EMPFEHLUNG: IT FÜR ORGANISATIONEN

Sicherheitskontakte mit Hilfe einer security.txt nach RFC 9116 angeben

Meldungen zu Schwachstellen empfangen

Soft- und Hardware ist ab einem gewissen Komplexitätsgrad fehlerbehaftet. Schwachstellen können daher zu jeder Zeit, in jedem Produkt oder in jeder Komponente gefunden werden: Schwachstellen sind allgegenwärtig. Es ist dennoch wichtig zu differenzieren, ob Soft- oder Hardware-Fehler potenziell sicherheitsrelevante Schwachstellen, auf die schnell reagiert werden muss, darstellen oder nicht.

Organisationen sollten ihre eigenen Produkte regelmäßig auf Schwachstellen prüfen, um sie ggf. mit Patches und Updates zu versorgen. Sicherheitslücken werden jedoch auch von unabhängigen Sicherheitsforschenden oder anderen gefunden. Oftmals stoßen diese durch Zufall auf Schwachstellen oder finden sie, weil sie sich mit bestimmten Produkten oder Produktgruppen auseinandersetzen. Die Findenden sind darauf angewiesen, dass die Informationen bei der Organisation an der richtigen Stelle und über geeignete Kanäle ankommen. Da es sich um sensible Informationen handeln kann, ist es sinnvoll, dass nicht nur die Informationsweitergabe standardisiert erfolgt, sondern auch die Echtheit des angegebenen Kontakts, optional kryptografisch gesichert, bestätigt wird.

Ziel

Um Sicherheitsforschenden und anderen das Auffinden des passenden Kontakts in Organisationen zu erleichtern, wurde die security.txt[1] ins Leben gerufen. Sie ist durch RFC 9116[2], der im April 2022 von der IETF (Internet Engineering Task Force) veröffentlicht wurde, definiert. Die security.txt ist eine Datei, die relevante Kontaktinformationen (siehe Abbildung 1) in menschen- und maschinenlesbarer Form bereitstellt. Sie befindet sich an einem definierten Ort auf der Internetseite der Organisation, wodurch die Kontaktaufnahme vereinfacht wird und sie mittels automatischer Werkzeuge (z. B. per Web-Crawler) gefunden werden kann. Viele Firmen, aber auch Behörden, haben eine security.txt bereits implementiert. Die security.txt ist als Ergänzung zu bereits bestehenden Kommunikations-Kanälen, Richtlinien und Informationen anzusehen und nicht als deren Ersatz. Organisationen, die noch keinen Kontakt für

[1] https://securitytxt.org/
[2] https://www.rfc-editor.org/info/rfc9116

Sicherheitsforschende und andere anbieten, haben mit der security.txt ein eindeutig spezifiziertes und einfach zu implementierendes Werkzeug an der Hand.

Darüber hinaus muss es innerhalb der Organisation Prozesse geben, wie mit den eingehenden Meldungen umgegangen wird. Diese sind beispielsweise in der BSI Cyber-Sicherheitsempfehlung Handhabung von Schwachstellen[3] beschrieben.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

# Our canonical URI
Canonical: https://example.com/.well-known/security.txt

# Our security address
Contact: mailto:security@example.com
Contact: mailto:productsecurity@example.com
Contact: https://example.com/security/contact.html
Contact: tel:+49-69-9000-9116

# Our OpenPGP key
Encryption: https://example.com/security/pgp-key.asc

# Our security acknowledgments
Acknowledgments: https://example.com/security/hall-of-fame.html

# Our preferred languages
Preferred-Languages: en, de, fr, nl, es

# Our security policy
Policy: https://example.com/security/disclosure-policy.html

Expires: 2024-12-31T00:00:00.000Z
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.2

