Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Vulnerability Disclosure Management

Ein Leitfaden für Organisationen und Unternehmen

01.02.2024

Inhaltsverzeichnis

1 Einführung

Wird eine IT-Schwachstelle in den Systemen oder Produkten Ihrer Organisation oder Unternehmung von einer unternehmensinternen oder -externen Person entdeckt, sollte dies umgehend und anhand eines klar definierten Prozesses der dafür zuständigen IT-Stelle in Ihrem Unternehmen / Ihrer Organisation gemeldet werden können.

Durch ein klares und einfach verständliches Meldeverfahren können Organisationen und Unternehmen jeder Grösse Informationen zu Schwachstellen direkt erhalten und diese somit rascher und zielgerichteter beheben. Ein klar definiertes Meldeverfahren zeigt, dass die Organisation / Unternehmung das Thema Sicherheit ernst nimmt und bestrebt ist, ihre Systeme und Produkte stetig zu verbessern.

Der vorliegende Leitfaden des Bundesamtes für Cybersicherheit (BACS) zur Offenlegung von Schwachstellen («Vulnerability Disclosure») richtet sich an Organisationen und Unternehmen und soll helfen, ein solches Meldeverfahren in ihrem Betrieb zu implementieren. Es umfasst die drei wesentlichen Komponenten: Kommunikation, Richtlinie und «security.txt».

Der Leitfaden basiert im Wesentlichen auf der internationalen Norm für die Offenlegung von Schwachstellen (ISO/IEC 29147:2018). Sie definiert die Techniken und Richtlinien, die für den Empfang von Schwachstellenmeldungen und die Veröffentlichung von Informationen zur Behebung von Schwachstellen verwendet werden können. Die Norm ISO/IEC 29147:2018 wurde vom «European Committee for Standardization» (CEN) am 3. Mai 2020 angenommen.

1.1. Ziele bei der Offenlegung von Schwachstellen

Die Offenlegung von Schwachstellen ermöglicht einerseits die Behebung der Schwachstellen und andererseits bewusstere Risikoentscheidungen. Gemäss ISO/IEC 29147:2018 gehören zu den prioritären Zielen bei der Offenlegung von Schwachstellen:

- Risikominderung durch Beheben von Schwachstellen und Informieren der Anwenderinnen und Anwender;
- Minimieren von Schäden und Kosten;
- Bereitstellen von ausreichend Informationen für die Anwenderinnen und Anwender, um die durch die Schwachstellen entstehenden Risiken zu bewerten;
- Festlegen der Erwartungshaltung aller Beteiligter, um Interaktion und Koordination zwischen den Beteiligten zu erleichtern.

2 Komponenten des BACS Leitfadens

Der vorliegende Leitfaden enthält drei wesentliche Komponenten für den Prozess zur Offenlegung von Schwachstellen:

2.1 Kommunikation

2.1.1 Spezifische Kontaktdaten verfügbar machen

Entscheidend ist eine schnelle und unkomplizierte Kommunikation für alle Beteiligten.
Haben Mitarbeitende Ihrer Organisation oder Unternehmung, Sicherheitsforschende, ethische Hacker, das BACS oder grundsätzlich die Öffentlichkeit Kenntnis von einer technischen Schwachstelle in Ihrer Organisation oder Unternehmung, ist es entscheidend, dass diese die zuständige IT-Stelle zur Behebung der Schwachstelle schnell finden und kontaktieren können.

Häufig sind diese spezifischen (Kontakt-)Daten nicht verfügbar. Auf der jeweiligen Internetseite ist oft nur eine zentrale Telefonnummer oder eine allgemeine E-Mail-Adresse aufgeführt. Als Konsequenz muss sich die meldende Person bis zur richtigen Ansprechperson durchfragen und das Problem mehrfach erklären, dadurch vergeht oft wertvolle Zeit. Bis die Information bei der verantwortlichen Person ankommt, kann es unter Umständen schon zu spät sein. Oft kommt es auch vor, dass diese Informationen gar nicht weitergeleitet und ignoriert werden und die dafür zuständige Stelle keine Kenntnis über die Schwachstelle erhält. Dies ist frustrierend für die meldende Person, aber auch ärgerlich für die betroffene Organisation / Unternehmung und eine verpasste Chance, die eigene Cybersicherheit zu verbessern.

