Schwachstellen korrekt melden

Schwachstellen kommen in praktisch jeder Software vor. Diese werden durch professionelle Penetration Tester, aber auch interessierten Informatiker gefunden (sogenannte Ethical Hacker). Doch wie sollen diese Schwächen gemeldet werden, damit sie geschlossen werden können? Mit dem Coordinated Vulnerability Disclosure (CVD) stehen ein Verfahren zur Meldung von Schwachstellen zur Verfügung.

CVD, die koordinierte Offenlegung von Schwachstellen bezieht sich auf einen strukturierten Ansatz zur Offenlegung von Sicherheitslücken in Software oder Systemen. Dieser Prozess zielt darauf ab, die Zusammenarbeit zwischen Sicherheitsforschern, Organisationen und Softwareanbietern zu fördern, um Schwachstellen verantwortungsbewusst zu identifizieren, zu melden und zu beheben. Angelehnt an die ISO-Standards ISO 29417 und ISO 30111 durchläuft dieser Prozess folgende Schritte:

1 Identifikation von Schwachstellen: Sicherheitsforscher entdecken potenzielle Sicherheitslücken in Software oder Systemen.
2. Vertrauliche Meldung: Die Forscher melden die Schwachstellen vertraulich an den Softwareanbieter oder die verantwortliche Organisation, anstatt sie öffentlich zu machen.
3. Koordinierung: Es wird eine Koordinationsphase eingeleitet, in der der Anbieter die Meldung prüft, die Schwere der Lücke bewertet und einen Plan für die Behebung erstellt.
4. Zeitplan für die Offenlegung: Ein Zeitplan für die Veröffentlichung der Schwachstelle wird festgelegt, um genügend Zeit für die Behebung zu gewährleisten, bevor Details öffentlich gemacht werden.
5. Zusammenarbeit: Es erfolgt eine enge Zusammenarbeit zwischen dem Sicherheitsforscher und dem Softwareanbieter, um die Lücke zu verstehen, zu beheben und sicherzustellen, dass die Informationen verantwortungsbewusst geteilt werden.
6. Veröffentlichung von Informationen: Nach der Behebung der Schwachstelle erfolgt die Veröffentlichung von Informationen über die Lücke, um die Benutzer zu informieren und sicherzustellen, dass sie angemessene Massnahmen ergreifen können.

In vielen Ländern existieren sogenannte Anti-Hacker-Paragrafen. Zum Beispiel im Schweizer Strafgesetzbuch:

Art. 143bis

1 Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
2 Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Art. 144bis

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Die rechtliche Situation ändern

Die Gratwanderung zwischen verboten und erlaubt, ist damit sehr eng gesteckt. Damit Sicherheitsforscher nicht mit dem Gesetz in Konflikt kommen, sind verschiedene Staaten daran, die rechtliche Situation zu ändern. Nachfolgende Punkte gilt es zu klären:

- Änderungen der Strafgesetze und der Richtlinie über Cyberkriminalität, um Sicherheitsforschern, die an der Aufdeckung von Sicherheitslücken beteiligt sind, rechtlichen Schutz zu bieten;
- die Festlegung spezifischer Kriterien für eine klare Unterscheidung zwischen «ethischem Hacking» und «Black Hat»-Aktivitäten vor der Einführung eines rechtlichen Schutzes für Sicherheitsforscher;
- Schaffung von Anreizen für Sicherheitsforscher, sich aktiv an der CVD-Forschung zu beteiligen, entweder durch nationale oder europäische Bug-Bounty-Programme oder durch die Förderung und Durchführung von Schulungen im Bereich der Cybersicherheit.

