ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Sicherheitslücke aufgedeckt – und jetzt?! Coordinated Vulnerability Disclosure aus rechtlicher und praktischer Sicht

Christian Köpp
Mit einem rechtlichen Problemaufriss von Linda Schreiber

Kurzzusammenfassung des gleichnamigen Vortrags im Rahmen der Veranstaltungsreihe „Rechtsrahmen der Cybersicherheitsforschung“

veranstaltet von Dr. Annika Selzer und Prof. Dr. Indra Spiecker gen. Döhmann

Impressum

Layout und Satz
Olivia Gude

Kontakt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Coordinated Vulnerability Disclosure aus rechtlicher und praktischer Sicht

Ein rechtlicher Problemaufriss von Linda Schreiber

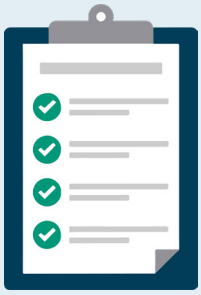
Gegenstand vieler Forschungsvorhaben im Bereich der IT-Sicherheitsforschung ist die Untersuchung von Hard- und Software verschiedener Hersteller, die sich im produktiven Einsatz befinden. Hierbei entdecken WissenschaftlerInnen häufig Schwachstellen, also Funktionsverhalten von Hard- oder Software das gegen explizite oder implizite Sicherheitsrichtlinien verstößt und dadurch beispielsweise Angreifern ermöglicht Aktionen auszuführen, die ihnen sonst nicht zur Verfügung stünden.

Beim Umgang mit entdeckten Schwachstellen sind verschiedene Risiken zu berücksichtigen: Solange die Schwachstelle offen ist und Anwender keine Kenntnis derer haben, können sie sich nicht vor möglichen Risiken schützen. Wenn allerdings Details zu einer Schwachstelle der breiten Öffentlichkeit bekannt werden, bevor es Abhilfemaßnahmen wie Sicherheitsupdates gibt, können diese von Kriminellen ausgenutzt werden, die sonst möglicherweise keine Kenntnis der Schwachstelle erlangt hätten.WissenschaftlerInnen stehen bei der Entdeckung von Schwachstellen vor der Frage, wie sie mit dem Wissen über die Schwachstelle umgehen sollen, mit wem sie es in welcher Form teilen sollten und auch, wie sie damit in wissenschaftlichen Publikationen umgehen.

Tätigkeiten von Forschenden sind durch die Wissenschaftsfreiheit nach Art. 5 Abs. 3 GG geschützt. Hiervon umfasst ist unter anderem die Entscheidungsbefugnis hinsichtlich des Forschungsgegenstands und der Fragestellung, der Methodik sowie der Publikation von Ergebnissen. Die Wissenschaftsfreiheit gilt allerdings nicht uneingeschränkt. Schranken ergeben sich aus anderen grundgesetzlich geschützten Rechtsgütern, wie im Falle der Veröffentlichung von Schwachstellen beispielsweise der Eigentums- oder der Berufsfreiheit (Art. 14 und 12 GG) des Herstellers und der Anwender der betroffenen Produkte. Bei kollidierenden Grundrechten sind diese im jeweiligen Einzelfall durch Abwägung zu einem angemessenen Ausgleich zu bringen. Im Verfassungsrecht spricht man hier von der Herstellung praktischer Konkordanz.

Ein Prozess, der in der Praxis der Meldung von Schwachstellen einen vergleichbaren Interessensausgleich und eine vertrauensvolle Zusammenarbeit anstrebt, ist das Responsible oder auch Coordinated Vulnerability Disclosure Verfahren. Coordinated Vulnerability Disclosure (CVD) meint den koordinierten Informationsaustausch zwischen Schwachstellenmeldenden, Hersteller bzw. Anbieter des betroffenen IKT-Produkts und ggf. anderen Beteiligten und hat die Minimierung des von der Schwachstelle ausgehenden Risikos zum Ziel. Dafür wird die Schwachstelle in einer Weise gemeldet, die eine Untersuchung, Diagnose und die Entwicklung von Maßnahmen zur Risikominimierung etwa durch Behebung oder Korrektur der Schwachstelle durch die produktverantwortliche Person oder Organisation erlaubt, bevor detaillierte Informationen zur Schwachstelle an die Öffentlichkeit gegeben werden.

