# DER.7 Bug-Bounty-Programme

## 1. Beschreibung

### 1.1. Einleitung

Die Komplexität moderner IT-Landschaften führt dazu, dass trotz umfassender interner Sicherheitsprüfungen Schwachstellen in produktiven Systemen verbleiben können. Bug-Bounty- und Vulnerability-Disclosure-Programme (VDP) bieten einen strukturierten und kooperativen Rahmen, um das globale Fachwissen externer, ethischer Sicherheitsforscher zur Identifizierung dieser Schwachstellen zu nutzen. Anstatt auf eine zufällige oder potenziell schädliche Entdeckung zu warten, schaffen Institutionen proaktiv einen Anreiz und einen sicheren Kanal für die Meldung von Sicherheitslücken.
Dieser Baustein ergänzt die reaktiven und proaktiven Sicherheitsmaßnahmen einer Institution. Während Bausteine wie DER.1 (Detektion von sicherheitsrelevanten Ereignissen) und DER.2 (Security Incident Management) auf die Erkennung und Behandlung von Angriffen abzielen und die hypothetischen Bausteine CON.12 (Threat Hunting) und DER.6 (Security Automation) die interne Abwehr stärken, öffnet DER.7 den Blick nach außen und nutzt die kollektive Intelligenz zur Schwachstellenidentifikation.

### 1.2. Zielsetzung

Dieser Baustein zeigt einen systematischen Weg auf, wie Institutionen Programme zur Meldung von Schwachstellen durch Externe planen, rechtssicher aufsetzen, durchführen und nachbereiten können. Ziel ist es, die Anzahl unentdeckter Sicherheitslücken zu reduzieren, die Reaktionszeit auf neu gefundene Schwachstellen zu verkürzen und eine positive, kooperative Beziehung zur Sicherheitsforschungsgemeinschaft aufzubauen.

### 1.3. Abgrenzung und Modellierung

Der Baustein DER.7 Bug-Bounty-Programme ist auf den Informationsverbund einmal anzuwenden.
Dieser Baustein beschreibt nicht die technische Behebung der gemeldeten Schwachstellen. Die Anforderungen an einen funktionierenden Schwachstellen- und Patchmanagement-Prozess sind im Baustein ISMS.3.2 Schwachstellen- und Patchmanagement beschrieben. Die Reaktion auf kritische, bereits ausgenutzte Schwachstellen muss über die Prozesse aus DER.2.1 Behandlung von Sicherheitsvorfällen erfolgen.

## 2. Gefährdungslage

Für den Baustein DER.7 Bug-Bounty-Programme sind folgende spezifische Bedrohungen und Schwachstellen von besonderer Bedeutung:

# Unentdeckte Schwachstellen in produktiven Anwendungen

Trotz etablierter Entwicklungs- und Testprozesse können Schwachstellen in Software und Systemen unentdeckt in den Produktionsbetrieb gelangen. Diese stellen ein erhebliches

Risiko dar, da sie von Angreifern ausgenutzt werden können, lange bevor sie intern bemerkt werden.

## Unkoordinierte Offenlegung von Schwachstellen

Wenn Sicherheitsforscher Schwachstellen entdecken, aber keinen klaren und sicheren Meldekanal vorfinden, können sie diese unkoordiniert veröffentlichen ("Full Disclosure"). Dies gibt der Institution keine Zeit, die Lücke zu schließen, und setzt die Systeme und Daten einem hohen Risiko aus.

## Rechtsunsicherheit im Umgang mit Sicherheitsforschern

Fehlt eine klare rechtliche Zusicherung ("Safe Harbor"), könnten Sicherheitsforscher aus Angst vor rechtlichen Konsequenzen davon absehen, gefundene Schwachstellen zu melden. Ebenso kann auf Seiten der Institution Unsicherheit darüber bestehen, wie mit Meldungen und den Forschern umzugehen ist, was zu fehlerhaften Reaktionen führen kann.

## Ineffiziente Bearbeitung von externen Schwachstellenmeldungen

Ohne einen definierten Prozess laufen Meldungen über unspezifische Kanäle (z. B. allgemeine E-Mail-Adressen, soziale Medien) ein. Dies führt dazu, dass Meldungen verloren gehen, nicht rechtzeitig an die zuständigen Stellen weitergeleitet oder von unqualifiziertem Personal nicht als relevant erkannt werden.

## Reputationsschaden durch unsachgemäße Kommunikation

Eine langsame, unprofessionelle oder abweisende Kommunikation mit Sicherheitsforschern, die eine Schwachstelle melden, kann zu erheblichem Reputationsschaden in der Fachgemeinschaft führen. Dies kann zukünftige Meldungen verhindern und die Institution als unkooperativ darstellen.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.7 Bug-Bounty-Programme aufgeführt.

## 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden. Ein grundlegendes Vulnerability Disclosure Program (VDP) ist das Minimum.

