Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess

Umgang des BSI mit Schwachstellenmeldungen

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	01.12.2022	Bundesamt für Sicherheit in der Informationstechnik. BSI – CERT-Bund	Initiale Veröffentlichung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: vulnerability@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

Die Verbesserung der Informationssicherheit und die Erhöhung des Schutzes der von IT-Systemen verarbeiteten Daten erfordern über den gesamten Produktlebenszyklus (und teilweise auch darüber hinaus) ein verantwortungsbewusstes Zusammenarbeiten und das Bewusstsein für eine positive Fehlerkultur aller Beteiligten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Deshalb gehört es zu den wesentlichen gesetzlichen Aufgaben des BSI, Schwachstellen auszuwerten und seine Zielgruppen über deren Risiko und ggf. notwendige Schutzmaßnahmen zu informieren (§ 3 Abs. 1 Nr. 2, 14, 14a; § 4 Abs. 2; § 8b Abs. 2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)) (siehe [BMJ2021]). Ein weiteres Ergebnis der Auswertung kann eine Warnung gem. § 7 BSIG sein (siehe [BMJ2021]).

Zur Wahrnehmung dieser Aufgaben bietet das BSI einen Coordinated Vulnerability Disclosure (CVD)-Prozess an, der auf international etablierten Verfahren basiert (vgl. [CMU2017], [ISO2018], [ISO2019]). Ziel dieses Prozesses ist es, durch eine koordinierte Veröffentlichung (durch Sicherheitshinweise und Patches bzw. Mitigationsmaßnahmen) Transparenz über die entdeckte Schwachstelle herzustellen, um Nutzende eines IT-Produkts oder Dienstleistung zu informieren und zu schützen.

Bei der Entwicklung von Software, Hardware und Spezifikationen/Standards lassen sich Schwachstellen nicht vollständig ausschließen. Je komplexer das gemeinsame Wirken verschiedener Entitäten in einem Gesamtsystem ist, desto häufiger treten Schwachstellen auf. Auch nach intensiven Tests werden oftmals nicht alle Schwachstellen in einem IT-System vor der Auslieferung an die Kunden entdeckt. In den meisten Fällen erfolgt die notwendig werdende Schwachstellenreaktion somit zu einer Zeit, in der sich das Produkt bereits im Einsatz befindet und macht die Erstellung und Installation von Updates oder ein Implementieren anderer, mitigierender Maßnahmen für das betroffene System erforderlich.

Sichere Entwicklungsprozesse minimieren zwar die Anzahl an bestehenden Schwachstellen in Produkten; eine Garantie, dass ein Produkt gar keine Schwachstelle aufweist, bieten sie allerdings auch nicht. Um das von einer Schwachstelle ausgehende Schadensszenario und das daraus resultierende Schadensrisiko zu reduzieren, ist das Etablieren eines verantwortungsbewussten und effizienten Reaktionsprozesses daher von zentraler Bedeutung.

Die vorliegende Leitlinie sowie die veröffentlichte Richtlinie für Sicherheitsforschende (siehe [BSI2022e]) beschreiben den BSI-seitigen Umgang mit Schwachstellenmeldungen, die IT-Produkte und Dienstleistungen der Bundesverwaltung oder solche von Drittherstellern betreffen. Im weiteren Verlauf dieser Leitlinie werden der Prozess, die wesentlichen Verantwortlichkeiten der Beteiligten sowie deren Zusammenwirken näher erläutert.

Diese Leitlinie soll zu einer Verbesserung, Vereinheitlichung und Beschleunigung des gesamten Reaktionsprozesses beitragen und ist als Ergänzung zu der veröffentlichten Richtlinie für den Umgang mit Schwachstellenmeldungen zu betrachten.

2 Die Rollen im CVD-Prozess

Im Rahmen der Meldung einer Schwachstelle treffen mit den Sicherheitsforschenden auf der einen und den Herstellern des betroffenen Systems auf der anderen Seite traditionell zwei Parteien mit scheinbar unterschiedlichen Interessen aufeinander. Beide Parteien verfolgen in der Regel jedoch das gleiche Ziel – die Schwachstelle zu schließen. Ein vertrauensvoller Austausch zwischen allen im Prozess beteiligten Parteien ermöglicht dabei den notwendigen konstruktiven Dialog. Im Idealfall reagiert ein Hersteller auf eine Schwachstellenmeldung durch eine schnellstmögliche und nachhaltige Behebung der Ursache, eine angemessene Informationsweitergabe an seine Kunden und eine geeignete Würdigung der Schwachstellenfindenden.

Im Folgenden werden diese beiden zentralen Rollen eines CVD-Prozesses (d.h. Sicherheitsforschende und Hersteller) noch eingehender erläutert. Zudem wird auf die vermittelnde und koordinierende Rolle des BSI im CVD-Prozess näher eingegangen. Details zum CVD-Prozess innerhalb des BSI werden in Kapitel 3 näher ausgeführt.

