Kommunikationsbereitschaft und hinterlässt oft einen positiven Gesamteindruck.

2.4 Meldung einer Schwachstelle

Schritt 0: Identifikation und Verifikation der Schwachstelle

Sobald Schwachstellensuchende eine Schwachstelle entdeckt haben, sollte diese auch als solche verifiziert werden, um Anbieterinnen und Anbietern sowie Koordinator vor inkorrekten Schwachstellenmeldungen zu bewahren.

Da Anbieterinnen und Anbieter sowie Koordinator möglicherweise eine Vielzahl an Schwachstellenmeldungen erhalten, bietet sich die Bewertung der Schwachstelle nach dem Common Vulnerability Scoring System (CVSS) in letzter Version sowie eine Einordnung anhand geeigneter Kategorisierungssysteme (z. B. Open Web Application Security Project (OWASP) Top 10, Common Vulnerabilities and Exposures (CVE)) an. Des Weiteren sollte die Kritikalität auch anhand der Tragweite der Schwachstelle im Gesamtbild und nicht nur anhand der Kritikalität der Schwachstelle an sich bewertet werden. Dies sollte auch unter Berücksichtigung der Ausnutzungswahrscheinlichkeit der Schwachstelle geschehen. Diese Bewertung soll dazu dienen, den akuten Schweregrad der Schwachstelle darzulegen und eine Priorisierung für Anbieterinnen und Anbieter sowie Koordinator zu erleichtern.

Schritt 1: Überprüfung der Kontaktmöglichkeiten der Anbieterinnen und Anbieter durch Schwachstellensuchende

Schwachstellensuchende sollten überprüfen, ob von der Schwachstelle betroffene Anbieterinnen und Anbieter eine eigene CVD-Policy publiziert haben, oder zumindest entsprechende Kontaktmöglichkeiten angeben. Ein gängiger Weg für die Publikation einer CVD-Policy ist der „security.txt"-Standard.[4] Geben die beteiligten Anbieterinnen und Anbieter eine eigene CVD-Policy an, sollte der durch die Anbieterinnen und Anbieter vorgesehene Prozess berücksichtigt werden, sofern dieser Ablauf der österreichischen nationalen CVD-Policy nicht widerspricht.

Sollten die Anbieterinnen und Anbieter keine eigene CVD-Policy bzw. Kontaktmöglichkeiten anführen oder deren CVD-Policy der nationalen widersprechen, ist eine Kontaktaufnahme über den Koordinator zu empfehlen. Der Koordinator kontaktiert in weiterer Folge die beteiligten Anbieterinnen und Anbieter.

Sie können den Koordinator jederzeit, auf Wunsch auch anonym[5] (z. B. anonymisierte E-Mail etc.), mit Ihrer Schwachstellenmeldung oder bei Kommunikationsproblemen und Unklarheiten kontaktieren. Bitte beachten Sie, dass bei einer anonymen Meldung eine Bearbeitung unter Umständen nur eingeschränkt möglich ist, außer es wird eine Kontaktmöglichkeit angegeben. Der Koordinator kann auf Wunsch auch die Identität und Kontaktdaten von Schwachstellensuchenden gegenüber den Anbieterinnen und Anbietern verbergen.

Sie können den Koordinator jederzeit bei Kommunikationsproblemen oder Unklarheiten kontaktieren. Der Koordinator kann auch inmitten des Prozesses, auf Wunsch, hinzugezogen werden.

Durch das Einrichten einer hauseigenen CVD-Policy wird der eigene Prozess erläutert und eine rasche Schwachstellenbehebung Ihrer Produkte gefördert.

4 https://datatracker.ietf.org/doc/html/rfc9116
5 Siehe Art 12 Abs 1 NIS-2-Richtlinie.

Schritt 2: Meldung der Schwachstelle durch Schwachstellensuchende

Um die Anonymität der Schwachstellensuchenden zu gewährleisten, können Schwachstellensuchende dem Koordinator derzeit per E-Mail eine Schwachstelle melden. Siehe dafür https://www.cert.at/de/services/vorfall-melden/.

Bei hochsensiblen Schwachstellen ist eine Ende-zu-Ende Verschlüsselung über E-Mail (Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail Extensions (S/MIME)) zu empfehlen. Die Meldung sollte alle notwendigen Informationen enthalten, die AnbieterInnen und Koordinator benötigen, um die Schwachstelle nachvollziehen zu können.

> Bitte beachten Sie, dass bei einer Schwachstelle, die mehrere Länder und/oder AnbieterInnen (multi-party) betrifft, eine Meldung an den Koordinator zu empfehlen ist.

Schritt 3: Verifikation und Bewertung der Schwachstelle durch AnbieterInnen/ Koordinator

Um eine Schwachstelle beheben zu können, müssen Anbieterinnen und Anbieter die Schwachstelle nachvollziehen können. Die Meldung der Schwachstelle sollte daher alle dafür notwendigen Informationen enthalten. Im Fall einer unvollständigen Schwachstellenmeldung kann es sein, dass zusätzliche Dokumente und Nachweise über die Schwachstelle von den Schwachstellensuchenden benötigt werden. Dies kostet Zeit und verursacht zusätzlichen Kommunikations- und Verwaltungsaufwand.

Der Koordinator wird in den meisten Fällen nach Kontaktaufnahme eine Plausibilitätsprüfung durchführen.

Nachdem die Schwachstelle bestätigt wurde, sollte durch die Anbieterinnen und Anbieter eine Priorisierung aufgrund der Kritikalität und anhand der Tragweite der Schwachstelle (Nutzerinnen- und Nutzerkreis, Ausnutzungsmöglichkeit etc.) vorgenommen werden.

