Deutsche Version: Um die Einführung eines eigenen BugBounty-Programmes zu erleichtern, stellt die IHK München und Oberbayern Muster zur Verfügung.

Versionierung des Dokumentes:

Version	Datum	Bearbeiter	Änderungen	Vertraulichkeitsstatus
1.0	24.07.2023	Bernhard Kux, IHK München und Oberbayern	Erstversion	Öffentlich

Rechtliche Hinweise zur Benutzung:

Bitte beachten Sie für die Verwendung des hier bereit gestellten Musters Folgendes:

- Das Muster wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit.
- Das Muster ist als Formulierungshilfen zu verstehen und soll nur eine Anregung bieten, wie die eigene Aktivität zur IT-Sicherheit sachgerecht gestaltet werden kann. Dies entbindet Sie jedoch nicht von der sorgfältigen eigenverantwortlichen Prüfung.
- Das Muster ist nur ein Vorschlag für eine mögliche Gestaltung. Sie können auch andere Formulierungen wählen. Vor einer Übernahme des unveränderten Inhaltes muss daher im eigenen Interesse genau überlegt werden, ob und in welchen Teilen gegebenenfalls eine Anpassung an die konkret zu gestaltende Situation erforderlich ist.
- Auf diesen Vorgang hat die Industrie- und Handelskammer keinen Einfluss und kann daher naturgemäß für die Auswirkungen auf keine Haftung übernehmen. Auch die Haftung für leichte Fahrlässigkeit ist grundsätzlich ausgeschlossen.

Um das Muster weiter zu verbessern sind wir für Anmerkungen und Verbesserungsvorschläge sehr dankbar.
Bitte schicken Sie diese an Bernhard Kux, kux@muenchen.ihk.de

---

Muster:

Hinweise auf Schwachstellen:
Name_Ihres_Unternehmens-BugBounty-Programm

Die *Name_Ihres_Unternehmens* setzt eine ganze Reihe von digitalen Services ein. Sicherheit der Daten und Prozesse hat dabei höchste Priorität. Trotzdem können diese digitalen Services Schwachstellen enthalten, die der *Name_Ihres_Unternehmens* noch nicht bekannt sind.
Daher sind wir sehr dankbar für Hinweise auf Schwachstellen!

Hierbei ist zu beachten: Bei der Suche nach Schwachstellen kann es sich ggf. um eine Straftat handeln. Daher bitten wir Sie, die folgenden Regeln zu beachten.

1. Was ist das *Name_Ihres_Unternehmens*-BugBounty Programm?

"BugBounty Programme" sind ein wichtiges Instrument zur Verbesserung der Sicherheit von digitalen Services, da sie eine Gemeinschaft von "ethischen Hackern" oder Sicherheitsforschern fördern, die dazu beitragen, potenzielle Schwachstellen aufzudecken, bevor sie von böswilligen Akteuren ausgenutzt werden können.

Das "*Name_Ihres_Unternehmens*-BugBounty Programm" ist eine Initiative der *Name_Ihres_Unternehmens*, um Personen zu belohnen, die Fehler, Sicherheitslücken oder "Bugs" in digitalen Services der *Name_Ihres_Unternehmens* aufdecken und melden. Der Ausdruck "Bug Bounty" kommt aus dem Englischen und bedeutet wörtlich übersetzt "Kopfgeld für Fehler".

Die Belohnung, das sogenannte "Bounty", variiert auf der Grundlage der Schwere und der Art des aufgedeckten Fehlers.

Am *Name_Ihres_Unternehmens*-BugBounty Programm kann jeder teilnehmen, der sich an die hier genannten Regeln hält.

2. Welche digitalen Services umfasst das Bug Bounty Programm?

Folgende Domains (inkl. ggf. vorhandener Subdomains) sind relevant für das Bug Bounty Programm der *Name_Ihres_Unternehmens*:

- Liste der Domains Ihres Unternehmens
- …

Manche der genannten Domains leiten auf nicht von der *Name_Ihres_Unternehmens* verantwortete Websites weiter. In diesem Fall umfasst das BugBounty-Programm nur die von der *Name_Ihres_Unternehmens* verantwortete Domain, aber nicht die Onlineanwendung (z. B. www…).

Bitte beachten Sie, dass nicht in der obigen Liste enthalte digitale Services nicht Teil des BugBounty Programms sind. Ggf. kann eine IT-Sicherheitsuntersuchung solcher nicht genannter Services als rechtswidrig eingestuft und entsprechend geahndet werden.