2.1 Sicherheitsforschende

Schwachstellen können von diversen Personengruppen gefunden bzw. gemeldet werden. Dazu zählen z. B. die Nutzenden eines Produkts, IT-Sicherheitsforschende, Penetrationstestende, Forschungseinrichtungen, Zertifizierungsstellen oder Behörden. Zu beachten ist, dass Schwachstellenfindende und Schwachstellenmeldende nicht zwangsläufig ein und dieselbe Person sein müssen. Es gibt bspw. Fälle, in denen Meldende im Auftrag von Findenden agieren. Im weiteren Verlauf des Dokuments werden diese Spezialfälle jedoch nicht weiter berücksichtigt, sondern beide Rollen unter dem Begriff „Sicherheitsforschende“ zusammengefasst.

Auf Grund der geltenden Rechtslage in Deutschland müssen Sicherheitsforschende darauf achten, dass die von ihnen durchgeführten Tests rechtmäßig sind bzw. mit Zustimmung der Betroffenen durchgeführt werden. Sicherheitsforschende sollten den Zugriff auf personenbezogene Daten vermeiden. Keinesfalls sollten personenbezogene Daten genutzt, gesichert - auch nicht in Form von Screenshots - oder aber weitergegeben werden. Es sollte versucht werden, das Sicherheitsteam des verantwortlichen Herstellers zu kontaktieren und ausreichende Details zur Verfügung zu stellen, damit das Vorhandensein der Schwachstelle geprüft und nachvollzogen werden kann.

Sicherheitsforschende sollten das Melden einer Schwachstelle nicht von der Zahlung einer finanziellen Kompensation abhängig machen.

Wenn Hersteller Bug-Bounty-Programme anbieten, sollten Sicherheitsforschende die vom Hersteller formulierten Bedingungen genauestens erfassen. Bei Unklarheiten sind Rückfragen an den Hersteller sowie ggfs. an einen spezialisierten Anwalt empfehlenswert, bevor mit den Tests begonnen wird. Das BSI darf ggü. Sicherheitsforschenden keine individuelle Rechtsberatung erbringen.

2.2 Hersteller/Produktverantwortliche

Als Hersteller werden Gruppen, Einzelne oder Organisationen bezeichnet, die ein IT-Produkt erstellt haben oder dieses aktuell pflegen (inklusive Open Source Software und deren Maintainer sowie Produzenten von Hardware). Im Rahmen dieses Dokuments fallen hierunter auch solche Organisationen, die ein IT-Produkt bei einem Dritten in Auftrag gegeben haben oder in deren Namen bzw. über deren Vertriebskanäle ein IT-Produkt angeboten wird, somit also auch Produktverantwortliche sind.

Trotz der Umsetzung eines Secure Development Lifecycle (SDL) (siehe [BSI2020b], [MOT2022], [MIC2022]) ist nicht auszuschließen, dass Schwachstellen in IT-Produkten vorhanden sind. Es gehört daher zur grundlegenden Verantwortung aller Hersteller, sich auf die Behebung entdeckter und gemeldeter Schwachstellen einzurichten. Demnach sind Schwachstellenmeldungen in IT-Produkten als Unterstützung im eigenen Interesse des Herstellers anzusehen.

Um das erfolgreiche Durchlaufen eines CVD-Prozesses zu ermöglichen, sollten Hersteller auf eingehende Schwachstellenmeldungen positiv reagieren und nicht mit rechtlichen Konsequenzen drohen, solange keine kriminellen Absichten erkennbar sind (vgl. CVD-Richtlinie des BSI für Meldungen von Schwachstellen [BSI2022e]). Zudem sollten Hersteller vorbereitet sein, wozu ein ganzheitlicher interner Prozess unter Beteiligung der relevanten Unternehmensbereiche, das Etablieren von Kommunikationskanälen und die eigentliche Reaktion auf eine Schwachstellenmeldung unabdingbar ist. Während des gesamten CVD-Prozesses sollten Hersteller sowohl in Richtung Sicherheitsforschenden als auch in Richtung des BSI proaktiv kommunizieren sowie eine ständige Optimierung des beim Hersteller internen Prozesses anstreben.

Das BSI hat unterstützende Empfehlungen für Hersteller zur Etablierung eines solchen Prozesses veröffentlicht (siehe [ACS2018]). Besonders wichtig für die erfolgreiche Durchführung eines CVD-Prozesses ist die Schaffung der Rolle eines verantwortlichen IT-Sicherheitskontaktes auf Seiten des Herstellers. Dadurch ist sichergestellt, dass Zuständigkeiten geklärt, die geeigneten Personen adressiert werden und handeln können. Dadurch kann einem Scheitern des CVD-Prozesses durch fehlende Rückmeldung vorgebeugt werden (siehe [ACS2018]).

Nach Abschluss des CVD-Prozesses erfolgt üblicherweise die Veröffentlichung einer Herstellerempfehlung für die Anwendenden des IT-Produkts. Diese sogenannten „Advisories“ oder „Security Bulletins“ enthalten Details zur Schwachstelle und Hinweise zu den notwendigen Schutzmaßnahmen. Das Verheimlichen von Schwachstellen ist zu unterlassen. Im Gegenteil sollte eine offene Reaktion dazu genutzt werden, nutzerseitig das Beheben der Schwachstelle zu beschleunigen. Hierfür wird Herstellern die Anwendung des maschinenlesbaren Common Security Advisory Framework (CSAF) mit dem Profil „Security Advisory“ empfohlen (siehe [BSI2022a]).