> Eine unvollständige Meldung, die zum Beispiel eine Reproduktion verhindert, kann zu einem Abbruch des CVD-Prozesses führen.

Schritt 4: Kontaktaufnahme durch Anbieterinnen und Anbieter/Koordinator

Nach Analyse der gemeldeten Schwachstelle – unabhängig der Einschätzung – informieren Anbieterinnen und Anbieter innerhalb von 14 Tagen nach Meldung (potenziell über den Koordinator) die Schwachstellensuchenden über die weitere Vorgehensweise.

Schritt 5: Entwicklung von Folgemaßnahmen durch Anbieterinnen und Anbieter

Die Anbieterinnen und Anbieter bemühen sich, schnellstmöglich und fristgerecht, Lösungen bereitzustellen.

Sollten die Anbieterinnen und Anbieter 60 Tage nach der eingelangten Schwachstellenmeldung keine geeigneten Maßnahmen getroffen haben, kann der Koordinator die Schwachstelle öffentlich offenlegen, wenn dies dem öffentlichen Interesse dient. Eine Nichteinhaltung der Frist, unter anderem aufgrund von komplexen Systemen und aufwendigen Lösungen, sollte jedenfalls mit dem Koordinator/Schwachstellensuchenden abgesprochen werden. Gegebenenfalls kann dies zu einer Verlängerung der Frist führen.

Schritt 6: Offenlegung der Schwachstelle durch Anbieterinnen und Anbieter

Um den CVD-Prozess abzuschließen, sollten Anbieterinnen und Anbieter die Existenz der Schwachstelle, die Verfügbarkeit einer korrigierten Version des Produktes und gegebenenfalls Mitigierungsmaßnahmen offenlegen (sog. Security Advisory/Schwachstellenwarnung). Letztlich dient vor allem eine öffentliche Offenlegung von Schwachstellen durch Anbieterinnen und Anbieter der Stärkung der Cybersicherheit in Österreich.

Nicht jede Schwachstelle verlangt jedoch eine öffentliche Offenlegung:

Zu unterscheiden ist zwischen der öffentlichen Offenlegung, bei der die Information der gesamten Öffentlichkeit zugänglich gemacht wird und einer teilweisen Offenlegung, bei der bloß direkt betroffenen Nutzerinnen und Nutzern gegenüber offengelegt wird. Darüber hinaus gibt es auch Fälle, in denen gar nicht offengelegt wird. Dies ist dann der Fall, wenn die Offenlegung nicht im Sinne des öffentlichen Interesses wäre. Bei komplexen Schwachstellen, die mehrere Anbieterinnen und Anbieter oder Mitgliedstaaten betreffen (multi-party), wodurch eine zeitgerechte Behebung nicht gewährleistet ist oder im Falle eines Überwiegens des öffentlichen Interesses, (z. B. der nationalen Sicherheit oder bei möglichen Schäden anderer) sollte von einer Offenlegung abgesehen werden. Bei einer Schwachstelle, die mehrere Anbieterinnen und Anbieter betrifft und auch Auswirkungen auf die Nutzerinnen und Nutzer hat, ist eine Offenlegung der Schwachstelle durch Anbieterinnen und Anbieter jedenfalls zu empfehlen.

Um die automatisierte Verarbeitung von Schwachstelleninformationen zu ermöglichen, sollte die Offenlegung zusätzlich zu üblichen Sicherheitshinweisen (Security Advisories) auch nach dem „Common Security Advisory Framework"-Standard (CSAF) erfolgen. Sollten sich Anbieterinnen und Anbieter für eine öffentliche Offenlegung entscheiden, ist die Zuteilung einer CVE-Nummer und ein entsprechender Eintrag in internationalen Schwachstellendatenbanken (wie etwa die European Vulnerability Database der Agentur der Europäischen Union für Cybersicherheit (ENISA)) zu empfehlen.

Veröffentlichen Sie Ihre Advisories im CSAF-Standardformat, um die Zeit zwischen Patch-Veröffentlichung und Patch-Anwendbarkeit zu verringern.

Senden Sie unterstützende Dokumente, die Folgemaßnahmen für die von der Schwachstelle betroffene Öffentlichkeit beinhalten.

Vermeiden Sie unkoordinierte öffentliche Offenlegungen. Sie könnten damit sich, Anbieterinnen und Anbieter sowie dem Nutzerinnen- und Nutzerkreis erheblich schaden.

2.5 Anerkennungsmöglichkeiten

Die Schwachstellensuche kann erfahrungsgemäß viel Zeit und Arbeit in Anspruch nehmen. Deshalb werden Anbieterinnen und Anbieter darauf hingewiesen, je nach Kritikalität der Schwachstelle, Schwachstellensuchenden eine passende Anerkennung zukommen zu lassen.

Führen Sie nach internationaler Praxis ein Bug-Bounty-Programm ein oder versuchen Sie, Schwachstellensuchende durch Anerkennung (wie z. B. einer „Hall-of-Fame“ bzw. Danksagungen) oder andere Anreize zur Schwachstellensuche zu motivieren.

Bitte beachten Sie, dass Anerkennung nicht eingefordert werden kann und eine Einforderung von Anerkennungen unter Drohung der öffentlichen Offenlegung der Schwachstelle unter anderem rechtswidrig sein kann.