Zur Festlegung der Rahmenbedingungen einer solchen koordinierten Schwachstellenmeldung gibt es CVD Policies. Hierin wird der CVD-Prozess beschrieben und Angaben gemacht wie bspw.:



- Zeitplan
- Kontakt und sichere Kommunikation
- Inhalt und Qualität
- Rechtliche Aspekte

CVD Policies dienen damit nicht nur WissenschaftlerInnen, die für Forschungseinrichtungen arbeiten, sondern allen zivilgesellschaftlichen Akteuren oder Unternehmen, die eine Schwachstelle melden wollen, dies in einem geregelten Rahmen zu tun. Allerdings gehört CVD noch nicht bei allen Akteuren zur gängigen Praxis. So gibt es immer wieder Fälle, in denen Wissenschaftler mit Informationen von durch sie identifizierte Schwachstellen an Herstellerunternehmen oder Organisationen herantreten, um diese auf Schwachstellen hinzuweisen und dort ablehnend, überhaupt nicht oder sogar durch das Einleiten rechtlicher Schritte reagiert wird. Abhängig von der jeweiligen nationalen Rechtslage bestehen beispielsweise straf- oder urheberrechtliche Haftungsrisiken bei der Erforschung von Schwachstellen.

Um CVD-Verfahren stärker in den EU-Mitgliedsstaaten zu etablieren, sieht die kürzlich beschlossene NIS-2-Richtlinie vor, dass Mitgliedsstaaten als Teil ihrer Nationalen Cybersicherheitsstrategie CVD Policies verabschieden. Zudem hat jeder Mitgliedsstaat ein Computer security incident response team als Koordinatoren bzw. vertrauenswürdigen Vermittler in CVD-Verfahren zu benennen, der die Interaktion zwischen Meldendem und Herstellern oder Anbietern erleichtern kann.

Linda Schreiber ist Referentin für Recht, Verträge und Finanzen in der Geschäftsstelle des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE am Fraunhofer SIT.

Coordinated Vulnerability Disclosure aus rechtlicher und praktischer Sicht

Ein praktischer Kurzüberblick von Christian Köpp

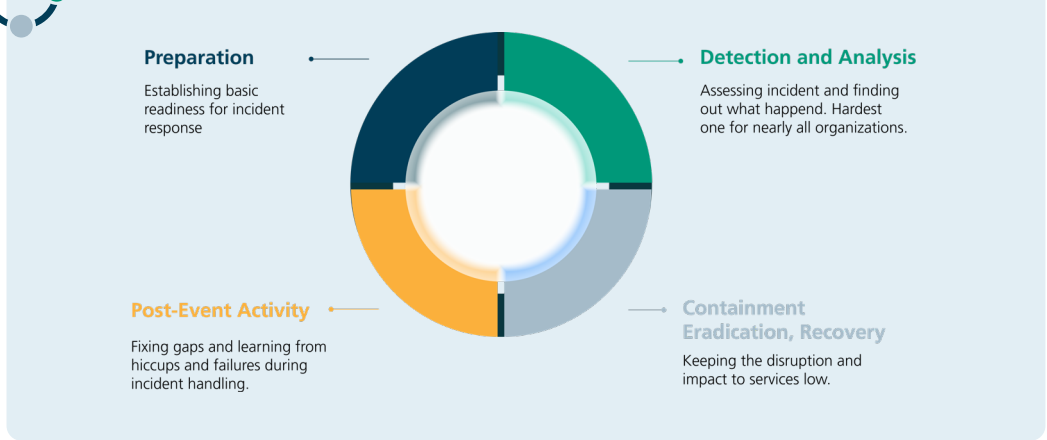
Das Ausnutzen von (bekannten) Schwachstellen in IT-Anwendungen und Infrastrukturen ist heute, mit Hilfe der Möglichkeiten des Internets, einfacher denn je. Fehlerhafte Konfigurationen, veraltete Softwareversionen, ein kleiner Fehler im Quelltext mit fatalen Folgen für angestrebte Schutzziele oder das sprichwörtlich offen einsehbare Passwort – es gibt viele Missstände, die in der Praxis täglich auftreten.