Das BSI erwartet, dass der Hersteller die Zuweisung eines eindeutigen Identifiers (einer sogenannten CVE-Nummer) für die Schwachstellen bei einer CVE Numbering Authority (CNA) beantragt. In Abstimmung mit den betroffenen Herstellern und Sicherheitsforschenden kann das BSI in begründeten Ausnahmefällen diese Beantragung übernehmen (z. B. auch wenn ein Hersteller keine Beantragung durchführen will, obwohl es sich um eine schwerwiegende Schwachstelle mit einem CVSS Score von mindestens 7 handelt - basierend auf der Bewertung des BSI).

Die Schaffung von Anerkennungsstrukturen kann die Bereitschaft zum Melden von Schwachstellen in IT-Produkten des Herstellers fördern. Durch die Etablierung von finanzieller Entlohnung (Bug-Bounty-Programm) für Schwachstellenfindende können Hersteller Ihre Anerkennung ausdrücken und eine positive Anreizstruktur schaffen. Auch das Angebot einer Anerkennungswebseite (englisch „Hall of Fame“) stellt eine zusätzliche Möglichkeit für Hersteller dar, Sicherheitsforschenden öffentlich für Ihre Schwachstellenmeldung zu danken.

2.3 Die Rolle des BSI

Im Rahmen eines CVD-Prozesses kann das BSI, vertreten durch das Computer Emergency Response Team des Bundes (CERT-Bund), eine Rolle als Koordinator oder Vermittler zwischen Sicherheitsforschenden und Herstellern einnehmen und dabei unterstützen, dass Schwachstellen schnellstmöglich behoben werden.

Die Einbindung von CERT-Bund in einen CVD-Prozess kann dabei sowohl durch Sicherheitsforschende, als auch durch Hersteller initiiert werden. So kann CERT-Bund bspw. von Sicherheitsforschenden als Anlaufstelle genutzt werden, um bei zuvor erfolglosen Kontaktaufnahmen den Erstkontakt zum Hersteller aufzubauen oder um bei bereits bestehenden Schwierigkeiten zwischen dem Sicherheitsforschenden und dem Hersteller eines betroffenen Systems zu vermitteln und zu schlichten. Dadurch kann das BSI zu einer Deeskalation zwischen Herstellern und Sicherheitsforschenden beitragen mit dem Ziel, Schwachstellen schnellstmöglich zu beheben.

Im Falle einer Schwachstellenmeldung, die vom BSI entwickelte, in Auftrag gegebene, zertifizierte oder zugelassene Produkte betrifft, koordiniert das CERT-Bund entsprechende Schwachstellenmeldungen mit den zuständigen Stellen innerhalb des BSI.

Schwachstellen, die Produkte bzw. Webanwendungen des Bundes betreffen, können und sollen dem BSI gemeldet werden. Als die nationale Cyber-Sicherheitsbehörde des Bundes werden die gemeldeten Schwachstellen in den CVD-Prozess überführt und an die zuständigen Hersteller bzw. Produktverantwortlichen weitergeleitet und eine Behebung der Schwachstellen angestrebt.

Das BSI kann im Rahmen eines CVD-Prozesses auch die Rolle des Sicherheitsforschenden einnehmen, sollten Referate des BSI Schwachstellen in IT-Produkten gefunden haben und diese an das CERT-Bund als koordinierende Stelle melden.

3 Der CVD-Prozess im BSI

Das BSI begleitet bei Bedarf als vermittelnde Instanz durch den CVD-Prozess und betreut alle involvierten Parteien. Grundsätzlich ist seitens des BSI festzuhalten:

Die im Rahmen eines CVD-Prozesses an das BSI gemeldeten validen Schwachstellen werden IMMER an den Hersteller bzw. Produktverantwortlichen weitergegeben und eine bestmögliche Behebung oder Mitigation der Schwachstelle angestrebt.

In Anlehnung an die in den bestehenden ISO-Standards ISO 29417 und ISO 30111 definierten Prozessphasen zum Umgang mit Schwachstellen (siehe [ISO2018], [ISO2019]), unterteilt sich die Schwachstellenkoordination im BSI wie folgt:

1. Schwachstellenmeldung
2. Schwachstellenbewertung
3. Kontaktaufnahme und Koordination
4. Offenlegung von Schwachstellen

Im folgenden Kapitel werden die verschiedenen Phasen der Schwachstellenkoordination näher erläutert und die damit verbundenen Erwartungshaltungen an Sicherheitsforschende und Hersteller konkretisiert.

3.1 Schwachstellenmeldung

Das BSI bietet Sicherheitsforschenden verschiedene Möglichkeiten an, gefundene Schwachstellen zu melden. Dabei können Schwachstellenmeldungen entweder direkt an eine dedizierte E-Mail-Adresse (vulnerability@bsi.bund.de) gesendet oder über ein Schwachstellenmeldeformular[1] (auch anonym) gemeldet werden.