Um diesem Problem entgegenzuwirken, müssen die Kontaktdaten der IT-Verantwortlichen leicht zu finden sein oder es sollte zumindest ein Meldeprozess innerhalb der Unternehmung definiert sein. Das BACS empfiehlt die Einbindung Ihrer Kontaktdaten auf der Internetseiten-Navigation «Kontakt». Zusätzlich sollten die Kontaktoptionen in einer speziell dafür erstellten Datei «security.txt» erfasst und auf der Internetseite abgelegt werden. (siehe dazu Komponente «security.txt»).

2.1.2 Technische Voraussetzungen

Mit einer eigens dafür eingerichteten E-Mail-Adresse oder einem Web-Formular wird sichergestellt, dass die Informationen der meldenden Person an die richtige Stelle in Ihrer Organisation / Unternehmung weitergeleitet werden.

Kommt ein webbasiertes Meldeverfahren (z. B. Web-Formular) zum Einsatz, muss die Übertragung der Daten verschlüsselt erfolgen, z. B. durch den Einsatz von TLS (HTTPS). Eine

Kommunikation über E-Mail sollte über verschlüsselte und signierte Verfahren wie S/MIME oder PGP erfolgen. Die dafür erforderlichen öffentlichen Schlüssel sollen auf der Internetseite abgelegt und zugänglich sein.

Ein Beispiel eines solchen Webformulars findet sich auf Internetseite des BACS:

https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html

2.1.3 Prozess

Der vorliegende Leitfaden definiert vier Schritte im Schwachstellenbehandlungsprozess:

Meldungseingang:
Erhalten Sie die Meldung über eine mögliche Schwachstelle, sollten Sie den Meldungseingang möglichst unverzüglich, aber spätestens innerhalb von sieben Kalendertagen bestätigen und sich bei der meldenden Person bedanken. Die Antwort kann automatisch generiert sein, sollte aber aussagekräftig sein. Die Antwort sollte eine Verfolgungsnummer oder eine Kennung enthalten sowie vorläufige Statusinformationen.

Verifizierung:
Anschliessend erfolgt die Prüfung und Verifikation der gemeldeten Schwachstelle. Bei einer hohen Anzahl von Meldungen sollte eine Triagierung anhand der Risikobetrachtung der Schwachstellen erfolgen. Nach erfolgter Prüfung empfehlen wir Ihnen, die meldende Person über das Ergebnis dieser Erstbeurteilung zu informieren.

Schwachstellenbehandlung:
Während dem weiteren Verlauf der Schwachstellenbehandlung sollten Sie mit der meldenden Person regelmässig kommunizieren. Diese Kommunikation sollte folgende Informationen enthalten:

- Statusaktualisierungen;
- relevante neue Informationen;
- Änderungen an bestehenden Plänen;
- Zeitplan für die Offenlegung.

Veröffentlichung:
Die Kommunikation ist das wesentliche Element. Ein einfach zu findender Kontaktweg sowie eine prompte, transparente und wertschätzende Kommunikation während der ganzen Schwachstellenbehandlung fördern das Engagement und die Motivation der meldenden Personen.

2.2 Richtlinie

Mit einer klaren Richtlinie legen Sie fest, was Sie einerseits von jemandem erwarten, der eine Schwachstelle meldet und anderseits, was die meldende Person von Ihrer Organisation / Unternehmung erwarten kann. Das bedeutet, dass die Meldenden mit Ihnen in einem vereinbarten Rahmen arbeiten können.

Gemäss ISO/IEC 29147:2018 gelten für Richtlinien zur Offenlegung von Schwachstellen zwingende und empfohlene Angaben:

- Kontaktaufnahmeverfahren, z. B. Link/E-Mail oder Web-Formular **(zwingend)**
- Im Schwachstellenbericht anzugebende Informationen, siehe auch ISO/IEC 29147:2018, Anhang B **(empfohlen)**
- Anforderungen an die Kommunikation **(empfohlen)**
- Würdigung **(empfohlen)**
- Rechtliche Aspekte **(empfohlen)**

Ein Beispiel einer solchen Richtlinie finden Sie auf der Internetseite des BACS:
https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html

Weitere Beispiele solcher Richtlinien finden sich in ISO/IEC 29147:2018, Anhang A.