3 Rechtliche Information für Einsteiger

Hinweis:

Der folgende Abschnitt widmet sich CVD-relevanten Informationen in Bezug auf rechtliche Aspekte. Ziel ist, eine Übersicht zur Best Practice und zu zentralen Fragen im Rahmen der geltenden österreichischen Rechtslage zu schaffen.

Es wird insbesondere darauf hingewiesen, dass Personen, die sich widerrechtlich Zugriff auf ein Computersystem verschaffen, eine Straftat begehen können.

Für Schwachstellensuchende sind die Umstände des Einzelfalls, also der Kontext, ausschlaggebend für die rechtliche Beurteilung ihrer konkreten Situation. Eine generelle Befreiung von – wie auch immer gearteten – rechtlichen Verpflichtungen und rechtlichen Folgen ergibt sich allein aufgrund dieses Leitfadens nicht. Insbesondere wenn Sie sich als Schwachstellensuchender bzw. Schwachstellensuchende im Unklaren über Ihre Situation sind, könnten Sie sich für die Einholung einer individuellen Beratung an eine rechtskundige Person wenden.

Für Schwachstellensuchende sowie Anbieterinnen und Anbieter sind die rechtlichen Rahmenbedingungen für die Offenlegung einer Schwachstelle von großer Bedeutung. Für beide Seiten können sich bei der Beurteilung der eigenen Situation im Hintergrund zur Suche und Offenlegung einer Schwachstelle unter anderem folgende Fragen ergeben:

- Droht mir durch das Vorgehen im Rahmen eines CVD-Prozesses die Verfolgung der Handlung als Straftat?
- Kann oder muss eine Handlung im Rahmen des CVD-Prozesses angezeigt werden?
- Setze ich mich zivilrechtlichen Ansprüchen anderer aus?
- Muss ich im Rahmen des CVD-Prozesses datenschutzrechtliche Aspekte beachten?
- Habe ich einen Anspruch darauf, nach NIS-2 eine Schwachstelle offenlegen zu können?
- Welche Aspekte muss ich beim Vorgehen im Rahmen des CVD-Prozesses aus rechtlicher Sicht überhaupt beachten?
- Gibt es einen neutralen Ansprechpartner und sonstige Hilfestellungen für mich im Rahmen des CVD-Prozesses?

Vor allem zur Abklärung dieser Fragen kann es hilfreich sein, bereits im Vorfeld und begleitend zur technischen Betreuung, rechtliche Beratung in Anspruch zu nehmen.

3.1 Hintergrundinformation: Unionsrechtlicher Kontext

Wenn es um die Frage geht, auf welche Rechtsgrundlage sich die CVD-Policy bezieht, ist Artikel 12 der NIS-2-Richtlinie zentral.

Er kann als die europäische rechtliche Basis der CVD gesehen werden und verankert die koordinierte Offenlegung von Schwachstellen explizit. Hintergrund ist die Förderung eines aktiven Cyberschutzes. Die Offenlegung von Schwachstellen soll dabei attraktiver gemacht werden. In einem strukturierten Prozess sollen Schwachstellen in einer Weise gemeldet werden, die die Diagnose und Behebung ermöglicht, bevor detaillierte Informationen an die Öffentlichkeit weitergegeben werden.[6] Da Schwachstellen häufig von Dritten (insbesondere aus der Zivilgesellschaft) entdeckt werden, sollen meldende Personen bei der Entdeckung und bei der geordneten Offenlegung unterstützt werden.[7]

Eine meldende Person kann dabei jede „natürliche oder juristische Person“[8] sein – es handelt sich dabei also um einen sehr weiten Adressatenkreis. Auf der anderen Seite können Anbieterinnen und Anbieter eines potenziell gefährdeten Produkts oder Dienstes mit digitalen Elementen beteiligt sein. Es kommt jeweils nicht darauf an, ob es sich um Einrichtungen im Anwendungsbereich der NIS-2-Richtlinie handelt.

Eine weitere wichtige rechtliche Grundlage kann der Vorschlag[9] für den Cyber Resilience Act (CRA) sein. So sollen im Rahmen des Cyber Resilience Act essenzielle Anforderungen für den *„vulnerability handling process“* durch die Anbieterinnen und Anbieter festgelegt werden. Konkret bedeutet das, dass Meldepflichten sowie Regelungen zur freiwilligen Meldung von Schwachstellen verbindlich festgelegt werden. Anbieterinnen und Anbieter werden etwa dazu angehalten, über Policies zur koordinierten Offenlegung von Schwachstellen zu verfügen. Auch soll der *„vulnerability handling process“* regelmäßig kontrolliert werden.

---

6 Erwägungsgrund 57 f NIS-2-Richtlinie
7 Erwägungsgrund 58 NIS-2-Richtlinie
8 Artikel 12 Absatz 1 lit b NIS-2-Richtlinie
9 Stand 08/2024: Im Gesetzwerdungsprozess

Besonders relevant ist dabei für Schwachstellensuchende im Einzelfall die Frage, ob es sich um einen CRA-bezogenen Fall handelt, oder allein die Vorgaben aus der NIS-2-Richtlinie ausschlaggebend sind. Dies ist für Sie insofern wesentlich, als nach dem CRA konkretere rechtliche Anforderungen und Pflichten (insbesondere für Herstellerinnen und Hersteller) bestehen, während die NIS-2-Richtlinie grundsätzlich bloß die Rolle des als Koordinator benannten CSIRT im Rahmen des CVD-Prozesses verankert.

Für Anbieterinnen bzw. Anbieter ist besonders die Frage von Bedeutung, ob sich für sie aus dem CRA-Regime im konkreten Einzelfall Pflichten ergeben können.