Gerade bei komplexen Schwachstellen ist es jedoch nicht auszuschließen, dass weitere Erklärungen und Dokumentationen benötigt werden. Da für das erfolgreiche Durchlaufen des CVD-Prozesses die vertrauensvolle Kommunikation mit Sicherheitsforschenden von hoher Relevanz ist, können Schwachstellenmeldungen ohne gültige Kontaktdaten nur eingeschränkt bearbeitet werden. Auf Wunsch wird das BSI im Rahmen der gesetzlichen Möglichkeiten die Anonymität der Sicherheitsforschenden gegenüber Dritten inklusive des betroffenen Herstellers jedoch wahren.

Grundsätzlich empfiehlt das BSI Sicherheitsforschenden, die keinen eigenen strukturierten Schwachstellenreport erstellt haben (bzw. ggf. wenig Erfahrung im Kontext von Schwachstellenmeldungen besitzen), das Meldeformular für Schwachstellen zu verwenden (siehe [BSI2022b]). Dieses Formular ermöglicht es Sicherheitsforschenden, die für die weitere Bearbeitung relevanten Informationen an das BSI strukturiert zu übermitteln.

Zusätzlich sollten im Rahmen einer Schwachstellenmeldung mögliche zeitliche Abhängigkeiten (z. B. das Datum einer geplanten Veröffentlichung oder - falls bekannt - einer Präsentation auf einer Konferenz) mitgeteilt werden.

Sicherheitsforschende, die ein eigenes etabliertes Meldungsformat haben (bspw. via PDF), können Schwachstellenmeldungen und Koordinierungsanfragen auch direkt per Mail an das BSI übermitteln. Bei solchen Meldungen sind die in der CVD-Richtlinie des BSI aufgeführten Aspekte zu beachten. Die verschlüsselte Kommunikation mit dem CERT-Bund sollte mittels Open Pretty Good Privacy (OpenPGP bzw. PGP) (siehe [IET2007]) erfolgen (siehe [BSI2022c]). Dabei sollte auch die Bereitstellung eines Proof of Concept (PoC) für die Bewertung der Schwachstelle mitangegeben werden.

Sicherheitsforschende erhalten auf ihre Schwachstellenmeldungen immer eine Eingangsbestätigung bzw. eine Rückmeldung zur Bestätigung des Erhalts der Meldung.

[1] Das Schwachstellenmeldeformular des BSI kann über nachfolgenden Link aufgerufen werden https://www.bsi.bund.de/Schwachstellenmeldung

Das BSI behält sich vor, die Koordinierung bestimmter Schwachstellen zu priorisieren. Kriterien für eine solche Priorisierung sind beispielsweise

- potentiell weitreichende Auswirkungen in und/oder auf Deutschland und seine Infrastruktur,
- eine Betroffenheit von Verwaltung oder Betreibern Kritischer Infrastrukturen,
- große Nutzerzahlen, Effekte auf eine Vielzahl von IT-Produkten oder Hersteller,
- anderweitig kritische Auswirkungen.

3.2 Schwachstellenbewertung

Jede Schwachstellenmeldung, welche über die beschriebenen Meldewege beim BSI eingeht, wird durch das BSI plausibilisiert und – soweit mit den zur Verfügung stehenden Informationen - auf wissenschaftlich-technischer Grundlage bewertet. Um diese Bewertung zu ermöglichen, sind bei jeder Schwachstellenmeldung, ausreichend Informationen dem BSI bereitzustellen.

Die zur Bewertung von Schwachstellen notwendige Analyse wird nach Möglichkeit seitens BSI durchgeführt. Hierfür kann es von Vorteil sein, wenn Sicherheitsforschende im Rahmen ihrer Meldung einen Common Vulnerability Scoring System (CVSS)-Wert und die dazugehörige Matrix (präferiert in der aktuellsten Version) zur Bestimmung des Schweregrads der Schwachstelle zur Verfügung stellen. Gleiches gilt für die Identifikation zusätzlicher möglicherweise betroffener Hersteller, sofern dies erforderlich scheint und nicht bereits mit der Meldung geschehen ist. Im Falle eines notwendigen Austauschs seitens des BSI mit weiteren Sicherheitsforschenden, innerhalb vertrauenswürdiger Computer Security Incident Response Team (CSIRT)-Gruppen (wie bspw. dem europäischen CSIRTs Netzwerk (siehe [CSI2022])) oder sonstigen externen Dritten wird dies mit den meldenden Sicherheitsforschenden abgestimmt und von deren Freigabe abhängig gemacht.

Im Anschluss an die Bewertung durch das BSI werden die Sicherheitsforschenden über die weiteren geplanten Schritte informiert.