Doch wohin sollen sich die Sicherheitsforscher bei der Entdeckung einer Schwachstelle wenden? Dazu werden zwei Möglichkeiten genutzt:

- Ein Formular auf der Webseite, mit welchem anonym Schwachstellen gemeldet werden können. Zwei Beispiele:

Schwachstellen kommen in praktisch jeder Software vor.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

NCSC (Nationales Zentrum für Cybersicherheit): www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html

European Telecommunications Standards: www.etsi.org/standards/coordinated-vulnerability-disclosure

– Anbringen einer Text-Datei mit dem Namen security.txt auf der Homepage. Der RFC 9116 (www.rfc-editor.org/rfc/rfc9116.html) beschreibt den Inhalt dieser Datei. Ein Beispiel kann unter www.gosecurity.ch/.well-known/security.txt abgerufen werden

Einige Firmen gehen noch einen Schritt weiter und bieten ein Bug Bounty Programm an. Die Schlüsselaspekte eines Bug-Bounty-Programms sind:

– Belohnungen: Das Unternehmen bietet finanzielle oder andere Belohnungen für die Entdeckung und Meldung von Sicherheitslücken. Die Höhe der Belohnungen kann je nach der Schwere der Schwachstelle variieren.
– Umfang: Das Bug-Bounty-Programm legt den Umfang fest, das heisst, welche Systeme oder Anwendungen für die Überprüfung durch Sicherheitsforscher offen sind. Dies schliesst typischerweise Webanwendungen, mobile Anwendungen, Server und andere Softwareprodukte ein.
– Regeln und Richtlinien: Das Programm enthält klare Regeln und Richtlinien für Sicherheitsforscher. Dazu gehören oft Anforderungen für die vertrauliche Meldung von Schwachstellen, eine Erklärung der Arten von Schwachstellen, die für Belohnungen in Frage kommen, und ethische Richtlinien.
– Kommunikation: Es wird ein Kommunikationskanal etabliert, über den Sicherheitsforscher ihre Erkenntnisse melden können. Dies kann eine dedizierte E-Mail-Adresse, ein Webformular oder ein anderes Medium sein.
– Bewertung und Koordination: Nach dem Erhalt einer Meldung bewertet die Organisation die Schwere der Schwachstelle und koordiniert mit dem Melder, um weitere Details zu erhalten. Dann wird ein Plan für die Behebung der Schwachstelle erstellt.

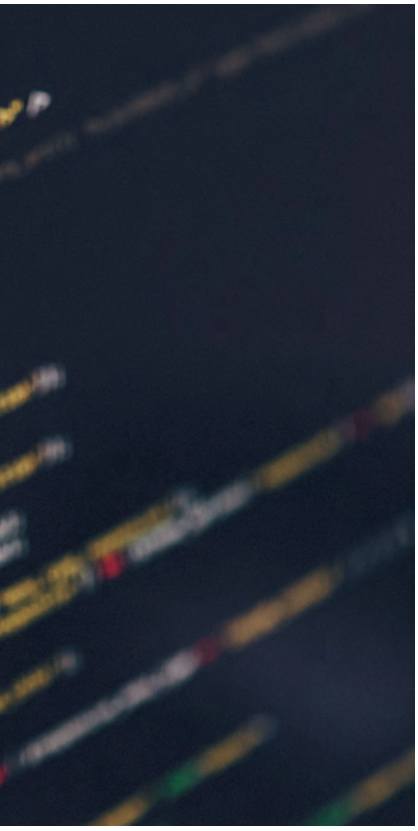

Bild: Pixabay

Zusammenfassend bieten Bug-Bounty-Programme eine proaktive Möglichkeit, die Sicherheit zu verbessern, indem ein Unternehmen die Fähigkeiten einer breiteren Sicherheitsgemeinschaft nutzt. Für Sicherheitsforscher bieten sie eine legale und ethische Plattform, um ihre Fähigkeiten zu nutzen und Belohnungen für ihre Bemühungen zu erhalten.

Fazit

Jedes Unternehmen sollte sich überlegen, welche Kontaktmöglichkeit es Sicherheitsforschern zur Verfügung stellt. Wahlweise via Formular oder der security.txt auf der Homepage. Ethical Hacker auf der anderen Seite sollten sich bewusst sein, dass ein Hacken ohne Auftrag in vielen Ländern strafbar ist. Wenn sie sich aber an das Vorgehen «coordinated vulnerability disclosure» halten, können sie einen nachhaltigen Beitrag zur Erhöhung der Informationssicherheit bieten.