3.2 Hinweisgeberinnen- und Hinweisgeberschutz

Externe und interne Meldestelle nach dem HinweisgeberInnenschutzgesetz (HSchG) beim Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK)

Wenn es um die Frage geht, ob für Schwachstellensuchende Regelungen im Zusammenhang mit der Hinweisgebung relevant sein können, ist das HSchG zentral:

Zum Schutz der Hinweisgeberinnen und Hinweisgeber wurde sowohl für den privaten und öffentlichen Bereich als auch für den internen Bereich des Bundesministeriums für Inneres eine Meldeplattform eingerichtet, die eine anonyme Kommunikation mit den Mitarbeiterinnen und Mitarbeitern der Meldestelle gewährleistet.

Die Meldestelle für den privaten und öffentlichen Sektor ist unter dem Link www.bkms-system.net/BAK erreichbar. Weiterführende Informationen sind unter FAQ (bak.gv.at) verfügbar.

Wer kann melden?

Wer im Rahmen einer laufenden oder früheren beruflichen Verbindung zu einem Rechtsträger von bestimmten Verstößen, Verschleierungshandlungen u. dgl. erfährt, kann eine nach dem HinweisgeberInnenschutzgesetz (HSchG) geschützte Person sein. Dazu zählen nicht nur Arbeitnehmerinnen und Arbeitnehmer, sondern auch Bewerberinnen und Bewerber, Lieferantinnen und Lieferanten, Personen mit einer ehemaligen Arbeitsbeziehung zu den betroffenen Organisationen etc.

Was kann gemeldet werden?

Meldungen können zu vielen verschiedenen Themengebieten abgegeben werden. Unter anderem auch **zum Thema Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen.**

Was passiert mit meiner Meldung?

Einlangende Meldungen werden von der Hinweisgebermeldestelle sorgfältig geprüft, auch auf den etwaig eröffneten Anwendungsbereich des HinweisgeberInnenschutzgesetzes.

Der Schutzbereich des HinweisgeberInnenschutzgesetzes gilt grundsätzlich ab dem Zeitpunkt der Abgabe der Meldung, wenn Sie zum Zeitpunkt der Meldung unter Berücksichtigung der tatsächlichen Umstände und der Ihnen vorliegenden Informationen davon ausgehen, dass Ihr Hinweis der Wahrheit entspricht und in den sachlichen und persönlichen Geltungsbereich dieses Gesetzes fällt.

Die Hinweisgebermeldestelle des BAK leitet – nach Erstprüfung – die abgegebene Meldung an die zuständige Stelle zur Bearbeitung weiter. Sofern sich aus dem Meldungstext ein Indiz für einen strafrechtlichen Anfangsverdacht ergibt, wird diese Meldung zur weiteren Verfolgung an die zuständigen Strafverfolgungsbehörden weitergeleitet. Sofern eine Kommunikationsmöglichkeit (z. B. Postkasten) im System bereitsteht, wird die Hinweisgeberin oder der Hinweisgeber über diesen Schritt informiert.

Beispiel: A ist Mitarbeiter eines großen österreichischen Unternehmens, das im Bereich der Energieversorgung tätig ist. A arbeitet in jener Abteilung, die für die laufende Systemprüfung zuständig ist, die gewährleistet, dass alle Industrieunternehmen im Gebiet mit ausreichend Strom versorgt werden. A erfährt durch einen Vortrag über die Notwendigkeit von Cybersicherheitsmaßnahmen und der Verpflichtung, diese regelmäßig zu prüfen und auf den neuesten Stand zu bringen. A erkennt im Rahmen seiner Tätigkeit, dass es wohl zu einem unberechtigten Zugriff auf die IT-Infrastruktur des Unternehmens gekommen ist und erkennt weiters, dass die Unternehmensleitung aus wirtschaftlichen Überlegungen heraus nicht alle vorgesehenen Systemüberprüfungen bzw. Wartungen der IT-Systeme durchgeführt hat. A kann diesen Vorfall an die Hinweisgebermeldestelle des BAK melden.

Wichtige Anmerkung zur Anonymität: Grundsätzlich besteht die gesetzliche Verpflichtung, die Identität der Hinweisgeberinnen und Hinweisgeber zu schützen. Bitte beachten Sie jedoch, dass Ihre Daten in bestimmten gesetzlich geregelten Fällen offengelegt werden können bzw. müssen. Insbesondere ab Vorliegen eines strafrechtlichen Anfangsverdachtes gemäß § 1 Abs. 3 Strafprozessordnung 1975 (StPO) kommen

die Bestimmungen der StPO zur Anwendung. Bei Anwendung der Strafprozessordnung muss in alle Richtungen ermittelt werden. Dies bedeutet unter Umständen auch gegen die Hinweisgeberin bzw. den Hinweisgeber, sofern sich dieser bzw. diese im Zuge der Erlangung der Informationen gesetzwidrig (§ 118a StGB etc.) verhalten hat.

3.3 Strafrechtliche Aspekte

Wenn es um die Frage geht, ob Schwachstellensuchenden eine strafrechtliche Verfolgung droht, ist die Auseinandersetzung damit, ob der Straftatbestand des **§ 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem)** im Einzelfall anzuwenden ist, zentral.