Das BSI kann sich auch dazu entscheiden, für eine Schwachstellenmeldung kein CVD-Verfahren einzuleiten. Dies ist dann der Fall, wenn nicht ausreichend technische Details der Schwachstelle zur Verfügung gestellt werden oder die möglichen Auswirkungen für den eigenen Wirkungskreis marginal sind. Weitere Gründe dafür, dass kein CVD-Verfahren durchgeführt wird, liegen vor, wenn

- sich ein Schwachstellenbericht ausschließlich auf den Debug- oder Entwicklungsmodus eines IT-Systems bezieht und keinerlei sicherheitsrelevante Auswirkungen auf den Produktivmodus des IT-Systems hat,
- nicht ausreichend Informationen zur technischen Nachvollziehbarkeit der Schwachstelle bereitgestellt werden oder
- die in der CVD-Richtlinie veröffentlichten Bedingungen (seitens des Sicherheitsforschenden) gravierend missachtet wurden.

Kein Grund zum Ablehnen eines CVD-Vorgangs seitens des BSI, sind das Suchen von Schwachstellen mittels gängiger Techniken für Sicherheitsforschende, wenn das Analysieren gefolgt vom Melden der Schwachstelle erfolgt. Wird ein CVD-Verfahren abgelehnt, werden Sicherheitsforschende über die Entscheidung und deren Begründung informiert. Dennoch kann das BSI den Sicherheitsforschenden geeignete Unterstützungsangebote unterbreiten, damit sie die Koordinierung und dadurch das CVD-Verfahren eigenständig übernehmen können. Diese unterstützenden Tätigkeiten können

- die Kontaktvermittlung zu Herstellern in Deutschland,
- dass das BSI bei nicht reagierenden Herstellern in Deutschland die Aufnahme eines CVD-Verfahrens wohlwollend prüft,
- eine Unterstützung bei der Schwachstellenbewertung oder Verfahrensberatung oder
- die BSI-seitige Weitergabe von Vorabinformation an national oder internationaler CERTs umfassen.

3.3 Kontaktaufnahme und Koordination

Sicherheitsforschende können bei ihrer Meldung an das BSI die **Kontaktvermittlung oder Übernahme der Schwachstellenmeldung** durch das BSI erbitten. Falls ein Hersteller bezüglich der Schwachstelle bereits kontaktiert wurde oder dies geplant ist, muss diese Information im Rahmen einer Schwachstellenmeldung angegeben werden. Ist die Meldung an das BSI lediglich nachrichtlich oder sind keinerlei Schwierigkeiten in der Kommunikation zwischen Sicherheitsforschenden und Hersteller durch das BSI ersichtlich, behält sich das BSI vor, keine zusätzliche Kontaktaufnahme zum Hersteller aufzunehmen, sondern die Schwachstellenmeldung nur zur Kenntnis zu nehmen. Sicherheitsforschende werden in diesen Fällen grundsätzlich über die Entscheidung des BSI informiert.

Wird das BSI um Übernahme bzw. Kontaktaufnahme mit dem Hersteller gebeten, wird als Reaktion auf den ersten Kontaktversuch eine Rückmeldung (Eingangsbestätigung) des Herstellers innerhalb von drei Werktagen (via Telefon oder E-Mail) erwartet. Sollte der Hersteller dieser Frist zur Rückmeldung nicht nachkommen, so unternimmt das BSI einen erneuten Kontaktversuch (sowohl telefonisch als auch via E-Mail). Reagiert der Hersteller hierauf erneut nicht innerhalb von spätestens drei Werktagen, wird das weitere Vorgehen zusammen mit den Sicherheitsforschenden abgestimmt. Dies kann mitunter zur Folge haben, dass das BSI entsprechend seines gesetzlichen Auftrages eine Warnung gem. § 7 BSIG vor dem Produkt veröffentlicht, wenn eine Einzelfallprüfung ergibt, dass die gesetzlichen Voraussetzungen zur Veröffentlichung einer Warnung vorliegt (vgl. [BMJ2021]).

Im weiteren Verlauf wird vom Hersteller innerhalb von zwei Wochen eine Verifikation der vorliegenden Schwachstellenmeldung, eine Bewertung nach dem CVSS Schema, die Nennung der betroffenen Produktversionen (und ggf. die Nennung weiterer betroffener Produkte) sowie das Skizzieren weiterer Schritte z. B. bzgl. Mitigationsmaßnahmen erwartet.

Betroffenen Herstellern wird zur Schließung von Schwachstellen eine angemessene Frist eingeräumt. Diese bewegt sich innerhalb der international üblichen 45 bis 90 Tage und ist in Absprache mit den Sicherheitsforschenden zu definieren, sollten diese eine entsprechende Frist setzen wollen. Abhängig von der Kritikalität und der Komplexität einer Schwachstelle kann die entsprechende Frist in Absprache mit dem Sicherheitsforschenden allerdings verkürzt oder verlängert werden. Für Hardware-Schwachstellen kann die Frist deutlich abweichen. Notwendig werdende Abweichungen sind seitens der Sicherheitsforschenden oder Hersteller zu begründen und im Rahmen der Koordinierung zu klären. Eine Verlängerung der maximalen Frist muss in Abstimmung mit Sicherheitsforschenden geschehen. Sollte zudem eine Frist seitens der Sicherheitsforschenden festgelegt worden sein, so ist dem Hersteller dies bei der Kontaktaufnahme durch das BSI mitzuteilen.

