Datenschutzkonzept für interne Phishing-Tests

Unternehmen: MJ Cybersecurity Services
Version: 1.0
Datum: 03.04.2024
Erstellt von: Jesscia Storrer, Datenschutzbeauftragter

Inhaltsverzeichnis

1. Einführung und Zweck

Dieses Dokument beschreibt das Datenschutzkonzept für die Durchführung von internen Phishing-Tests mit dem Partner MJ Cybersecurity Services. Ziel ist es, das Bewusstsein und die Wachsamkeit der Mitarbeiter gegenüber Phishing-Angriffen zu erhöhen und die Sicherheit der Informationssysteme zu stärken.

2. Geltungsbereich und Anwendungsbereich

Das Konzept gilt für alle Abteilungen und Mitarbeiter, die in die Durchführung und Analyse der Phishing-Tests involviert sind. Es bezieht sich auf personenbezogene Daten, die während der Tests anonymisiert gesammelt werden.

3. Beschreibung der Datenverarbeitung

Versand von Phishing-E-Mails: Simulierte Phishing-E-Mails werden an Mitarbeiter gesendet, um ihre Reaktionen zu testen.
Fake-Login-Seite: Mitarbeiter, die auf Links in den E-Mails klicken, werden zu einer

kontrollierten Fake-Login-Seite weitergeleitet.
Datenanonymisierung: Persönliche Daten, die auf der Fake-Login-Seite eingegeben werden, werden sofort anonymisiert.
Klickratenreport: Erstellung eines Berichts über die Reaktionen der Mitarbeiter, einschliesslich Klickraten, ohne Zuordnung zu individuellen Personen.

4. Rechtliche Grundlage

Die Verarbeitung personenbezogener Daten für interne Phishing-Tests basiert auf dem legitimen Interesse vom Partner MJ Cybersecurity Services, die Sicherheit der Informationstechnologie zu gewährleisten

5. Risikobewertung und Datenschutz-Folgenabschätzung

Eine vorläufige Bewertung hat gezeigt, dass das Risiko für die Rechte und Freiheiten der Mitarbeiter als niedrig eingestuft wird, da die Daten anonymisiert verarbeitet und ausschliesslich für Sicherheitszwecke genutzt werden.

6. Technische und organisatorische Massnahmen

Verschlüsselung: Einsatz von Verschlüsselungstechnologien für die Übertragung und Speicherung von Daten.
Zugriffskontrolle: Zugriff auf die Daten ist streng beschränkt auf autorisierte Personen.
Schulungen: Regelmässige Schulungen der Mitarbeiter zu Datenschutzbestimmungen und Sicherheitspraktiken. Das dazugehörige DSG-Konzept wird separat für den CAT-Service aufgeführt.

7. Rechte der betroffenen Personen

Mitarbeiter werden über ihre Datenschutzrechte informiert, einschliesslich des Rechts auf Auskunft, Berichtigung und Löschung ihrer Daten. Anfragen können an den Datenschutzbeauftragten gerichtet werden.

8. Verfahren bei Datenschutzverletzungen

Im Falle einer Datenschutzverletzung werden umgehend Massnahmen ergriffen, um den Schaden zu minimieren und die zuständige Datenschutzbehörde gemäss den gesetzlichen Anforderungen zu benachrichtigen.

9. Überwachung und Überprüfung

Das Datenschutzkonzept wird jährlich überprüft und aktualisiert, um seine Effektivität sicherzustellen und auf Änderungen in den Geschäftspraktiken oder gesetzlichen Anforderungen zu reagieren.

10. Anhang

Änderungsprotokoll:

Erstellung; 03.04.2024

Kontaktinformationen: MJ Cybersecurity Services

Dieses Dokument dient als Grundlage für die Durchführung sicherer und rechtskonformer Phishing-Tests durch MJ Cybersecurity Services. Es unterstreicht unser Engagement für den Schutz personenbezogener Daten und die Verbesserung der Cybersicherheit.