Vereinfacht dargestellt spielen dabei **vier Aspekte** eine Rolle: (i) das „Computersystem" beziehungsweise ein Teil eines solchen (Achtung: weites Verständnis, nicht unbedingt immer deckend mit IT-Verständnis); (ii) das Überwinden einer spezifischen Sicherheitsvorkehrung; (iii) die Verfügungsbefugnis; (iv) der erweiterte Vorsatz in der Form der Absicht (§ 5 Abs. 2 StGB).

i. Computersystem

Gemäß § 74 Abs. 1 Z 8 StGB handelt es sich bei einem Computersystem im strafrechtlichen Sinne *„sowohl [um] einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen"*. Solche Vorrichtungen sind jedenfalls die körperlichen Bestandteile wie Prozessor, Drucker, Bildschirm usw. Unter einem Computersystem ist nicht nur der klassische PC zu verstehen, sondern beispielsweise auch Mobiltelefone oder andere computergesteuerte Geräte.

Für § 118a StGB reicht es aus, wenn sich die Täterin bzw. der Täter bloß zu einem Teil eines Computersystems, über das sie bzw. er nicht oder nicht allein verfügen darf, Zugang verschafft. Solche Teile können die einzelnen körperlichen Vorrichtungen und alle möglichen anderen externen Komponenten, aber auch andere Bestandteile wie z. B. die Kabel bei einem kabelverbundenen System sein. Aber auch was sich innerhalb des Systems befindet – installierte Hard- und Software – ist als Teil des Systems anzusehen. Somit stellen auch die auf einem PC abgespeicherten **Daten** (etwa Text- und Bilddateien ebenso wie Dateien, die für bestimmte Funktionalitäten wie bspw. Online-Banking-Portale, Accounts, Clouds usw. nötig sind) einzelne Bestandteile eines Computersystems dar *(Reindl-Krauskopf in Höpfel/Ratz, WK² StGB § 118a Rz 6).*

ii. Überwindung einer spezifischen Sicherheitsvorkehrung

Darüber hinaus stellt sich die Frage, ob sich eine Person durch **Überwindung einer spezifischen Sicherheitsvorkehrung** Zugang zu einem Computersystem verschafft. Das ist dann der Fall, wenn sie ein gewisses Mindestmaß an Anstrengungen erbringt, um eine solche Sicherheitsvorkehrung zu überwinden.

Die Grundidee dahinter ist, dass das System durch solche Vorkehrungen vor dem Zugriff durch unbefugte Eingriffe geschützt wird. Solche Sicherheitsvorkehrungen können beispielsweise Computerpasswörter oder dergleichen sein. Nicht gemeint sind in dem Zusammenhang Hürden bloß physischer Art (die in keinem unmittelbaren Zusammenhang mit dem Computersystem stehen), wie etwa das bloße Versperren des Raumes, um den Zutritt zu dem Computersystem, das sich darin befindet, zu erschweren. Damit übereinstimmend wird dieses Element so verstanden, dass die Anstrengung, mit der eine solche Vorkehrung überwunden wird, auch technische Angriffsarten umfasst, die nicht eine Verletzung der Datenintegrität zur Folge haben. Auch erfasst sind also Zugriffe, die nicht dem vom System vorgesehenen Zulassungsverfahren entsprechen, wie beispielsweise das rechtswidrige Erlangen von Passwörtern durch Mitlesen von Datenverkehr oder Brute-Force-Methoden.

Unterschiedlich zu bewerten sind Konstellationen, in denen „bloß" Sicherheitslücken (z. B. Programmfehler) ausgenutzt werden. Diese Fallvarianten sind im Zusammenhang mit der koordinierten Offenlegung von Schwachstellen besonders von Bedeutung. Handelt es sich um eine Sicherheitslücke, die geradezu offensichtlich ist, wird eher nicht von einer Überwindung i. S. d. StGB auszugehen sein. Anders kann es sein, wenn die Person erst unter Einsatz eines hohen Maßes an technischem Know-how und (krimineller) Energie die Lücke erfassen und somit die Vorkehrung überwinden kann.

Im Fall von Schwachstellensuchenden im Sinne der CVD nach Art 12 NIS-2-Richtlinie ist davon auszugehen, dass die Suche nach Schwachstellen nicht für kriminelle Zwecke erfolgt, sondern eine Verbesserung des Cybersicherheitsniveaus der Zweck der Suche ist. Darauf aufbauend kann zwischen zwei in der Praxis auftretenden Formen der Suche und Offenlegung unterschieden werden.

iii. Tatbestandsausschließende Verfügungsbefugnis

Im ersten Fall werden Schwachstellensuchende von einer gewissen Herstellerin/Anbieterin bzw. einem Hersteller/Anbieter beauftragt, Schwachstellen zu finden. Damit wird in der Regel davon auszugehen sein, dass Schwachstellensuchende in solchen Fällen in diesem Ausmaß eben über das System verfügen dürfen. Der Zugriff wird hier somit nicht „widerrechtlich" erfolgen und § 118a StGB wäre nicht erfüllt.

Im zweiten Fall, in dem Schwachstellensuchende „auf eigene Faust“ nach Schwachstellen suchen, ist die Absicht der Schwachstellensuchenden im Rahmen des erweiterten Vorsatzes besonders zu prüfen.

iv. Subjektive Tatseite / erweiterter Vorsatz

Strafbar ist ein Zugriff im Sinne des § 118a StGB dann, wenn sogenannte „**Spionageabsicht**“ (also *„sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Beteiligten verletzt“*, § 118a Abs. 1 Z 1 StGB) oder sogenannte „**Verwendungsabsicht**“ (also *„einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen“*, § 118a Abs. 1 Z 2 StGB) vorliegt.