[signature]
-----END PGP SIGNATURE-----
```

Abbildung 1 Beispiel einer signierten security.txt-Datei mit verpflichtenden, minimalen Angaben, Kommentaren und zusätzlichen Angaben

Aufbau und Inhalt der security.txt

Die security.txt ist eine Textdatei in Klartext und muss über HTTPS abrufbar sein. Sie enthält zum einen verpflichtende, minimale sowie zusätzliche Angaben. Prinzipiell kann sie aber weitere Felder mit Angaben enthalten, wobei jedes Feld in einer eigenen Zeile steht und jede Zeile mit einem Zeilenumbruch enden muss. Es ist zudem möglich, Kommentare zu einzelnen Feldern beizufügen. Eine digitale Signatur (mittels OpenPGP nach RFC 4880[4]) für die security.txt ist empfehlenswert, insbesondere in Verbindung mit dem Feld

[3] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf
[4] https://www.rfc-editor.org/rfc/rfc4880#section-7

Canonical, um den Ort der security.txt zu authentifizieren. Darüber hinaus können Organisationen auch weitere Informationen, wie Richtlinien zum Umgang mit Schwachstellenmeldungen und deren Veröffentlichung, hinterlegen (bspw. Coordinated Vulnerability Disclosure, CVD).

Verpflichtende, minimale Angaben

Contact (Kontaktinformation)

Diese Angabe spezifiziert den primären Kontakt zu der Organisation. Es handelt sich entweder um eine URL (Uniform Resource Locator, gemäß RFC 7230[5] und RFC 3986[6]) oder um eine E-Mail-Adresse (im Format mailto:security@example.com, gemäß RFC 6068[7]) oder um eine Telefonnummer, gemäß RFC 3966[8].

Expires (Ablaufdatum)

Diese Angabe muss entsprechend RFC 3339[9] umgesetzt sein und zeigt Sicherheitsforschenden und anderen, dass die Daten des Sicherheitskontakts noch gültig sind. Dieser Zeitstempel ist dabei zwingend mit einem großgeschriebenen T als Trennzeichen zwischen Datums- und Uhrzeitfeld, gemäß RFC 3339 Abschnitt 5.6, anzugeben.

Zusätzliche Angaben

Encryption (Verschlüsselung)

In diesem Feld ist eine URI (Uniform Resource Identifier, gemäß RFC 7230) angegeben, die zum öffentlichen OpenPGP-Schlüssel der Organisation führt. Dieser kann von Sicherheitsforschenden und anderen zum Verschlüsseln von Nachrichten an die Organisation genutzt werden. Dieser Schlüssel unterscheidet sich von dem für die digitale Signatur verwendeten. Die Prüfung der Authentizität des Schlüssels liegt in der Verantwortung der Meldenden.

Acknowledgments (Danksagung)

Dieses Feld verweist auf eine Webseite, auf der Sicherheitsforschende für ihre Schwachstellenfunde wertgeschätzt werden können (hall of fame).

Preferred-Languages (bevorzugte Sprachen)

Hier kann angegeben werden, welche natürlichen Sprachen, gemäß BCP 47/RFC 5646[10], für die Übermittlung von Sicherheitsmeldungen von der Organisation akzeptiert werden. Es können mehrere Sprachen angegeben werden, die mittels Komma separiert werden. Eine einzelne Sprache wird dabei als Primary Language Subtag gemäß BCP 47 Abschnitt 2.2.1[11] angegeben. Wenn dieses Feld nicht genutzt wird, dann ist davon auszugehen, dass die Organisation englischsprachige Meldungen akzeptiert.

Canonical (kanonische URI)

Die kanonische URI (gemäß RFC 7230) gibt an, wo die security.txt zu finden ist. Mit Hilfe der digitalen Signatur kann dieser Ort überprüft werden und bietet so Sicherheitsforschenden die Möglichkeit zur Validierung.

[5] https://www.rfc-editor.org/info/rfc7230
[6] https://www.rfc-editor.org/info/rfc3986
[7] https://www.rfc-editor.org/info/rfc6068
[8] https://www.rfc-editor.org/info/rfc3966
[9] https://www.rfc-editor.org/info/rfc3339
[10] https://www.rfc-editor.org/rfc/rfc5646.html#section-2.2.1
[11] https://www.iana.org/assignments/language-subtag-registry/language-subtag-registry

Policy (organisationsspezifische Richtlinien)

Diese Angabe verweist auf eine Verknüpfung zu organisationsspezifischen Richtlinien, beispielsweise zum Umgang mit der Veröffentlichung von Schwachstellen oder der Wertschätzung von Meldenden.

Hiring (Stellenangebote)

Die Organisation kann mit Hilfe dieser Angabe auf offene Stellen aufmerksam machen.

CSAF (Common Security Advisory Framework)

In diesem Feld kann in Form einer URI (gemäß RFC 7230) auf die provider-metadata.json für CSAF-Dokumente verwiesen werden.