Wird die Frist zur Schließung der Schwachstelle durch den Hersteller überschritten, kann nicht ausgeschlossen werden, dass Sicherheitsforschende Details zur Schwachstelle mit Hinweis auf die Teilnahme am CVD-Prozess des BSI ohne weitere Rücksprache mit dem Hersteller veröffentlichen. Zudem kann die Fristüberschreitung mitunter zur Folge haben, dass das BSI entsprechend seines gesetzlichen Auftrages eine Warnung gem. § 7 BSIG vor dem IT-Produkt veröffentlicht, wenn eine Einzelfallprüfung ergibt, dass die gesetzlichen Voraussetzungen zur Veröffentlichung einer Produktwarnung vorliegt.

Die Einschätzung des Herstellers sowie weitere Informationen (z. B. Statusänderung, betroffene / nicht betroffene Produkte) werden vom BSI grundsätzlich mit Sicherheitsforschenden geteilt. Bestehen aufgrund außergewöhnlicher Umstände Vorbehalte gegen dieses Verfahren, kann der Hersteller diese schriftlich dem BSI zur Kenntnis bringen. Die Sicherheitsforschenden werden durch das BSI stets über alle Schritte und Entwicklungen in Kenntnis gesetzt.

Im Kontext von CVD-Prozessen, bei denen internationale Partnerbehörden die zentrale Koordinierung übernommen haben, kann von dem in diesem Abschnitt beschriebenen Verfahren ggf. abgewichen werden, sofern die Regelungen des BSI den Übereinkünften oder der Praxis der Koordinierungsgruppe internationaler Partnerbehörden entgegenstehen.

3.3.1 Schwachstellen, die mehrere Hersteller betreffen

Falls eine Schwachstelle direkt oder indirekt mehrere Hersteller betrifft, wird ein sogenanntes Mehrparteienverfahren (engl. „Multi-Party CVD“) eingeleitet. Im Rahmen eines solchen Verfahrens werden durch das BSI mehrere Hersteller kontaktiert. Diese Mehrparteienverfahren werden üblicherweise unter folgenden Bedingungen durchgeführt:

- Es handelt sich um eine Schwachstelle innerhalb der sogenannten „Supply Chain“ (Lieferkette) eines Produktes. Zur Behebung ist in diesem Fall üblicherweise die Beteiligung mehrerer Hersteller notwendig.
- Es handelt sich um eine Schwachstelle in einer gemeinsam genutzten Bibliothek, an der ein vorgelagerter Entwickler beteiligt ist. Dieser muss die Schwachstelle zuerst beheben, um nachgelagerten Herstellern eine Möglichkeit zu geben, die Behebung anzuwenden.
- Es existiert eine Schwachstelle in einer Protokollspezifikation, an der verschiedene Entwickler mit Implementierungen des Protokolls beteiligt sind.

Durch die zunehmende Verteilung der Entwicklung/Herstellung über verschiedene Parteien und die Integration von Software aus Drittquellen in ein Gesamtprodukt, insbesondere auch im Bereich von Internet of Things (IoT)-Produkten, nimmt einerseits die Komplexität des Herstellungsprozesses zu, andererseits steigt die Zahl der direkt oder indirekt von einer Schwachstelle betroffenen und somit zu involvierenden Parteien.

Wenn das BSI an einem Mehrparteienverfahren[2] beteiligt ist, wird es unter Wahrung des Ziels einer koordinierten Offenlegung versuchen, die Interessen aller Beteiligten während des Verlaufs zu wahren und auszugleichen. Dabei orientiert sich das BSI an internationalen Standards und Empfehlungen zum Umgang mit Mehrparteienverfahren (siehe [FIR2020]).

3.3.2 Kontakt zu weiteren Stellen jenseits des Herstellers

Das BSI nimmt in der Regel zunächst Kontakt zu betroffenen Produktherstellern auf. In Ausnahmefällen kann es sein, dass es für das erfolgreiche Durchlaufen eines CVD-Prozesses notwendig wird, weitere Stellen zu konsultieren. Beispielsweise kann dies notwendig werden, um

- Aufsichtsbehörden um Unterstützung zu bitten (z. B. Kraftfahrt-Bundesamt (KBA), Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) oder Bundesnetzagentur (BNetzA)),
- einen Herstellerkontakt zu ermitteln oder
- Unterstützung bei der technischen Analyse betreffender Schwachstellen zu suchen.

[2] Als exemplarische Mehrparteienverfahren können bspw. die unter den Namen Amnesia:33 (siehe [FOR2020], [BSI2020a]) und Heartbleed (siehe [HEA2014]), aber auch Efail (siehe [EFA2018]) bekannt gewordenen Schwachstellen aufgeführt werden.

3.3.3 Scheitern eines CVD-Prozesses

Trotz Kontaktaufnahmen und Vermittlungsversuchen können CVD-Prozesse auch scheitern. Einige der häufigsten Gründe hierfür sind:

- Kontaktabbruch seitens einer oder mehrerer an dem Prozess beteiligten Parteien.
- Es kommt zwischen Sicherheitsforschenden und Herstellern zu einem nicht lösbaren Disput.
- Die Kontaktaufnahmeversuche seitens BSI zum Hersteller schlagen fehl.