Nur wenn es also dem Schwachstellensuchenden auf eine der beiden Absichten geradezu ankommt, wäre der Tatbestand des § 118a StGB erfüllt. Dies würde nach allgemeiner Lebenserfahrung jedoch dem typischen Bild von Schwachstellensuchenden im Sinne von Art 12 NIS-2-Richtlinie bzw. *„white hat hackers“* widersprechen, wollen diese ja Standards der Systeme verbessern und das Niveau heben. Für die Strafbarkeit in diesem Sinne reicht es insbesondere nicht, dass sich Schwachstellensuchende denken: *„Es wird schon nicht so sein“* oder sogar *„Na und wenn schon, …“*. Es ist daher wichtig, dass Schwachstellensuchende ihre Intention und ihre Kommunikation gut dokumentieren und ihre guten Absichten nachvollziehbar darlegen.

Im Kontext der CVD stehen Schwachstellensuchende nicht selten in einer Art positiven Wettbewerb zueinander. Das Zufügen eines Nachteils einem anderen gegenüber wird jedoch auch in diesen Fällen in der Regel gerade nicht beabsichtigt sein. Insofern ist es wichtig, dass Schwachstellensuchende im Rahmen von Bug-Bounty-Programmen andere nicht mit eigeninitiierten finanziellen Forderungen unter Druck setzen.

Da es aber – wie überall – auch schwarze Schafe geben kann, kann eine Verwirklichung des Tatbestands des § 118a StGB im Einzelfall nicht pauschal ausgeschlossen werden. Eine Verwirklichung ist dann gegeben, wenn alle Merkmale des Delikts erfüllt sind. Insofern ist die einleitend betonte detaillierte Prüfung des Einzelfalls unumgänglich.

3.4 Zivilrechtliche Aspekte

Wenn es um die Frage geht, welche zivilrechtlichen Aspekte bei der Schwachstellensuche zu beachten sind, ist insbesondere an eine mögliche Haftungsgefahr zu denken.

Generell werden Schwachstellensuchende und Anbieterinnen bzw. Anbieter darauf hingewiesen, dass auch im Rahmen des CVD-Prozesses die allgemeinen zivilrechtlichen Regelungen zur Anwendung kommen.

Werden bei der Suche nach Schwachstellen Schäden verursacht, so richtet sich die Haftung dafür nach dem allgemeinen Schadenersatzrecht. Insbesondere wenn kein Konsens über die Suche nach der Schwachstelle hergestellt worden ist, wird davon auszugehen sein, dass eine Schadenszufügung rechtswidrig und schuldhaft erfolgt ist. Die bzw. der Schwachstellensuchende wird daher einen allfälligen Schaden, wie etwa den Aufwand für notwendige Reparaturmaßnahmen, zu ersetzen haben.

Vor diesem Hintergrund ist es ratsam, jegliche Schädigung zu vermeiden oder vorab die Zustimmung für Eingriffe und damit potenziell verbundene, unvermeidbare Schäden einzuholen.

Auch in Zusammenhang mit einer möglichen Beeinträchtigung der wirtschaftlichen Tätigkeit von Anbieterinnen bzw. Anbietern sollte eine potenzielle Haftung von Schwachstellensuchenden bedacht werden. Anknüpfend daran wird Schwachstellensuchenden davon abgeraten, bei der Schwachstellensuche erlangte Informationen eigenständig weiterzugeben.

3.5 Datenschutzrechtliche Aspekte

Wenn es um die Frage der datenschutzrechtlichen Bewertung des CVD-Prozesses geht, wird im Allgemeinen auf Folgendes hingewiesen:

Neben den oben angeführten rechtlichen Rahmenbedingungen können in Zusammenhang mit der Offenlegung von Schwachstellen auch Fragen zur Verarbeitung personenbezogener Daten (die in einem Dateisystem gespeichert sind oder dort gespeichert werden sollen) auftreten. Der Schutz betroffener Personen bei der Verarbeitung personenbezogener Daten stützt sich auf Regelungen, denen mitunter ein weites Verständnis zugrunde liegt.

Um Schwachstellensuchende und Anbieterinnen bzw. Anbieter im CVD-Prozess zu schützen, gilt es auch hier, eine sorgfältige Prüfung des Einzelfalls vorzunehmen – dies gegebenenfalls durch externe Beratung und dies insbesondere zur Rechtmäßigkeit der Verarbeitung (Art 6 DSGVO beziehungsweise §§ 36 ff DSG) und zum Vorliegen von Betroffenenrechten (Art 12 bis 22 DSGVO und § 1 DSG) im konkreten Sachverhalt.

Einführend dazu werden Schwachstellensuchende und Anbieterinnen bzw. Anbieter auf folgende Grundzüge hingewiesen:

- **Verarbeitung (Art 4 Z 2 DSGVO)**

Darunter wird jeder, mit oder ohne Hilfe automatisierter Verfahren, ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung verstanden.

Die Verarbeitung personenbezogener Daten kann ganz oder teilweise automatisiert erfolgen. Darüber hinaus können auch physische Informationen (etwa Aktenordner) in den Schutzbereich der DSGVO fallen, sofern diese in einem Dateisystem (Art 4 Z 6 DSGVO) gespeichert sind oder gespeichert werden sollen. Ein Dateisystem liegt dann vor, wenn die (physischen) Informationen nach bestimmten Kriterien abgefragt werden können. Im Umkehrschluss sind etwa unstrukturierte Papierblätter nicht vom Anwendungsbereich der DSGVO umfasst.