3. Regeln für das das BugBounty Programm!

Um am BugBounty Programm teilzunehmen, gilt grundsätzlich:
Der *Name_Ihres_Unternehmens* darf durch die Tätigkeiten im Rahmen des BugBounty Programms kein Schaden entstehen.
Das bedeutet:

- Beim Suchen nach Schwachstellen dürfen Verfügbarkeit, Vertraulichkeit und Integrität der Daten und Prozesse der *Name_Ihres_Unternehmens* nicht beeinträchtigt werden.
  Bitte führen Sie daher keine Phishing-Mail-, DDoS-, Brute-Force-Tests o. ä. durch. Ändern Sie keine Daten.
- Es dürfen keine Backdoors o.ä. eingebaut werden, die dauerhaften Zugriff ermöglichen.

- Gefundene Schwachstellen werden erst veröffentlicht, wenn diese von der *Name_Ihres_Unternehmens* geschlossen wurden.

Des Weiteren gilt:

- Nur die erstmalige Meldung einer Schwachstelle kommt für eine Bug Bounty-Auszahlung in Frage.
- Aktuelle und ehemalige Mitarbeiter der *Name_Ihres_Unternehmens* sowie Dienstleister und Zulieferer können nicht am BugBounty-Programm teilnehmen.
- Die *Name_Ihres_Unternehmens* legt den Auszahlungsbetrag fest (siehe 4.). Eine Auszahlung kann nur erfolgen, wenn der Teilnehmer am Bug Bounty-Programm der *Name_Ihres_Unternehmens* eine entsprechende und der geltenden Umsatzbesteuerung gerecht werdende Rechnung stellt.

4. So können Sie uns eine Schwachstellen-Meldung zukommen lassen

Bitte geben Sie uns im Falle einer Kontaktaufnahme folgende Informationen:

- Exakte Domain an, auf welcher Sie die Schwachstelle gefunden haben
- Möglichst viele Details zur Reproduktion der Schwachstelle, um uns die Analyse zu erleichtern und damit die Auszahlung der Belohnung zu beschleunigen. Z. B. IP-Nummer von der aus getestet wurde, Proof-Of-Concept-Skizzen.

Bitte kommunizieren Sie mit uns über E-Mails an
bugbounty@*MAIL_DOMAIN_IHRES_UNTERNEHMENS*

5. Was tut die *Name_Ihres_Unternehmens* mit Meldungen von Schwachstellen?

Eine eingereichte Schwachstellenmeldung wird von der *Name_Ihres_Unternehmens* bewertet und in eine Kritikalitätsstufe eingeordnet. Maßstab hierbei ist das Gefahrenpotenzial.
Orientierung kann hier der „Common Vulnerability Scoring System Calculator“ (siehe https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) sein, mit dem Schwachstellenmeldungen in Kategorien eingeordnet werden können.

Schwachstelle-Einordnung	**Niedrig**	**Mittel**	**Hoch**	**Kritisch**
CVSS-Score	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0
BugBounty (Nettobetrag vor Umsatzversteuerung)	bis 100 €	100 – 500 €	500 – 1.000 €	über 1.000 €

Hierbei sind für die *Name_Ihres_Unternehmens* insbesondere Schwachstellen interessant, die es Unberechtigten ermöglichen auf vertrauliche Daten zuzugreifen, diese zu ändern oder zu löschen.

Beispiele für relevante Schwachstellen finden sich z. B. bei OWASP (https://owasp.org/www-project-top-ten/) wie z. B.

- Cross-site request forgery (CSRF / XSRF) (https://de.wikipedia.org/wiki/Cross-Site-Request-Forgery)
- persistent Cross-Site-Scripting (XSS) https://www.enisa.europa.eu/topics/incident-response/glossary/cross-site-scripting-xss
- SQL Injections (https://owasp.org/www-community/attacks/SQL_Injection)

Nicht relevant im BugBounty-Programm sind beispielweise:

- Grundsätzliche Erreichbarkeit von digitalen Services
- Phishing-Mails u. ä., insbesondere solche, in denen z. B. die Mailadressen der *Name_Ihres_Unternehmens* missbraucht werden
- Schwachstellen ohne Nachweis einer Ausnutzbarkeit
- Schwachstellen, die nur veraltete oder mit eingeschränkten Sicherheitsmerkmalen betriebene Browser betreffen
- Von Scannern erzeugte Berichte, die keinen konkreten und komplett nachvollziehbaren Bezug zu einer Schwachstelle ermöglichen
- Nicht eingesetzte Best-Practices in Headern, SSL/TLS, DNS