Schwachstellen offenlegen

Unentdeckte Schwachstellen sind Einfallstore für Cyber-Angriffe. Mit der CVD-Policy setzt Österreich auf koordinierte Prozesse zur frühzeitigen Risikoerkennung und gezielten Gegensteuerung.

In einer zunehmend digitalisierten und vernetzten Gesellschaft sind digitale Produkte und Dienste zu tragenden Säulen des Alltags geworden – von Finanzdienstleistungen bis hin zu staatlichen Verwaltungsprozessen. Mit dieser Entwicklung wächst die Angriffsfläche für Cyber-Bedrohungen. Bislang unbekannte Schwachstellen stellen ein erhebliches Risiko dar, da zum Zeitpunkt ihrer Entdeckung noch keine Gegenmaßnahmen verfügbar sind. Um diesen Risiken strukturiert zu begegnen, hat Österreich im Jahr 2024 eine nationale *Policy zur Coordinated Vulnerability-Disclosure (CVD)* eingeführt. Die Policy wurde zwischen staatlichen Stellen, Forschungseinrichtungen und privaten Akteuren abgestimmt. Sie definiert Abläufe, Rollen und Verantwortlichkeiten und trägt zur Harmonisierung des Umgangs mit Sicherheitslücken bei. Zudem regelt sie den Prozess, wie Sicherheitslücken von ethischen Hackern an Hersteller gemeldet werden. Ziel ist es, Schwachstellen vor ihrer Veröffentlichung zu beheben, um Schäden zu minimieren und einen sicheren Meldekanal bereitzustellen. Im Dezember 2025 wurde im Nationalrat ein Entschließungsantrag zum Thema „Ethical Hacking straffrei stellen – proaktives Aufdecken von Sicherheitslücken zur Erhöhung der Cyber-Sicherheit“ eingebracht. In der Folge wurde beschlossen, die bestehende CVD-Policy weiterzuentwickeln. Die überarbeitete Fassung befindet sich in Finalisierung und soll im Sommer 2026 veröffentlicht werden.

Was ist eine Schwachstelle? Als Schwachstellen gelten technische oder konzeptionelle Fehler in Software, Hardware, Protokollen oder digitalen Diensten, die von Dritten ausgenutzt werden können. Ihre Entdeckung erfolgt häufig im Rahmen gezielter Analysen oder zufällig im Zuge der Nutzung. Die CVD-Policy stellt sicher, dass Erkenntnisse zunächst kontrolliert und an die zuständigen Stellen übermittelt werden, bevor eine Veröffentlichung erfolgt.

Wer ist beteiligt? Wer profitiert? Die Policy definiert Akteursgruppen:

Koordinierte Offenlegung von Schwachstellen stärkt die Cybersicherheit

- *Schwachstellensuchende* (insbesondere Sicherheitsforschende, Unternehmen sowie Nutzerinnen und Nutzer) identifizieren und melden Sicherheitslücken. Voraussetzung ist ein Handeln in guter Absicht („Ethical Hacker“) und im Interesse der allgemeinen Cyber-Sicherheit.
- *Anbieterinnen und Anbieter digitaler Produkte und Dienste* sind für die Analyse, Priorisierung und Behebung gemeldeter Schwachstellen verantwortlich. Die Policy unterstützt sie dabei, frühzeitig auf Risiken zu reagieren und geeignete Schutzmaßnahmen umzusetzen.
- *Koordinator (CSIRT):* Gemäß dem Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) übernimmt das nationale Computer-Security-Incident-Response-Team (CSIRT) eine koordinierende Rolle. Es unterstützt die Kommunikation zwischen den Beteiligten, strukturiert den Informationsfluss und wird insbesondere bei komplexen oder sektorübergreifenden Fällen aktiv.

Koordination schützt vor Risiken. Eine verfrühte Offenlegung kann ausgenutzt werden, bevor Schutzmaßnahmen verfügbar sind, während ein zu langes Zuwarten bestehende Risiken verlängert. Die Policy definiert klare Zeitrahmen, Kommunikationswege und Grundprinzipien wie Verhältnismäßigkeit, Kooperation und Datenschutz. Dies schafft Planungssicherheit für alle Beteiligten und stärkt das Vertrauen in den Umgang mit sicherheitsrelevanten Informationen. So wissen Schwachstellensuchende, Anbieterinnen und Anbieter sowie der Koordinator jederzeit, welche Schritte vorgesehen sind, und können Schäden für Nutzerinnen und Nutzer sowie die digitale Infrastruktur minimieren.

Von der Meldung zur Offenlegung. Der CVD-Prozess folgt einer strukturierten Abfolge: Identifikation und Verifikation der Schwachstelle, Meldung an die zuständige Stelle, Analyse und Risikobewertung, Entwicklung und Umsetzung von Gegenmaßnahmen sowie koordinierte Offenlegung (öffentlich oder zielgerichtet). Diese systematische Vorgehensweise ermöglicht eine kontrollierte Risikoreduktion und verhindert unkoordinierte Informationsabflüsse.

Mit der nationalen CVD-Policy etabliert Österreich einen einheitlichen Rahmen für den verantwortungsvollen Umgang mit Schwachstellen. Dies stärkt die technische Sicherheit digitaler Systeme und die institutionelle Resilienz gegenüber Cyber-Bedrohungen. Die Weiterentwicklung der Policy im Jahr 2026 unterstreicht die sicherheitspolitische Relevanz koordinierter Offenlegungsprozesse und trägt dazu bei, Österreichs Cybersicherheitsarchitektur zu stärken. *Alexander Bernard*

FOTO: ZABHIE - STOCK.ADOBE.COM