DER.7.A1 Festlegung einer Richtlinie für die Entgegennahme von Schwachstellenmeldungen (B)
Es MUSS eine von der Leitungsebene verabschiedete Richtlinie für den Umgang mit extern gemeldeten Schwachstellen geben. Diese Richtlinie MUSS die grundlegenden Ziele, Verantwortlichkeiten und die Verpflichtung der Institution zur Zusammenarbeit mit Sicherheitsforschern festlegen.
DER.7.A2 Erstellung und Veröffentlichung einer Vulnerability Disclosure Policy (VDP) (B)
Es MUSS eine klare und leicht auffindbare Vulnerability Disclosure Policy (VDP) erstellt und veröffentlicht werden. Die VDP MUSS mindestens folgende Punkte enthalten: eine Erklärung der Absicht, den Meldekanal, eine grundlegende Beschreibung der Systeme, die im Geltungsbereich liegen (Scope), und welche Arten von Tests nicht gestattet sind.
DER.7.A3 Einrichtung eines dedizierten und sicheren Meldekanals (B)
Es MUSS ein klar definierter und sicherer Kanal für die Entgegennahme von Schwachstellenmeldungen eingerichtet werden (z. B. security@institution.de mit veröffentlichtem PGP-Schlüssel). Dieser Kanal MUSS regelmäßig überwacht werden.
DER.7.A4 Formulierung einer rechtlichen Schutzzusage (Safe Harbor) (B)
Die VDP MUSS eine "Safe Harbor"-Klausel enthalten. Diese MUSS zusichern, dass die Institution keine rechtlichen Schritte gegen Personen einleitet, die Schwachstellen im Rahmen der in der VDP definierten Regeln und in gutem Glauben suchen und melden.
DER.7.A5 Definition eines initialen Triage-Prozesses (B)
Es MUSS ein interner Prozess definiert werden, wie eingehende Meldungen bestätigt, auf ihre Validität geprüft und an die zuständigen Stellen weitergeleitet werden. Alle Melder MÜSSEN eine Eingangsbestätigung erhalten.

### 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden, um ein effektives Bug-Bounty-Programm zu betreiben.
DER.7.A6 Detaillierte Definition von Scope und Testregeln (S) [Fachverantwortliche, ISB]
Der Geltungsbereich (Scope) des Programms SOLLTE detailliert definieren, welche Anwendungen, Systeme und Arten von Schwachstellen abgedeckt sind und welche explizit ausgeschlossen werden. Es SOLLTEN klare Regeln für die Durchführung von Tests festgelegt werden, um Störungen des produktiven Betriebs zu vermeiden (z. B. Verbot von DoS-Tests, Social Engineering).
DER.7.A7 Etablierung eines transparenten Belohnungssystems (S) [Leitungsebene]
Für ein Bug-Bounty-Programm SOLLTE ein transparentes und motivierendes Belohnungssystem (Bounty-Schema) etabliert werden. Die Höhe der monetären Belohnungen SOLLTE sich an der Kritikalität der Schwachstelle (z. B. anhand des CVSS-Scores) orientieren. Auch nicht-monetäre Anreize (z. B. Hall of Fame) SOLLTEN in Betracht gezogen werden.
DER.7.A8 Etablierung eines Kommunikations- und Eskalationskonzepts (S) [ISB]
Es SOLLTE ein Kommunikationskonzept erstellt werden, das klare Service-Level-Ziele für die Kommunikation mit den Forschern definiert (z. B. Zeit bis zur ersten Reaktion, Zeit bis zur Triage, Zeit bis zur Behebung). Der Prozess SOLLTE sicherstellen, dass die Forscher über den Status ihrer Meldung informiert bleiben.
DER.7.A9 Integration in das Schwachstellen- und Incident-Management (S)
Verifizierte Schwachstellenmeldungen SOLLTEN systematisch in den internen

Schwachstellenmanagementprozess (siehe ISMS.3.2) überführt werden. Für kritische Schwachstellen SOLLTE eine direkte Anbindung an den Incident-Response-Prozess (siehe DER.2.1) existieren, um eine sofortige Reaktion zu gewährleisten.

DER.7.A10 Nutzung einer Bug-Bounty-Plattform (S)

Für die effiziente Verwaltung des Programms SOLLTE der Einsatz einer spezialisierten Bug-Bounty-Plattform (als Dienstleister) evaluiert werden. Solche Plattformen können die Kommunikation, die Triage, die Auszahlung von Belohnungen und die Einbindung von Forschern erheblich vereinfachen.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Die folgenden Anforderungen sind für diesen Baustein exemplarische Vorschläge für ein Schutzniveau, das über den Stand der Technik hinausgeht. Sie SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden.

DER.7.A11 Durchführung von privaten oder zeitlich begrenzten Programmen (H)

Für besonders schützenswerte Systeme oder vor der Einführung neuer kritischer Anwendungen SOLLTEN private, nur für eingeladene und geprüfte Forscher zugängliche Bug-Bounty-Programme durchgeführt werden. Alternativ können zeitlich begrenzte Programme mit hohen Belohnungen ("Bug Bashes") genutzt werden, um die Aufmerksamkeit auf bestimmte Bereiche zu lenken.

DER.7.A12 Proaktives Forscher-Management und Beziehungsaufbau (H)

Es SOLLTEN aktiv Beziehungen zu bekannten und erfolgreichen Sicherheitsforschern aufgebaut werden. Die Institution SOLLTE diese proaktiv in private Programme einladen und eine Gemeinschaft um ihr Sicherheitsprogramm herum fördern.

DER.7.A13 Analyse und Optimierung der Programm-Metriken (H) [ISB]

Das Bug-Bounty-Programm SOLLTE anhand von Metriken kontinuierlich überwacht und optimiert werden. Wichtige Kennzahlen wie die durchschnittliche Zeit bis zur Behebung, die Kosten pro gefundener Schwachstelle oder die am häufigsten betroffenen Systembereiche SOLLTEN regelmäßig analysiert werden, um die defensive Sicherheitsstrategie anzupassen.

DER.7.A14 Verknüpfung von Erkenntnissen mit dem Secure SDLC (H)

Die aus dem Programm gewonnenen Erkenntnisse über Schwachstellenmuster SOLLTEN systematisch in den Software Development Lifecycle (SDLC) zurückgeführt werden. Entwickler SOLLTEN gezielt zu den gefundenen Schwachstellenklassen geschult werden, um ähnliche Fehler in Zukunft zu vermeiden.