Zu beachten ist jedoch, dass das Recht auf Geheimhaltung gemäß § 1 Abs. 1 DSG (welches „parallel“ zum Recht auf Datenschutz nach der DSGVO besteht) nicht auf eine spezifische Verarbeitungsform abstellt und daher personenbezogene Daten im Ergebnis immer zu schützen sind.

- **Personenbezogene Daten/Person**

Als personenbezogene Daten kommen alle Informationen in Frage, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen (Art 4 Z 1 DSGVO).

Zu beachten ist, dass in Österreich neben natürlichen Personen grundsätzlich auch juristische Personen durch das Datenschutzrecht geschützt werden (§ 1 DSG). Für einen Schutz nach der DSGVO kommt es dabei insbesondere auf die Bezeichnung der juristischen Person an. Im Rahmen eines CVD-Prozesses können grundsätzlich alle Varianten einschlägig sein.

Identifizierbar ist eine (natürliche) Person dann, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Im Zusammenhang mit dem CVD-Prozess können dies etwa E-Mail-Adressen, Identifikationsnummern, Online-Kennungen, IP-Adressen oder Standortdaten sein. Es kommt auf die Identifizierbarkeit der betroffenen Person an.

- **Rollendefinition**

Im Vordergrund steht die Frage der Rollendefinition: Je nachdem, ob jemand als (gemeinsam) Verantwortliche bzw. Verantwortlicher oder als Auftragsverarbeiterinnen bzw. Auftragsverarbeiter zu qualifizieren ist, ergeben sich unterschiedliche Rechtsfolgen (vergleiche einerseits die Pflichten nach Art 30 bis Art 37 DSGVO, andererseits den Umstand, dass die Verantwortliche bzw. der Verantwortliche die Adressatin bzw. der Adressat von Betroffenenrechten wie Auskunft, Berichtigung oder Löschung ist).

Der CVD-Prozess sieht keine pauschale Rollenverteilung nach datenschutzrechtlichen Gesichtspunkten vor, sodass dies im Einzelfall zu beurteilen sein wird. Denkbar sind im horizontalen Verhältnis insbesondere Konstellationen, in denen Schwachstellensuchende als Auftragsverarbeiterin bzw. Auftragsverarbeiter und Anbieterinnen bzw. Anbieter als Verantwortliche auftreten.

- **Verantwortliche**

Als Verantwortliche in Erscheinung treten können Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden (Art 4 Z 7 DSGVO). Für die Eigenschaft als Verantwortliche bzw. Verantwortlicher kommt es zudem nicht darauf an, dass diese bzw. dieser personenbezogene Daten tatsächlich selbst verarbeitet. Es reicht aus, wenn er die Entscheidung über Zwecke und Mittel dieser Verarbeitung getroffen hat, selbst wenn die Verarbeitung faktisch durch eine andere Stelle (etwa durch eine Auftragsverarbeiterin bzw. einen Auftragsverarbeiter) durchgeführt wird.

- **Auftragsverarbeiter**

Darunter werden Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten, verstanden (Art 4 Z 8 DSGVO). Die Verarbeitung durch die Auftragsverarbeiterin bzw. den Auftragsverarbeiter

erfolgt dabei entweder aufgrund eines Vertrags oder einer anderen Rechtsgrundlage, die sie bzw. ihn in Bezug auf die Verantwortliche bzw. den Verantwortlichen bindet und bei der Gegenstand und Dauer der Verarbeitung sowie deren Art und Zweck, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte der Verantwortlichen bzw. des Verantwortlichen festgelegt sind (Art 28 Abs 3 DSGVO).

- **Grundsätze für die Verarbeitung personenbezogener Daten (Art 5 DSGVO)**

  – Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Rechtmäßig ist die Verarbeitung nur bei Vorliegen einer der in Art 6 DSGVO genannten Bedingungen. Neben der für Schwachstellensuchende zentralen Einwilligung sind dort auch andere Möglichkeiten für eine rechtskonforme Verarbeitung (wie etwa die der Wahrnehmung einer Aufgabe im öffentlichen Interesse) angeführt.

Im Rahmen des § 9 DSG (bzw. Art 85 Abs 2 DSGVO) bestehen Ausnahmen von der DSGVO zugunsten der Freiheit der Meinungsäußerung und der Informationsfreiheit.

  – Zweckbindung

Grundsätzlich muss die Erhebung personenbezogener Daten für festgelegte, eindeutige und legitime Zwecke erfolgen und die Verarbeitung darf nicht in einer damit nicht zu vereinbarenden Weise erfolgen.

Auch im Rahmen einer Offenlegung von Schwachstellen gilt es zu prüfen, weshalb und wie personenbezogene Daten verarbeitet werden.

  – Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

  – Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Alle angemessenen Maßnahmen sind zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

– Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Sie dürfen länger gespeichert werden, soweit sie, vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von der DSGVO zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden.

– Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

– Rechenschaftspflicht

Die Verantwortliche bzw. der Verantwortliche ist für die Einhaltung oben angeführter Grundsätze verantwortlich und muss die Einhaltung dieser nachweisen können.

3.6 Information zu Art 10 EMRK

Wenn es um die Frage nach grundrechtlichen Aspekten geht, ist Art 10 der Europäischen Menschenrechtskonvention (EMRK) zentral:

Art 10 EMRK schützt neben der Meinung, wie sie im alltäglichen Sprachgebrauch verstanden wird, auch die Freiheit, Nachrichten und Informationen zu teilen und zu erhalten. Auch das Whistleblowing als Methode zur Bekanntgabe von für die Öffentlichkeit wichtigen Informationen, wird von Art 10 EMRK geschützt. Es handelt sich beim Recht nach Art 10 EMRK um unmittelbar anzuwendendes nationales Verfassungsrecht. Das heißt insbesondere, dass es nicht nur für Staaten untereinander gilt, sondern dass sich auch einzelne Personen darauf berufen können.

