Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT-HERSTELLER

Handhabung von Schwachstellen

Empfehlungen für Hersteller

Viele Unternehmen verfolgen bei der Information über Schwachstellen häufig das Prinzip „Security by Obscurity“, d. h. es werden keine oder nur unzureichende Informationen über mitunter gravierende Schwachstellen veröffentlicht. Jedoch kann gerade diese Denkweise dazu führen, dass Angreifer solche Schwachstellen ausnutzen, wenn sie bereits durch eigene Erkenntnisse oder den Zukauf aus entsprechenden Quellen bekannt sind. In letzter Konsequenz werden somit die Anwender der betroffenen Softwareprodukte geschädigt. Nach dem Prinzip des „Coordinated Disclosure“ (auch „Responsible Disclosure“) wird bei der Veröffentlichung von Schwachstellen ebenfalls selten verfahren. „Koordiniert“ bedeutet, dass eine Schwachstelle zunächst vertraulich an den Hersteller gemeldet wird. Der Entdecker kooperiert mit dem Hersteller bei Analyse und Behebung der Schwachstelle. Informationen zur Schwachstelle werden Dritten erst dann zugänglich gemacht, wenn die Risiken für die Betroffenen hinreichend minimiert werden konnten. Der Grund, warum Entdecker einer Schwachstelle diesem Prinzip häufig nicht folgen ist, dass der jeweilige Hersteller keine hinreichenden oder leicht aufzufindenden Kontaktmöglichkeiten anbietet oder nach einer schwachstellenspezifischen Kontaktaufnahme nicht mehr reagiert.

Dieses Dokument beschreibt Empfehlungen zum richtigen Umgang mit Schwachstellen – sowohl für Hersteller von Software als auch von Geräten mit Firmware. Dabei werden interne Vorbereitungen, das Etablieren von Kommunikationskanälen, das eigentliche Incident Handling sowie die Nachbereitung behandelt. Hersteller, die diese Empfehlungen berücksichtigen, werden sich mitunter deutlich von Mitbewerbern absetzen können, was nicht zuletzt Kundenzufriedenheit und Unternehmenserfolg positiv beeinflusst.

Ergänzend zu diesem Dokument stellt die BSI-Veröffentlichung „Lebenszyklus einer Schwachstelle“[1] die Grundlagen zu Schwachstellen allgemein und zu Prinzipien, wie „Coordinated Disclosure“ und „Full Disclosure“ vor.

1 Interne Vorbereitung

Schon bevor eine Schwachstelle gemeldet wird, sollte ein Hersteller eine Reihe sinnvoller Vorbereitungen treffen. Insbesondere ist der Umgang mit Schwachstellen innerhalb des Unternehmens zu regeln. Dies umfasst

- Disclosure Policy,
- Rollen und Berechtigungen (Wer hat welche Aufgaben und Befugnisse?),
- Interne Prozesse inklusive zeitlicher Fristen (garantierte Antwortzeiten) für das Nachstellen und die Analyse der Schwachstelle, das Erarbeiten von Workarounds sowie Entwicklung und Testen von Patches.

1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Praesentationen/Lebenszyklus_einer_Schwachstelle.html

- Die Erkenntnis, dass der professionelle Umgang mit Schwachstellen in Produkten sowohl hinsichtlich der eigenen Kunden als auch der Entdecker einer Schwachstelle erforderlich ist.

Die sogenannte „Disclosure Policy“ (auch „Vulnerability Handling Policy“) ist eine Leitlinie, in welcher der Hersteller den Umgang mit Schwachstellen definiert. Sie ist die Grundlage für die vertrauensvolle Zusammenarbeit zwischen Herstellern und Sicherheitsexperten. Hierzu liefert diese Policy detaillierte Informationen, wie der Hersteller den Begriff „Coordinated Disclosure“ interpretiert und was dies für einen Sicherheitsexperten bedeutet, der eine Schwachstelle meldet. Zudem werden Zusicherungen darüber gemacht, wie der Hersteller mit den Daten und Informationen des Sicherheitsexperten hinsichtlich Vertraulichkeit und einer möglichen Veröffentlichung umgeht. Auch sollte die Erwartungshaltung an den Sicherheitsexperten dargestellt werden. Die Disclosure Policy sollte detaillierte Informationen über die internen Prozesse hinsichtlich der Behandlung von Schwachstellen bzw. den damit verbundenen Folgen für den Sicherheitsexperten enthalten. So kann der Hersteller beispielsweise vom Entdecker erwarten, dass Informationen zur Schwachstelle erst dann veröffentlicht oder weiterverwendet werden, wenn in einem angemessenen Zeitraum ein Patch veröffentlicht wird und die Betroffenen hinreichend Zeit zur Aktualisierung hatten. Sollten Informationen zur Schwachstelle durch Dritte veröffentlicht oder die Schwachstelle bereits öffentlich ausgenutzt werden, wird empfohlen, dass Hersteller und Entdecker in Abstimmung auch Informationen zur Schwachstelle publizieren.