Falls eine der genannten Situationen innerhalb der vereinbarten Frist nach der initialen Kontaktaufnahme zum Hersteller durch das BSI eintritt, kann der laufende Koordinierungsprozess eingestellt werden. Reagiert ein Hersteller nicht mehr, erfolgt eine Aufforderung zur Stellungnahme mit Frist. Verstreicht die Frist ohne Stellungnahme, werden die Prozessbeteiligten darüber informiert.

In Folge eines Scheiterns des Prozesses prüft das BSI gemäß seinem gesetzlichen Auftrag mögliche weitere Schritte. Beispielsweise kann das BSI die aus dem CVD-Prozess gewonnenen Erkenntnisse zur Erfüllung der gesetzlichen Aufgaben ohne weitere Beteiligung des Herstellers weiterverwenden, in geeigneter Weise mit anderen Stellen teilen und bei Bedarf kurzfristige Warnungen veröffentlichen.

3.4 Koordinierte Offenlegung von Schwachstellen

Es wird von dem betroffenen Hersteller erwartet, dass dieser selbst valide Schwachstellen inkl. CVE-Nummer veröffentlicht und somit Transparenz für seine (potentiellen) Kunden schafft. Dies sollte spätestens dann erfolgen, wenn die Schwachstelle behoben ist. In der Regel werden dafür Security Advisories veröffentlicht. Das BSI empfiehlt hierfür die Nutzung des maschinenverarbeitbaren CSAF-Standards (siehe [OAS2022]). Daraus können nahtlos auch menschenlesbare Security Advisories erstellt werden. Zudem wird von Herstellern erwartet, dass keinerlei rechtliche Schritte gegenüber Sicherheitsforschenden eingeleitet werden, sollten diese Details zu der Schwachstelle nach einer international üblichen Frist (siehe Abschnitt 3.3) veröffentlichen und sich an die in der CVD-Leitlinie (siehe Abschnitt 2.1) sowie CVD-Richtlinie (siehe [BSI2022e]) festgeschriebenen Punkte gehalten haben.

Sofern das BSI in seiner Rolle als koordinierende Stelle tätig war, wird das BSI, nach Behebung der Schwachstelle, im Rahmen des CVD-Prozesses einen entsprechenden Hinweis (bestehend aus Name/Alias, gewünschte Referenzen, sowie Art der gemeldeten Schwachstelle) auf der Danksagungswebseite des BSI veröffentlichen.

Eine Referenzierung der durch die Schwachstelle betroffenen IT-Produkte oder IT-Systeme ist dabei nicht vorgesehen. Unbenommen davon kann das BSI in seiner Rolle als koordinierende Stelle selbst ein Security Advisory herausgeben. Dies geschieht in der Regel im Format des CSAF-Standards.

Sofern der oder den Schwachstellen und ihrer erfolgreichen Ausnutzung eine besondere Bedeutung beigemessen wird und/oder diese bspw. in ihren Auswirkungen wesentliche Zielgruppen des BSI betreffen (z. B. KRITIS-Unternehmen, Bundes- oder Landesverwaltungen), kann das BSI Sicherheitswarnungen veröffentlichen. Solche Sicherheitswarnungen beziehen sich detaillierter auf einzelne Schwachstellen, ihre Auswirkungen oder aktuelle Angriffskampagnen und umfassen technische Gegenmaßnahmen die eine schnelle Schadensminimierung ermöglichen. Die gesetzlichen Informationspflichten nach §4 Abs. 2 und §8b Abs. 2 BSIG bleiben hiervon unberührt (siehe [BMJ2021]).

3.4.1 Anerkennungsmöglichkeiten

Das BSI bietet Sicherheitsforschenden als Anerkennungsmöglichkeit die Referenzierung (Name oder Alias), sowie einen gewünschten Referenzlink auf der Danksagungswebseite („Hall-of-Fame“) des BSI an (siehe [BSI2022d]).

Im Rahmen eines durchgeführten CVD-Prozesses bietet das BSI Sicherheitsforschenden aktuell keine finanzielle Kompensation an. Die Implementierung weiterer Anerkennungsmöglichkeiten für die Produkte der Bundesverwaltung werden jedoch kontinuierlich evaluiert.

4 Anhang

4.1 Alternative Meldemöglichkeiten in Deutschland

Nicht alle Sicherheitsforschenden möchten Schwachstellen direkt an das BSI melden bzw. suchen alternative Meldemöglichkeiten für ein CVD-Verfahren. In solchen Fällen können Forschungseinrichtungen, Vereine bzw. Organisationen wie der Chaos Computer Club (CCC)[3] (siehe [CCC2022a]), Kollektive wie zerforschung (siehe [ZER2022]) oder unabhängige nationale CERTs wie das CERT@VDE (für Industrielle Steuerungssysteme (ICS, Industrial Control System) sowie medizinische und Embedded Systeme) (siehe [VDE2022]) Sicherheitsforschende unterstützen, Schwachstellen entgegenzunehmen und geeignet in einen CVD-Prozess zu überführen.