Im Falle des CVD-Prozesses bedeutet das, dass die Verringerung des (Cybersicherheits-) Risikos und die koordinierte Offenlegung von Schwachstellen ein Mittel sein kann, das im öffentlichen oder privaten Interesse liegt. Im Einzelnen ist dementsprechend auch während des Offenlegungsprozesses zu prüfen, ob Handlungen im Rahmen der Offen-

legung zur Erreichung dieses Ziels überhaupt geeignet sind, ob schonendere Handlungen denkbar sind, und ob schwerer ins Gewicht fallende Interessen anderer mit Handlungen im Rahmen der Offenlegung in Konflikt stehen.[10]

Auch in zivil- und strafrechtlichen Verfahren – also in Fällen, in denen sich Schwachstellensuchende Ansprüchen anderer ausgesetzt sehen oder gegen sie ein strafrechtlicher Vorwurf erhoben wird – muss die Informationsfreiheit im Wege der Interessenabwägung beachtet werden. So sind insbesondere Handlungen schützenswert, bei denen die Quelle (auf die man sich bezieht) selbst vertrauenswürdig ist oder diese über einen hohen Wahrheitsgehalt verfügt und der Beitrag einer Debatte von öffentlichem Interesse dient. Zu denken ist dabei an bewährte, in Fachkreisen anerkannte Methoden und Formate für den Bezug von Information. Eine Debatte von öffentlichem Interesse wird etwa dann vorliegen, wenn der Beitrag die Cybersicherheit für Unternehmerinnen und Unternehmer, Bürgerinnen und Bürger sowie für die Gesellschaft erhöht. Auch spielt es bei der Beurteilung eine Rolle, ob die Information in gutem Glauben bezogen wurde und beim Bezug der Information sorgfältig gehandelt wurde.

Schwachstellensuchende sollten daher im konkreten Anlassfall insbesondere folgende Gesichtspunkte prüfen:

- ob es sich bei den Umständen, die man findet und die man gedenkt offen zu legen, um falsifizierbare Feststellungen handelt;

- ob die Kenntnis der Umstände, die Gegenstand der Suche und Offenlegung sind, im allgemeinen Interesse liegt und ob ein solches allgemeines Interesse stark ausgeprägt ist (eine Schwachstelle kann zum Beispiel die Sicherheitslücke innerhalb eines Betriebssystems für Autos sein, das Außenstehenden ermöglicht, das Auto „fernzusteuern“ oder das Einsehen von Daten, auf die man eigentlich keinen Zugriff haben sollte);

- ob die Art und Weise, wie man zur Information gelangt oder gelangt ist, sorgfältig gewählt ist bzw. wurde und ob es sich dabei um eine seriöse, vertrauenswürdige Herangehensweise handelt.

Eine besondere Form der Freiheiten nach Art 10 EMRK ist die Medienfreiheit. Darüber hinaus ist in Österreich etwa ein Konzessionssystem, in dem Journalismus vom Bestehen einer Bewilligung abhängig gemacht wird, unzulässig. Auch ist die Zensur, in der Inhalte ex ante geprüft werden, unzulässig. Verfahrensrechtliche Sicherheiten, wie etwa die Anonymität von Quellen, spielen beim Schutz der journalistischen Meinungsfreiheit eine besondere Rolle, teilweise trifft den Staat in dem Zusammenhang eine Schutzpflicht.

---

10 Siehe Kapitel 2.3.

Als Schwachstellensuchende könnten Sie im Rahmen des CVD-Prozesses journalistisch tätig werden. Auch kann dieser Aspekt etwa dann von Bedeutung sein, wenn Schwachstellensuchende etwa einen Blog betreiben oder sonst medial auftreten. Schwachstellensuchende sollten ihre konkrete Situation vor diesem Hintergrund prüfen.

Insgesamt ist es für Schwachstellensuchende von besonderer Bedeutung, im Rahmen der Offenlegung von Schwachstellen verhältnismäßig zu handeln und sorgsam vorzugehen. Auch ist wichtig, dass Schwachstellensuchende bei der Vorgehensweise der Schwachstellensuche an sich sorgfältig vorgehen. Auch auf mögliche negative Folgen für andere sollte im Rahmen des CVD-Prozesses Bedacht genommen werden und insofern kein rücksichtsloses Verhalten gesetzt werden.

Schwachstellensuchende sollten die oben genannten rechtlichen Einflussfaktoren berücksichtigen, da diese für die Beurteilung ihrer Handlungen im Einzelfall (insbesondere für die Beurteilung, ob ihr Verhalten geschützt ist oder nicht) von Bedeutung sein können. Jedenfalls ist der Entscheidung über den CVD-bezogenen Sachverhalt im Einzelfall eine grundrechtskonforme Auslegung zugrunde zu legen. Insofern kann die Berücksichtigung der in dieser Policy dargestellten Parameter für die Frage, ob Schwachstellensuchenden aufgrund ihres konkreten CVD-Sachverhalts eine Verfolgung droht, von Bedeutung sein.

Für den Inhalt verantwortlich: BMI, BKA, BMJ (Straf- und Zivilrecht), DSB, CERT.at