Um Sicherheitsexperten nicht abzuschrecken, sollte der Hersteller möglichst auf formelle oder juristische Verträge oder Vereinbarungen, wie Non-disclosure Agreements (NDA), verzichten. Insbesondere empfiehlt es sich für die Hersteller-Seite, eine klare Aussage dahingehend zu treffen, dass Entdecker einer Schwachstelle keine juristischen Schritte zu befürchten haben, sofern sie sich an die Regelungen und Vorgaben des Herstellers halten.

Zudem sollte die Disclosure Policy Informationen darüber enthalten, was ein Entdecker einer Schwachstelle vom Hersteller erwarten kann. Dies umfasst eine mögliche Gewährung von Prämien (Bug Bounties) für die vertrauliche Meldung von Schwachstellen (Coordinated Disclosure) oder andere Anreize zur Befolgung des Prinzips „Coordinated Disclosure“.

2 Kommunikationskanäle

Die Etablierung geeigneter Kommunikationskanäle ist essenziell, um im Falle von Schwachstellen effizient und zeitnah agieren zu können. Prinzipiell empfiehlt es sich nicht, einzelne Personen als Ansprechpartner für IT-Sicherheitsfragen zu benennen, da es beispielsweise durch die Fluktuation von Mitarbeitern zu Problemen kommen kann. Vielmehr sollten Rollenorientierte Kontaktmöglichkeiten auf der Unternehmenswebseite sowie in der Produktdokumentation aufgeführt werden.

2.1 Die Webseite des Herstellers

Als primäre Kommunikationskanäle sind Unternehmens-Webseite sowie E-Mail und Telefon zu empfehlen. Ein Verweis auf geeignete Möglichkeiten zur Meldung von Schwachstellen sollte bereits auf der Startseite des Unternehmens vorhanden sein.

Jeder Hersteller sollte Sicherheitsinformationen an zentraler Stelle in seinem Webangebot bereitstellen. Hierzu gehören sowohl allgemeine Sicherheitsinformationen (z. B. http(s)://www.company.tld/security) als auch Sicherheitsinformationen spezifisch für bestimmte Produkte, je nach Komplexität des Produktportfolios ggf. auf separaten Seiten, wie beispielsweise http(s)://www.company.tld/productname/security.

Mögliche Inhalte einer solchen Webseite sind:

- Schwachstelleninformationen (Advisories zu noch nicht geschlossenen Schwachstellen, Informationen zu möglichen Workarounds sowie Bulletins zu Schwachstellen, für die Sicherheitsupdates verfügbar sind),
- Kontaktinformationen (E-Mail, Telefonnummer inkl. Erreichbarkeitszeiten, öffentliche PGP-Schlüssel und S/MIME-Zertifikate des Unternehmens, um eine verschlüsselte Übermittlung von Schwachstelleninformationen zu ermöglichen),
- die Disclosure Policy des Unternehmens,
- Patches und Updates,
- ergänzende Dokumente (Whitepaper, FAQ, etc.) zum sicheren Einsatz der Produkte,
- ein Kontaktformular, da dieses die Strukturierung von gemeldeten Sicherheitsproblemen sowie die Forderung von Mindestangaben ermöglicht. Zudem wird die Möglichkeit zum anonymen Melden von Schwachstellen gefördert. Ein solches Formular kann entweder einfach und überschaubar sein (z. B. Ebay[2]) oder auch sehr umfangreich (z. B. cert.org[3]).

