ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Good Disclosure Practices

Empfehlungen zur verantwortungsvollen Veröffentlichung von Schwachstellen

Dr. Steven Arzt, Dr. Michael Kreutzer, Linda Schreiber

1 Auffinden der Schwachstelle

2 Erste Einschätzung/Prüfung
Technische Beschreibung der gefundenen Schachstelle, Bestimmung der Kritikalität (entsprechend Common Vulnerability Scoring System (CVSS)), Einschätzung der Auswirkungen auf Wirtschaft und Gesellschaft

3 Qualitätssicherung
Absicherung und Dokumentation der gefundenen Informationen. Diskussion mit internen Expertinnen und Experten – Information der eigenen Informationssicherheitsbeauftragten, Datenschutzbeauftragten, Leitungsebene und weiterer Verantwortungsträger.

4 Schwachstelle melden
Vertrauliche Mitteilung an den Hersteller (inklusive Nennung des geplanten Datums zur Veröffentlichung – nach Behebung, aber i.d.R. maximal 90 Tage nach Benachrichtigung). Ggf. Information an betroffene Organisationen/Personen bzw. zuständige staatliche Stellen und/oder Behörden – unter Umständen Anpassung des Veröffentlichungszeitpunkts, wenn es möglich und sinnvoll ist.

Nach Behebung, i.d.R. aber max. Frist von 90 Tagen

5 Veröffentlichung
ggf. CVE-Meldung, fristgerechte Veröffentlichung der Schwachstelle mit/ohne Hersteller, möglichst mit Hilfestellungen für Nutzende.

Die zunehmende Digitalisierung der Gesellschaft ermöglicht zahlreiche Innovationen und Verbesserungsmöglichkeiten für Gesellschaft, Wirtschaft sowie Bürgerinnen und Bürger. Gleichzeitig steigt die Abhängigkeit von IT-Systemen und damit auch die Bedeutung von IT-Sicherheitsschwachstellen. Wer solche Schwachstellen kennt und verantwortungsvoll damit umgeht, kann zur Verbesserung der allgemeinen Cybersicherheit beitragen. Die Wissenschaftlerinnen und Wissenschaftler am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE entdecken während ihrer Forschungsarbeit regelmäßig Sicherheitslücken. Der hier beschriebene Prozess ist ein Beispiel für die Umsetzung von Coordinated Vulnerability (siehe Kasten) im Rahmen von geförderten Forschungsprojekten und vergleichbaren Forschungsaktivitäten. In der Auftragsforschung für Dritte kann sich das Vorgehen von diesem Beispiel unterscheiden. Entwickelt wurde der Prozess am Fraunhofer-Institut für Sichere Informationstechnologie, das IT-Hersteller auch bei der Umsetzung von CVD-Policies unterstützt.

Was ist Coordinated Vulnerability Disclosure (CVD)?

CVD ist ein Vorgehen, bei dem der Finder/die Finderin einer Sicherheitslücke versucht, das Wissen um die gefundene Schwachstelle gemeinschaftlich mit allen verantwortlichen und betroffenen Parteien zu teilen. Hierzu gehören etwa Hersteller, Verkäufer oder Infrastrukturbetreiber, aber auch betroffene Nutzer. Ziel von CVD ist es, eine Veröffentlichung der Softwarefehler zu ermöglichen, die sowohl für Benutzer als auch Hersteller vorteilhaft ist, die illegale Nutzung der Schwachstelle durch Kriminelle verhindert und die öffentliche Cybersicherheit verbessert. Im Idealfall wird eine Sicherheitslücke erst dann veröffentlicht, wenn die Sicherheitslücke behoben und zum Beispiel eine entsprechende Aktualisierung der Software verfügbar ist.

Praxistipps für IT-Sicherheitsforschende

Das Nationale Forschungszentrum ATHENE hat große Erfahrung mit der Veröffentlichung von Schwachstellen. Hier finden Sie einige praktische Empfehlungen, die zur erfolgreichen Durchführung eines CVD-Prozesses beitragen.

Kommunikation verschlüsseln

Die Übermittlung der Schwachstellen sollte stets verschlüsselt erfolgen.

Ausdauer zeigen

Viele Unternehmen haben keine spezielle Anlaufstelle für Vulnerability Disclosure benannt. In diesen Fällen müssen Sicherheitsforschende über die öffentlichen Unternehmenskontakte ausdauernd versuchen, eine kompetente Ansprechperson zu finden. Ist dies trotz zahlreicher Versuche nicht möglich, kann eine Information über die PR- und Marketingabteilung erfolgen. In diesen Fällen sollte dann zunächst telefonisch besprochen werden, wie das weitere Vorgehen zur eigentlichen inhaltlichen Meldung und Übermittlung von Informationen zur Schwachstelle aussehen soll.

