Responsible Disclosure

Meldung von Schwachstellen vor Veröffentlichung

OZG-Security-Challenge 2023

Stand: 02.04.2023 BETA

Management Summary

Ethisch motivierte Hackerinnen und Hacker (White Hats) wollen gefundene Sicherheitslücken erst für die Allgemeinheit veröffentlichen, nachdem diese geschlossen wurden. Aus Sicht des Betreibers schafft die Angabe eines Kontakts zur Meldung ein wertvolles Zeitfenster. In diesem können die Sicherheitsprobleme behoben werden, bevor potenzielle Angreifende diese für Schäden oder Datenabflüsse ausnutzen können.

Ressourcenabschätzung

Gering
(< 5 PTEinrichtungsaufwand)

Ohne neue Hardware

Erläuterung für Onlinedienst-Verantwortliche

Beim Responsible Disclosure Verfahren wird eine Schwachstelle für die Allgemeinheit erst mit einer Verzögerung veröffentlicht. Die Vorabmeldung verschafft dem Betreiber ein Zeitfenster zur Behebung des Sicherheitsproblems. Aufgrund der Sensibilität der Informationen sind die bestehenden Kommunikationskanäle wie der First-Level-Support hierfür nicht geeignet. Es gibt einen Internet-Standard zur Veröffentlichung dieser Kontaktmöglichkeit, welcher Format und Pfad innerhalb des Onlinedienstes definiert. Darüber hinaus ist ein Prozess zur Behandlung der Sicherheitsmeldung in angemessener Zeit notwendig. In der Regel kann hier auf bereits vorhandene Prozesse aufgesetzt werden.

Referenz

BSI APP.3.2.A20
RFC 9116
securitytxt.org
rc3.zerforschung.org

Umsetzung

Softwareentwicklung oder/und RZ-Betrieb

Technischer Umsetzungsansatz

Für Responsible Disclosure wird eine Text-Datei (text/plain) mit den Kontaktinformationen im Pfad „/.well-known/security.txt“ abgelegt (vgl. RFC 9116). Es empfiehlt sich die Angabe eines öffentlichen PGP-Schlüssels zur Verschlüsselung. Aufgrund der latenten Gefahr einer Strafanzeige nach §202c StGB (Hackerparagraf) erhöhen anonyme Kontaktmöglichkeiten die Meldewilligkeit. Die Behandlung der Sicherheitsmeldungen sollte auf etablierte Prozessstrukturen aufsetzen, z.B. analog CERT-Meldungen. Durch eine Funktionsmailadresse erreichen die sensiblen Informationen direkt und zuverlässig den richtigen Adressatenkreis. Bei Meldung einer Sicherheitslücke durch ethische motivierte Hackerinnen und Hacker empfiehlt sich ein wertschätzender Umgang. Sie haben die Lücke nur gefunden, nicht eingebaut und helfen Onlinedienste sicherer zu machen.

```
# For Coordinated Vulnerability Disclosure
Contact: mailto:vulnerability@bsi.bund.de
# For BSI related Security Issues
Contact: mailto:certbund@bsi.bund.de
Contact: https://www.bsi.bund.de/Security
-Contact
Encryption: https://www.bsi.bund.de/Security
-Contact
Expires: 2099-06-29T12:00:00.000Z
Preferred-Languages: de, en
Canonical: https://bsi.bund.de/.well-known/
security.txt
Hiring: https://www.bsi.bund.de/Jobs
CSAF: https://cert-bund.de/.well-known/csaf/
provider-metadata.json
```

security.txt für die Webseite des BSI (exemplarisch)

Bundesministerium des Innern und für Heimat
Bundesamt für Sicherheit in der Informationstechnik

OZG Onlinezugangsgesetz