Diese Webseiten sollten mittels gültiger und verifizierbarer SSL-Zertifikate geschützt sein, um die Authentizität und Vertraulichkeit der Informationen zu gewährleisten.

Als zentrale E-Mail-Adresse für sicherheitsspezifische Fragen bzw. Meldungen von Schwachstellen bieten sich E-Mail-Adressen, wie z. B. product-security@company.tld, security-team@company.tld, productname.security@company.tld oder secure@company.tld an. Security@company.tld hingegen sollte nicht verwendet werden, da dieser Adresse gemäß RFC 2142 eine andere Bedeutung zugeordnet ist. Auch sollten allgemeine Adressen wie info@company.tld oder support@company.tld nicht für Sicherheitsvorfälle genutzt werden.

Sicherheitsspezifische Fragen oder Meldungen über die etablierten Kommunikationskanäle sollten innerhalb von 24 Stunden mit einer persönlichen und nicht automatisch generierten E-Mail beantwortet werden (1st Level). Nach einer weitergehenden Analyse sollte eine ausführlichere Rückmeldung innerhalb von weiteren 48 oder 72 Stunden erfolgen (2nd oder 3rd Level).

Hersteller sollten Mailinglisten speziell für sicherheitsspezifische Meldungen anbieten. Die darüber versendeten E-Mails sollten mittels Signaturen geschützt werden. Dabei empfiehlt es sich, dieselben Schlüssel zu verwenden, die auch auf der Webseite des Unternehmens genannt sind.

Insbesondere in kritischen Einsatzbereichen ist mitunter eine Veröffentlichung von Schwachstellen-Informationen nur bedingt gewünscht. In diesem Fall sollten Betroffene – also Kundenkontakte, Integratoren und OEM-Partner – direkt benachrichtigt werden.

Zusätzlich zur eigenen Webseite des Herstellers gibt es weitere Möglichkeiten, um die Kontaktinformationen in einer der existierenden Listen zu veröffentlichen. Bekanntes Beispiel hierfür ist u. a. das Open Source Security wiki: http://oss-security.openwall.org/wiki/vendors

2 http://pages.ebay.com/securitycenter/Researchers.html
3 https://forms.cert.org/VulReport/

2.2 Networking mit Dritten

Weiterhin empfiehlt sich die Pflege von Kontakten zu Dritten, um bei Bedarf auch hierüber zeitnah agieren zu können. Zu diesen Kontaktstellen gehören neben staatlichen Stellen, wie dem BSI, ggf. auch Industrieverbände oder CERTs in anderen Ländern. Gerade bei Produkten, die im KRITIS-Umfeld eingesetzt werden, kann das BSI unterstützen und als Multiplikator fungieren. Hierzu ist es häufig hilfreich, bzgl. der Branchen und Szenarien, in denen die Produkte eingesetzt werden, aussagefähig zu sein. Darüber hinaus sollten sich Hersteller bei den relevanten CERTs registrieren, um stets mit den neuesten Advisories und Warnungen versorgt zu werden – besonders wenn diese die eigenen Produkte oder die eigene IT-Landschaft betreffen. Auch eine aktive Vernetzung mit Mitbewerbern, Partnern und anderen Institutionen, wie beispielsweise Industrieforen und Testlaboren, ist eine wichtige Voraussetzung für eine hinreichende Handlungsfähigkeit.

Der Austausch zwischen Herstellern ist besonders wichtig im Falle von Schwachstellen in sehr weit verbreiteten Produkten und Protokollen. Auch Komponenten von Dritten, wie beispielsweise Frameworks oder Bibliotheken, müssen besondere Beachtung finden. Durch die Verwendung solcher Drittkomponenten werden diese Bestandteil des eigenen Produkts. Daher sollte ein Kontakt für Sicherheitsfragen zum jeweiligen Hersteller etabliert werden. Zudem sollten die Advisories solcher Hersteller mindestens täglich gesichtet und ggf. bewertet werden. Die Veröffentlichung von Advisories und Bulletins für Drittkomponenten sollten im eigenen Unternehmen entsprechende Prozesse anstoßen, wie eine fachliche Analyse, die Rückportierung von Patches, die Aktualisierung von Komponenten sowie die Veröffentlichung eigener Advisories.