2.3 Security.txt

Der Standard «security.txt» ermöglicht es, den richtigen Sicherheitskontakt in einer Organisation / Unternehmung schnell zu finden. Der Standard gibt vor, eine Textdatei mit dem Namen «security.txt» im vordefinierten Verzeichnis «/.well-known» auf dem Webserver der Internetseite abzuspeichern. In dieser Datei sind mindestens die Kontaktdaten abgespeichert, mit denen man sich mit den Sicherheitsverantwortlichen einer Internetseite respektive einer Organisation oder Unternehmung in Verbindung setzen kann. Zusätzlich können auch Links zu Verschlüsselungs-Keys, Sicherheitsrichtlinien, speziellen Vulnerability Disclosure- oder Bug-Bounty-Programmen deponiert werden.

Seit April 2022 wurde dieser Standard auch offiziell als «RFC 9116» verankert und wird weltweit im Internet immer häufiger sowohl von Tech-Firmen wie auch von Regierungsorganisationen eingesetzt.

Die «security.txt» Datei beinhaltet zwingende und optionale Angaben:

Was	**Beschrieb**	**Zwingend notwendig**	**Optional**
Kontakt	Ein Link oder eine E-Mail-Adresse, über die die Organisation oder Unternehmung bei Sicherheitsfragen kontaktiert werden kann. Denken Sie daran, bei URLs «https://» und «mailto:» anzugeben.	X	

Ablaufdatum	Datum und Uhrzeit, ab wann der Inhalt der Datei «security.txt» als veraltet betrachtet werden sollte. Stellen Sie sicher, dass Sie diesen Wert regelmässig aktualisieren und Ihre Datei ständig überprüfen.	X	
Bevorzugte Sprache	Eine durch Kommas getrennte Liste von Sprachen, die Ihre IT-Stelle spricht. Sie können mehr als eine Sprache angeben		X
Verschlüsselungsoptionen	Ein Link zu einem Schlüssel (z. B. PGP oder S/MIME), den Sicherheitsforscher verwenden können, um sicher mit Ihnen zu kommunizieren.		X
Verdankungen	Ein Link zu einer Internetseite, auf der die Organisation / Unternehmung sich bei Sicherheitsforschern bedankt, die Ihnen ein Sicherheitsproblem gemeldet haben und eine solche Erwähnung wünschen. Denken Sie daran «https://» anzugeben.		X
Link zur Datei security.txt	Die URLs für den Zugriff auf Ihre security.txt-Datei. Es ist wichtig, diese anzugeben, wenn Sie die Datei security.txt digital signieren, damit der Speicherort der Datei security.txt ebenfalls digital signiert werden kann.		X
Policy	Ein Link zu einer Richtlinie, die beschreibt, wie Sicherheitsforscher vorgehen sollten, wenn sie Ihnen Sicherheitsprobleme melden wollen. Denken Sie daran «https://» anzugeben.		X
Jobangebote	Ein Link zu allen sicherheitsrelevanten Stellenangeboten in Ihrem Unternehmen. Denken Sie daran «https://» anzugeben.		X

Diese Aufzählung ist nicht abschliessend. Weitere Informationen finden Sie im Standard RFC9116 (siehe Anhang).

2.3.1 Beispiel «security.txt» des BACS-Internetauftrittes

https://www.ncsc.admin.ch/.well-known/security.txt

```
# In the event that you have discovered a technical vulnerability in an IT system of the federal government,
# we encourage you to report it to the National Cyber Security Centre NCSC using the Coordinated Vulnerability
Disclosure program.
# We forward your request to the appropriate unit.
# If you are interested in participating in the NCSC bug bounty programs you can apply here: https://www.bug-
bounty.ch/ncsc

Contact: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-mel-
den.html
Contact: mailto:incidents@ncsc.ch
Expires: 2024-12-31T23:59:59.000Z
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/pgp_ncsc_incidents.asc.download.asc/NCSC_Incidents.asc
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/smime_incidents_ncsc_ch_22.cer.download.cer/
smime_incidents_ncsc_ch_22.cer
Preferred-Languages: en, de, fr, it
Canonical: https://www.ncsc.admin.ch/.well-known/security.txt
Policy: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-
melden/scope-and-rules.html
```

3 Links

ISO/IEC 29147:2018 Standard: Vulnerability disclosure
https://www.iso.org/standard/72311.html

ENISA - Coordinated Vulnerability Disclosure policies in the EU
https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu

IETF - RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure
https://www.ietf.org/rfc/rfc9116.pdf

OSCE learning: cyber/ICT security CBM 16: Coordinated Vulnerability Disclosure
https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about

BACS - Im Fokus: Vermeintliche Sicherheitsforscher drängen auf eine Belohnung
https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/wochenrueckblick_38.html