Eigene Rolle klar machen

Sicherheitsforschende sollten plausibel machen, dass es sich um CVD handelt und kein kriminelles und erpresserisches Interesse besteht. Bei Unternehmen, die nicht regelmäßig mit der Meldung von Schwachstellen in eigenen Produkten durch externe Sicherheitsforschende zu tun haben, sollten Forschende darauf vorbereitet sein, ihre Tätigkeit und Rolle als Sicherheitsforschende zu erklären. In diesem Zusammenhang kann beispielsweise kommuniziert werden, dass die Untersuchung des betroffenen Produktes nicht erfolgte, um dem Unternehmen Schaden zuzufügen, sondern weil sich verschiedene Produkte einer spezifischen Technologie oder Branche angeschaut und auch Schwachstellen in Produkten anderer Hersteller gefunden wurden. Hierbei kann es in der weiteren Kommunikation auch erforderlich sein, plausibel machen zu können, dass die Schwachstelle nicht durch den Entdecker ausgenutzt wurde und keine strafbaren Handlungen erfolgt sind.

Hersteller mit Informationen unterstützen

Um dem Hersteller die Möglichkeit zu geben, die gefundene Schwachstelle möglichst schnell und einfach zu beheben, sollten Sicherheitsforschende in der Lage sein, Anhaltspunkte für die Schwere der Schwachstelle zu liefern. Damit helfen sie dem Hersteller bei der Priorisierung, bei der internen Kommunikation und schaffen eine gute Voraussetzung für den Hersteller, geeignete Maßnahmen einzuleiten.

Auf eigene Disclosure Policy verweisen

Sicherheitsforschende sollten zu Beginn der Kommunikation darauf verweisen, dass sie sich entsprechend der Disclosure Policy bzw. des Prozesses ihrer Heimatorganisation verhalten. Dies hilft dem Sicherheitsforschenden zu demonstrieren, dass er/sie nicht willkürlich agiert, sondern entsprechend einem planbaren Vorgehen folgt. Veröffentlichte Disclosure Policies oder Prozesse der jeweiligen Entdeckerorganisation sind hier von Vorteil.

Ausreichende Frist

Ein wichtiger Grundsatz beim CVD ist es, dem Unternehmen genügend Zeit zum Beheben der Schwachstelle einzuräumen. Üblicherweise beträgt die Frist hierfür 90 Tage, kann bei besonders komplexen Schwachstellen im Einzelfall aber auch verlängert werden. Außerdem sollten Sicherheitsforschende von Anfang an geplante Publikationen und Konferenzbeiträge mit den jeweiligen Deadlines offen kommunizieren. Es ist ratsam, auch während der gesetzten Frist, in der das Unternehmen die Schwachstelle zu beheben sucht, im regelmäßigen Austausch mit dem Hersteller zu bleiben. Hierdurch können Verzögerungen frühzeitig berücksichtigt werden und – falls notwendig und möglich – eine Verlängerung der Frist überlegt und umgesetzt werden..

Prozess gut dokumentieren

Damit einhergehend empfiehlt sich eine gute Dokumentation des gesamten Meldeprozesses, sämtlicher Kommunikation (ggf. Gedächtnisprotokolle von Telefonaten) sowie der jeweiligen Ansprechpartner. Dies kann im Zweifelsfall auch als Beweis von getroffenen Absprachen dienen, insbesondere hilft es beiden Parteien aber, einen reibungslosen Ablauf aufrecht zu erhalten, falls zuständige Personen auf Entdeckerseite oder Unternehmensseite während des Prozesses ausscheiden. Die Dokumentation sollte so erfolgen, dass auch beim Auscheiden von Personen die entsprechende Dokumentation zugänglich bleibt (z. B. durch Export von Emails und zentrale Archivierung der Dokumente).

Erreichbar sein

Sicherheitsforschende müssen ihre eigene Erreichbarkeit sicherstellen und klar kommunizieren. Dies schließt insbesondere mit ein, dass mögliche Personalwechsel im jeweiligen Projektteam der Entdeckerorganisation einkalkuliert werden und damit ggf. persönliche E-Mail-Adressen oder Telefon-/Handynummern nicht mehr zur Verfügung stehen.

Weiterführende Links zum Thema:

Veranstaltung: https://www.athene-center.de/aktuelles/veranstaltungen/lunch-lectures-zum-cra-coordinated-vulnerability-d-1765
Whitepaper: https://www.sit.fraunhofer.de/fileadmin/dokumente/artikel/20230208_Kurzfassung_Rechtsrahmen_der_Cybersicherheitsforschung.pdf
Website: https://www.sit.fraunhofer.de/de/cvd/