Bei der Analyse von gemeldeten Schwachstellen ergibt sich mitunter, dass die Ursache in der Komponente eines Dritten liegt. Der betroffene Hersteller sollte möglichst zeitnah informiert werden. Dabei ist eine konstruktive und professionelle Zusammenarbeit besonders wichtig, da es sich um eine sehr komplexe Wechselwirkung zwischen den Produkten bzw. Komponenten handeln kann und häufig Haftungsfragen und die Möglichkeit einer negativen Wahrnehmung in der Öffentlichkeit im Raum stehen. Dieselben konstruktiven und offenen Bemühungen sollten unternommen werden, wenn andere Hersteller ein eigenes Produkt als Drittkomponente einsetzen und dadurch von einer Schwachstelle betroffen sind.

3 Incident Handling

Im Mittelpunkt der Außendarstellung im Rahmen des Incident Handling, welches stets möglichst zeitnah erfolgen sollte, stehen die veröffentlichten Advisories bzw. Bulletins.

Folgende Inhalte sollten in einem Advisory enthalten sein:

- Bezeichnung des Advisories (z. B. systematisch vergeben mit fortlaufender Nummer)
- Datum der Veröffentlichung
- betroffenes Produkt inkl. Versionsangaben und Konfiguration
- betroffene Plattformen / Betriebssysteme und ggf. deren Konfiguration
- Kritikalität der Schwachstelle (Kategorisierung nach niedrig/mittel/hoch) und Einschätzung nach dem Common Vulnerability Scoring System (CVSS)[4]
- Auswirkungen (z. B. Denial-of-Service, Remote Code Execution, Local Privilege Escalation, ...)

4 http://www.first.org/cvss

- Beschreibung der Schwachstelle (Management Summary)
- Detailinformationen (für Techniker)
- voraussichtliche Verfügbarkeit von Sicherheitsupdates
- Historie der Events im Kontext dieser Schwachstelle
- Workarounds
- Würdigung des Entdeckers / des Meldenden
- Angabe, ob die Schwachstelle gemäß Coordinated Disclosure gemeldet wurde
- Angabe, ob PoC-Code / Exploit frei verfügbar ist
- Autor(en) des Advisory
- CVE bzw. CVE Candidate Reference Number[5].
- Weiterführende Informationen (z. B. URLs der Unternehmens-Webseite)
- URL der aktuellen Version des Advisories

In einem aktualisierten Advisory sollten die ergänzten bzw. geänderten Passagen deutlich als Update gekennzeichnet sein.

Nicht in einem Advisory enthalten sein sollten Informationen, die technisch versierten Personen das Ausnutzen der Schwachstelle erlaubt. Auch PoC Exploit Code sollte in keinem Fall veröffentlicht werden.

Es ist zu empfehlen, Advisories mit denselben kryptografischen Schlüsseln zu schützen / zu signieren, die auch auf der Webseite (Kontaktmöglichkeiten) angegeben sind. Ein entsprechender Link sollte im Advisory enthalten sein.

Sobald ein Sicherheitsupdate verfügbar ist, wird aus dem Advisory ein Bulletin, das zusätzlich zu den o. g. Angaben auf das Sicherheitsupdate hinweist. Dabei werden auch Informationen zu den Bezugswegen für das Sicherheitsupdate, mögliche Inkompatibilitäten bei Anwendung sowie alternative Schutzmöglichkeiten durch Workarounds – sollte aus technischen Gründen die Installation eines Updates nicht möglich sein – aufgezeigt.

4 Nachbereitung

Im Nachgang eines Incident Handling sollten die gesammelten Erfahrungen (lessons learned) aufbereitet werden. So kann es beispielsweise erforderlich sein, das Kommunikationsverhalten oder das Incident Handling selbst zu optimieren. In vielen Fällen ist es auch erforderlich, den Entwicklungsprozess und das Qualitätsmanagement der Produktherstellung zu verbessern, indem beispielsweise Quality Gates oder zusätzliche Testmethoden etabliert werden. Grundsätzlich sollte die Produktion von Software innerhalb eines etablierten, sicherheitsorientierten Software-Entwicklungsprozesses erfolgen.

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.

5 http://cve.mitre.org