Sample Incident Report

1. Basisinformationen

Incident-ID	IR-2025-PHISH-001
Datum/Uhrzeit Entdeckung	20.08.2025, 09:35
Entdeckt durch	SOC Analyst über SIEM
Meldende Abteilung	IT-Security Operations

2. Incident-Klassifikation

Typ	Phishing / Credential Theft
Severity-Level	High
Betroffene Systeme	Exchange, Active Directory
Betroffene Daten	Personenbezogene Mitarbeiterdaten

3. Beschreibung des Vorfalls

Ein Mitarbeiter erhielt eine täuschend echt aussehende Phishing-Mail mit einem Link zu einer gefälschten Login-Seite. Nach Eingabe seiner Zugangsdaten wurden unautorisierte Zugriffe festgestellt. Der Vorfall wurde durch das SOC frühzeitig erkannt.

4. Maßnahmen (Containment, Eradication, Recovery)

- Account des betroffenen Mitarbeiters sofort gesperrt - Phishing-Domain im Proxy und E-Mail-Gateway blockiert - Passwort-Reset für betroffenen Nutzer und MFA aktiviert - Systeme auf Malware untersucht – keine weiteren Funde - Awareness-Mail an alle Mitarbeiter verschickt

5. Kommunikation & Eskalation

SOC eskalierte den Vorfall an den IT-Admin, anschließend an den CISO. Legal/DSB wurden informiert, da personenbezogene Daten betroffen waren. Eine Meldung gemäß DSGVO Art. 33 wurde innerhalb von 72 Stunden an die Aufsichtsbehörde übermittelt.

6. Lessons Learned

- Früherkennung durch SIEM und Awareness hat funktioniert - Eskalationswege funktionierten wie vorgesehen - Verbesserungspotenzial: schnellere Information aller Mitarbeiter - Awareness-Kampagne zu Phishing wird intensiviert

7. Abschlussbewertung

Status: Behoben Rest-Risiken: Keine, da Passwörter zurückgesetzt und MFA aktiviert
Dokumente/Anhänge: Log-Auszüge, Awareness-Mail, Eskalationsdiagramm