[3] Schwachstellenmeldungen an den CCC können über die E-Mail Adresse disclosure@ccc.de erfolgen. Weitere Informationen zu möglichen Richtlinien für Meldungen kann die Hacker-Ethik des CCC bieten (siehe [CCC2022b]).

Abkürzungsverzeichnis

Tabelle 2 Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BNetzA	Bundesnetzagentur
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
CCC	Chaos Computer Club
CERT	Computer Emergency Response Team
CSAF	Common Security Advisory Framework
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CNA	CVE Numbering Authority
CVD	Coordinated Vulnerability Disclosure
ICS	Industrielle Steuerungsanlagen / Industrial Control System
IoT	Internet of Things
ISO	International Organization for Standardization
KBA	Kraftfahrt-Bundesamt
PoC	Proof of Concept
PGP	Pretty Good Privacy
SDL	Secure Development Lifecycle

Literaturverzeichnis

[ACS2018] Allianz für Cyber-Sicherheit. Handhabung von Schwachstellen - Empfehlungen für Hersteller. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf. 2018.

[BMJ2021] Bundesministerium der Justiz. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG). https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html. 2021.

[BSI2020a] Bundesamt für Sicherheit in der Informationstechnik. AMNESIA33: Teils kritische Schwachstellen gefunden. https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Amnesia_201208.html. 2020.

[BSI2020b] Bundesamt für Sicherheit in der Informationstechnik. CON.8: Software-Entwicklung (Edition 2020). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/03_CON_Konzepte_und_Vorgehensweisen/CON_8_Software_Entwicklung_Edition_2020.pdf. 2020.

[BSI2022a] Bundesamt für Sicherheit in der Informationstechnik. Common Security Advisory Framework (CSAF). https://www.bsi.bund.de/CSAF. 2022.

[BSI2022b] Bundesamt für Sicherheit in der Informationstechnik. Onlineformular für Schwachstellen und Sicherheitslücken. https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Online_Meldung_Schwachstellen/schwachstellenmeldung_node.html. 2022.

[BSI2022c] Bundesamt für Sicherheit in der Informationstechnik. PGP-Key für verschlüsselte Meldungen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT-Sicherheitsvorfall/PGP-Schluessel.asc. 2022.

[BSI2022d] Bundesamt für Sicherheit in der Informationstechnik. Danksagungswebseite des BSI. https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Hall_of_Fame/Hall_of_Fame_node.html. 2022.

[BSI2022e] Bundesamt für Sicherheit in der Informationstechnik. Ich möchte eine Schwachstelle melden. https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html. 2022.

[CCC2022a] Chaos Computer Club. Startseite CCC. https://www.ccc.de/. 2022.

[CCC2022b] Chaos Computer Club. Hacker-Ethik des CCC. https://www.ccc.de/de/hackerethik. 2022.

[CSI2022] Computer Security Incident Response Team. CSIRTs Network. https://csirtsnetwork.eu/. 2022.

[CMU2017] Carnegie Mellon University. The CERT Guide to Coordinated Vulnerability Disclosure. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf. 2017

[EFA2018] Startseite EFAIL. https://efail.de/. 2018.

[FIR2020] Forum of Incident Response and Security Teams. Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure. https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1.2020

[FOR2020] Forescout. AMNESIA:33. https://www.forescout.com/research-labs/amnesia33/. 2020

[HEA2014] The Heartbleed Bug. https://heartbleed.com/. 2014.

[ISO2018] ISO Central Secretary. Information technology — Security techniques —Vulnerability disclosure. en. Standard ISO/IEC 29147:2018. Geneva, CH: International Organization for Standardization, 2018. URL: https://www.iso.org/standard/72311.html.

[ISO2019] ISO Central Secretary. Information technology — Security techniques— Vulnerability handling processes. en. Standard ISO/IEC 30111:2019. Geneva, CH: International Organization for Standardization, 2013. URL: https://www.iso.org/standard/69725.html.

[IET2007] Internet Engineering Task Force. OpenPGP Message Format. https://datatracker.ietf.org/doc/html/rfc4880 . 2007

[MIC2022] Microsoft. Microsoft Security Development Lifecycle Practices. https://www.microsoft.com/en-us/securityengineering/sdl/practices. 2022

[MOT2022] Projekt “Motivation Jenny”. Developer Security Toolkit. https://motivatingjenny.org/. 2022

[OAS2022] OASIS-Open. Common Security Advisory Framework Version 2.0 - Committee Specification Draft 02. https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html. 2022

[OWA2021] Open Web Application Security Project. OWASP Vulnerability Disclosure Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html. 2021

[VDE2022] Verband der Elektrotechnik Elektronik und Informationstechnik. CERTStartseite CERT@VDE. https://cert.vde.com/de/. 2022.

[ZER2022] Zerforschung. Kontakt –zerforschung. https://zerforschung.org/kontakt/. 2022.