Lokalisation und Implementierung der security.txt

Die Implementierung einer security.txt kann mit wenig zeitlichem Aufwand realisiert werden. Sie muss mindestens mittels HTTP 1.0 oder einer höheren Version per HTTPS abrufbar sein. Sollte eine HTTP-Weiterleitung notwendig sein, beispielsweise aufgrund einer vorgegebenen Webseitenstruktur, so sollten Meldende diese überprüfen, um sicherzustellen, dass es sich nicht um eine Kompromittierung handelt.

Empfehlung 1: Lokalisation der security.txt

Es wird eine Datei mit dem Namen security.txt im Pfad /.well-known/ (also /.well-known/security.txt) oder direkt unterhalb des Wurzelverzeichnisses einer Website (also /security.txt) erstellt. Die security.txt-Datei muss eine Klartextdatei mit ASCII- bzw. UTF8-Kodierung sein, wobei für Nicht-Kommentare nur die ASCII-Zeichen 0x20 bis 0x7E verwendet werden dürfen.

Empfehlung 2: Unterscheidung der Kontaktinformation für Produkte und Services

Bei den Kontaktinformationen sollte zwischen den Kontakten für Produkte und Services (klassisch: PSIRT mit mailto:psirt@example.com bzw. ProductCERT mit mailto:productcert@example.com) und denen für Infrastruktur (klassisch SOC/CERT/CSIRT mit mailto:security@example.com, mailto:cert@example.com oder mailto:csirt@example.com) unterschieden werden. Dies erfolgt üblicherweise durch die Verwendung von zwei verschiedenen E-Mail-Adressen. So kann, insbesondere in größeren Organisationen, sichergestellt werden, dass die Informationen zu Schwachstellenfunden an der richtigen Stelle ankommen.

Empfehlung 3: Angabe des Wertes für Expires

Bei Expires ist darauf zu achten, dass dieser Wert regelmäßig überprüft und ggf. erneuert wird. Üblicherweise sollte ein Datum, das weniger als ein Jahr in der Zukunft liegt, gewählt werden. Dies senkt die Wahrscheinlichkeit, dass die security.txt inkorrekte Daten enthält.

Empfehlung 4: Verpflichtende, minimale und zusätzliche Angaben

Die Angaben Contact und Expires sind verpflichtende, minimale Angaben in einer security.txt-Datei. Zusätzlich können noch die zuvor genannten, zusätzlichen Angaben, wie Encryption, Acknowledgements, Preferred-Languages, Canonical, Policy, Hiring und CSAF, hinzugefügt werden.

Empfehlung 5: Auffinden der security.txt mittels Web-Crawlern

Für die Nutzung von Werkzeugen, wie z. B. https://findsecuritycontacts.com/ oder https://www.internet.nl/, muss die security.txt automatisiert (d. h. mittels Web-Crawlern) gefunden werden können. Daher sind Firewall-Regeln und DDoS-Schutzregeln ggf. entsprechend anzupassen.

Empfehlung 6: Nutzung einer digitalen Signatur und einer kanonischen URI

Die Nutzung einer digitalen Signatur und kanonischen URI können vor Webseitenmanipulationen durch Angreifende schützen. Dennoch sollten die security.txt und die URI, die auf sie referenziert, regelmäßig überprüft werden, um Missbrauch zu verhindern.

Empfehlung 7: Veröffentlichung von organisationsspezifischen Richtlinien

Die Veröffentlichung von organisationsspezifischen Richtlinien stellt klar, wie diese Organisation mit Schwachstellenfunden umgeht und wie sie Sicherheitstests gegenübersteht.

Weitere Informationen

Eine Vielzahl von Risiken und Bedrohungen kann nicht alleine durch die Umsetzung technischer Maßnahmen, wie einer security.txt-Datei, sondern vielmehr durch die Kombination von organisatorischen Regelungen und technischen Maßnahmen minimiert werden. Die in diesem Dokument vorgeschlagene Implementierung einer security.txt ist eine grundlegende Maßnahme. Sie hilft dabei definierte Kontaktstellen zu einer Organisation zu benennen und somit die Zeit zu verkürzen, eine Schwachstelle zu melden. Weiterführende Informationen zum Common Security Advisory Framework (CSAF) oder zu Coordinated Vulnerability Disclosure-Prozessen, die weitere wichtige Teile des Schwachstellenmanagementprozesses darstellen und auch in der security.txt hinterlegt sein können, sind auf den Webseiten des BSI verfügbar:

https://www.bsi.bund.de/csaf

https://www.bsi.bund.de/dok/schwachstellenmeldung

für Rückfragen zu diesem Thema steht das BSI unter folgender E-Mail-Adresse zur Verfügung:

vulnerability@bsi.bund.de

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.