Obwohl Betreiber von IT-Infrastrukturen und Softwareautoren signifikante Aufwände betreiben, um derartige Probleme präventiv zu verhindern, sind sie nicht ausgeschlossen und Teil des Alltags einer jeden IT-Abteilung. Auch wir Cybersecurity Experten befassen uns täglich in reaktiver Form mit ihnen, denn sie dienen ebenso als eine der Hauptangriffsvektoren für Kriminelle und staatliche Akteure, wenn es darum geht, in fremde Netze einzudringen. Unternehmen, Behörden sowie Privatpersonen sind darauf angewiesen, dass sicherheitskritische Bugs schnellstmöglich beseitigt werden, um Missbrauch zu verhindern und IT-Systeme zeitnah abzusichern. Bei der Coordinated Vulnerability Disclosure (CVD) wirken Finder mit den Betroffenen und den Herstellern in einem strukturierten Verfahren zusammen.

» Der Mehrwert von einer Coordinated Vulnerability Disclosure kommt zum Tragen, da es essenziell ist, dass der Finder bzw. Security Researcher mit uns zusammenarbeitet und uns eine gute Beschreibung liefert: Was genau denkt man gefunden zu haben? Eine Step-by-Step Anleitung, wie man vorgehen muss, um da etwas zu exploiten und auch das Statement, ob es reproducable ist. Je tiefer unser Verständnis von der Schwachstelle ist, desto sicherer ist der Patch am Schluss. «

Dazu haben viele Firmen Spezialistenabteilungen, Computer Emergency Response Teams (CERT), ins Leben gerufen, die als zentrale Schnittstelle zwischen Sicherheitsforschern und den operativen Einheiten in Unternehmen fungieren. Außerhalb des betroffenen Unternehmens wird selten bekannt, welche firmeninternen Prozesse in diesen Fällen abgerufen werden und wie Unternehmen auf derartige Meldungen im Detail reagieren.

Incident Response Life Cycle



Quelle: NIST Computer Security Incident Handling Guide

- **Preparation**

» Die erste Phase ist die schöne Phase, da ist erst mal gar nichts passiert, sondern man bereitet sich auf eine Incident Meldung vor. Haben wir alles, was wir brauchen? Müssen wir irgendwas verbessern oder sind wir bereit loszurennen, sobald die Alarmglocken schrillen? «

- **Detection and Analysis**

» Die nächste Phase ist die Detection and Analysis Phase, da geht es vor allem darum zu verstehen, was überhaupt passiert ist. Jemand hat irgendwas gefunden, wie schlimm ist es und wen brauchen wir? Was müssen wir tun? Das ist auch die Phase, die am Anfang etwas dauert, wenn Schwachstellen gemeldet werden. An der Stelle muss man ein tiefes Verständnis dafür bekommen, was genau los ist, um richtig reagieren zu können. «

- **Containment, Eradication, Recovery**

» Die Phase, bei der man dann wirklich von einem Feuerwehreinsatz sprechen kann und die Lösch-fahrzeuge quasi ausrücken, ist die Containment, Eradication und Recovery Phase. Hier geht es wirklich darum, den Brand einzudämmen und zu sagen „wir müssen jetzt folgende Maßnahmen ergreifen, in dieser Priorität". «

- **Post-Event Activity**

» Eine Phase, die wirklich wichtig ist und die viele vergessen, sobald der Brand aus ist, ist die Post-Event Activity. Jeder Incident ist anders. Es ist wirklich wichtig, auch danach noch mal durchzugehen zu sagen „Was hat denn gut funktioniert, was müssen wir verbessern, was sind die Lessons Learned". «

Christian Köpp ist der Head des Europäischen Cybersecurity Incident Response Teams in SAP.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Sicherheitslücke aufgedeckt – und jetzt?! Coordinated Vulnerability Disclosure aus rechtlicher und praktischer Sicht