Bug-Bounty-Programm

Unsere Sicherheitsexperten unterstützen Sie bei Aufbau, Betrieb und Organisation eines Bug-Bounty-Programms. Wir unterstützen Sie mit unserer Expertise bei der Planung des Prüfungsumfangs bis hin zur Sichtung, Prüfung und Priorisierung eingehender Schwachstellenberichte.

Grundlegendes zum Bug-Bounty-Programm

Das Ziel eines Bug-Bounty-Programms ist es, Schwachstellen zu identifizieren, bevor diese ausgenutzt werden. Durch das Programm kann sich Ihr Unternehmen das Know-how und den Ideenreichtum einer Gemeinschaft von Sicherheitsexperten (Community) zunutze machen. Hierzu wird die Community eingeladen, einen vorher definierten Bereich Ihres Unternehmens auf Schwachstellen zu analysieren. Die Regeln, an die sich die Community während des Programms zu halten hat, werden im Vorfeld von Ihrem Unternehmen festgelegt. Der Entdecker einer Schwachstelle erhält ggf. eine Belohnung, die von der Kritikalität der gefundenen Schwachstelle abhängig ist.

Bug-Bounty-Plattformen

Ein Anbieter von Bug-Bounty-Plattformen stellt die Expertise der angeschlossenen Community von Sicherheitsexperten zur Verfügung. Die Regeln sind klar definiert und die Schwachstellenberichte werden ausschließlich über die Plattform ausgetauscht. Dadurch werden die Schwachstellen koordiniert und sicher an das Unternehmen herangetragen. Bug-Bounty-Programme können auch anbieterunabhängig, ohne zentrale Bug-Bounty-Plattform realisiert werden. Dabei wird die Kommunikation und die Koordination mit den Sicherheitsexperten vom Unternehmen selbst durchgeführt.

Ihre Vorteile durch unsere Leistung

Damit das Bug-Bounty-Programm effektiv und ohne unnötige Einschränkung durchgeführt werden kann, muss es passgenau auf die Bedürfnisse des Unternehmens zugeschnitten sein und die Organisationsstrukturen berücksichtigen. Als Full Service Provider verfügen wir über die nötige Expertise, den Untersuchungsumfang mit Ihnen zusammen zu bestimmen. Wir haben Erfahrung in der Zusammenarbeit mit führenden Anbietern von Bug-Bounty-Plattformen und übernehmen für Sie die Kommunikation mit der Community von Sicherheitsexperten. Die Schwachstellenberichte werden von unseren Sicherheitsexperten überprüft und priorisiert. Auf Wunsch unterstützen wir Sie bei der Behebung der identifizierten Schwachstellen.

Preis

Der Umfang dieser Leistung wird individuell bestimmt. Er ist beispielsweise abhängig von der gewünschten Unterstützung während des Bug-Bounty-Programms. Kontaktieren Sie uns! Gerne erstellen wir Ihnen ein individuelles Angebot.

Vorgehensmodell-Phasen

Unsere Vorgehensweise wird individuell an Ihre Bedürfnisse und die Projektphase angepasst. Das untenstehende Vorgehen ist als exemplarisch anzusehen.

Kick-off

Die Vorbereitung erfolgt im Rahmen eines Kick-off-Meetings mit den technischen und organisatorischen Verantwortlichen Ihres Unternehmens. Wir besprechen mit Ihnen die Ausgangssituation und Ihre Zielsetzung sowie die Art der Belohnung. Gemeinsam mit Ihnen bestimmen wir das weitere Vorgehen entsprechend Ihrer Bedürfnisse, Ressourcen und den Gegebenheiten in Ihrem Unternehmen.

Konzeptausarbeitung

Während der Konzeptausarbeitung klären wir mit Ihnen, inwiefern die internen Fachabteilungen eingebunden werden und welche Schnittstellen vorhanden sind. Wir bestimmen mit Ihnen zusammen den Untersuchungsumfang, die Richtlinien der Responsible Disclosure und die Handhabung eintreffender Schwachstellenberichte der Community. Außerdem definieren wir kommunikative Prozesse und Eskalationswege. Auf Wunsch realisieren wir eine Anbindung an Ihr internes Ticketsystem.

Optionale Beurteilung

Bevor das Bug-Bounty-Programm startet, überprüfen unsere Sicherheitsexperten auf Wunsch den festgelegten Untersuchungsumfang mithilfe eines Pentests oder Code Reviews.

Livegang des Programms

Gemeinsam mit unseren Sicherheitsexperten wird das Bug-Bounty-Programm gestartet. Je nach definiertem Prozess werden die eingehenden Berichte zu identifizierten Schwachstellen durch unsere Sicherheitsexperten validiert und priorisiert. Wir übernehmen die Kommunikation mit der Community und leiten gefundene Schwachstellen an die Fachabteilung weiter. Die Ausgabe der Belohnung wird durch den Verantwortlichen Ihres Unternehmens veranlasst.

Schwachstellenbehebung

Unsere Sicherheitsexperten empfehlen Maßnahmen zur Beseitigung identifizierter Schwachstellen und unterstützen Sie bei Bedarf bei der Umsetzung dieser Empfehlungen. Optional übernehmen wir für Sie die Kommunikation mit den beteiligten Fachabteilungen.

Hinweis

Ein Bug-Bounty-Programm ersetzt nicht die Implementierung und Ausführung einer allgemeinen IT Sicherheitsstrategie.

Dieses Produktblatt hat Gültigkeit, sofern keine aktuellere Version veröffentlicht wurde. *Erstellungsdatum: 15.11.2018*

usd AG
Frankfurter Straße 233, Haus C1 | 63263 Neu-Isenburg
www.usd.de
Telefon: +49 6102 8631-190 | E-Mail: vertrieb@usd.de
PGP oder S/MIME für verschlüsselte Kommunikation.