Coordinated Vulnerability Disclosure (CVD) Richtlinie

Die Sicherheit unserer Produkte, Systeme und Dienste ist uns wichtig. Trotz sorgfältiger Entwicklung, Implementierung, Konfiguration, Prüfung und sonstigen Sicherheitsmaßnahmen können Schwachstellen auftreten.

Sollten Sie eine oder mehrere Schwachstellen gefunden haben, können Sie sich vertrauensvoll im Rahmen dieser Richtlinie an uns wenden.

Unser Ziel ist es, gemeldete Schwachstellen schnell zu verstehen, zu beheben und – soweit angemessen – gemeinsam mit der meldenden Person eine koordinierte Veröffentlichung zu ermöglichen.

Anwendungsbereich

Unter dem Anwendungsbereich dieser Richtlinie fällt jedes reproduzierbare Security-, Design- oder Implementierungsproblem bei unseren Produkten, Webanwendungen oder anderweitigen Dienstleistungen, sofern es die Informations- oder IT-Sicherheit unserer Produkte oder der mit den Produkten verbundenen Dienste betrifft.

NICHT im Anwendungsbereich

Die Richtlinie gilt nicht für folgende Aktivitäten sowie Produkte und sollten nicht im Rahmen dieser Richtlinie gemeldet werden:

- Produkte und/oder Dienstleistungen von Drittanbietern, die nicht in unserem Eigentum stehen oder von uns verwaltet werden;
- fehlerhafte Konfigurationen auf Kundenseite;
- unsachgemäße Benutzung;
- physische Angriffe auf etwaige Produkte;
- Meldungen, die aus automatisierten Scan-Tools oder automatisierten Analysen resultieren.

Unser Versprechen

- Jeder Schwachstellenbericht wird innerhalb des gesetzlichen Rahmens vertraulich behandelt;
- personenbezogene Daten werden nicht ohne Ihre ausdrückliche Zustimmung an Dritte weitergegeben;
- Rückmeldung wird zu jeder getätigten Schwachstellenmeldung gegeben;
- Ansprechpartner für den vertrauensvollen Austausch während des gesamten Prozesses zu sein.

Unsere Erwartung

- Die gefundene Schwachstelle wurde nicht missbräuchlich ausgenutzt;
- es wurden keine Angriffe (wie z.B. Social-Engineering-, Spam-, (Distributed) DoS- oder „Brute Force“-Angriffe, etc.) gegen IT-Systeme oder Infrastrukturen durchgeführt;
- es wurde keine Manipulation, Kompromittierung oder Veränderung von möglichen Systemen oder Daten Dritter vorgenommen.

Eine Schwachstelle melden

Zur Analysierung, Reproduzierbarkeit und Behebung sollte die Meldung folgende Informationen erhalten:

- Eine kurze Beschreibung der Schwachstelle;
- eine Beschreibung der möglichen Auswirkungen;

- eine detaillierte Beschreibung der zur Reproduktion erforderlichen Schritte;
- Proof-of-Concept-Code oder Screenshots;
- eine Einschätzung des Schweregrads,
- gegebenenfalls Vorschläge zur Behebung.

Im Falle einer anonymen Meldung ist zu berücksichtigen, dass fachliche und inhaltliche Rückfragen nicht beantwortet und entsprechende Schwachstellenmeldungen daher nur eingeschränkt oder gegebenenfalls nicht bearbeitet werden können.

Zur Schwachstellenmeldung

Anerkennung

Wir schätzen die Unterstützung von Personen, die uns bei der Verbesserung unserer Sicherheit helfen und möchten Mitwirkende öffentlich durch eine Hall of Fame würdigen.

Eine Veröffentlichung des Namens oder anderer personenbezogener Daten erfolgt nur mit Zustimmung der betreffenden Person.

Safe-Harbor

Wir betrachten Sicherheitsforschung, die nach bestem Wissen und Gewissen sowie im Einklang mit dieser Richtlinie durchgeführt wird, als autorisierte Sicherheitsforschung.

Wir werden wegen einer solchen Forschung keine rechtlichen Schritte einleiten, sofern die Person:

- diese Richtlinie einhält;
- die Tests auf das notwendige Maß beschränkt;
- keine Daten manipuliert oder zerstört;
- keine unnötigen Risiken für unsere Systeme oder Dritte erzeugt;
- entdeckte Schwachstellen unverzüglich und vertraulich meldet;
- die Informationen bis zur abgestimmten Veröffentlichung vertraulich behandelt.

Diese Richtlinie stellt keine allgemeine Genehmigung für Aktivitäten außerhalb des definierten Geltungsbereichs dar.

Aktualisierung

Diese Richtlinie wird regelmäßig überprüft und kann bei Bedarf aktualisiert werden.