CYBERTELL / CHECKLISTE FÜR DEN CYBERTELL-START

Checkliste für den CyberTell-Start

Was Ihre Firma vor dem Einrichten bereitstellt. Liegen diese Angaben vor, ist das Setup in einer Sitzung erledigt.

Schritt für Schritt · 8 Schritte

01 ### Ansprechpartner und ersten Admin bestimmen

Eine Person, die CyberTell für die Firma verwaltet: Vorname, Nachname und eine persönliche geschäftliche E-Mail-Adresse. Die Anmeldung läuft über einen E-Mail-Link und einen Passkey, Passwörter gibt es keine.

02 ### Postfach security@ einrichten

Ein Postfach oder eine Weiterleitung **security@ihre-domain.ch** anlegen, das zuverlässig E-Mails empfängt und regelmässig gelesen wird. CyberTell schickt die Bestätigung Ihrer Domain dorthin. Die Adresse dient auch als Meldestelle für Sicherheitsvorfälle.

> ! Ohne funktionierendes security@-Postfach lässt sich die Domain nicht bestätigen.

03 ### Domain und DMARC vorbereiten

Die Hauptdomain der Firma festlegen und den Zugang zur DNS-Verwaltung klären. Für die DMARC-Auswertung einen TXT-Record auf **_dmarc.ihre-domain.ch** setzen, mit CyberTell als Empfänger der Berichte:

```
v=DMARC1; p=none; rua=mailto:dmarc@cybertell.io
```

04 ### Mailversand für Phishing-Simulationen

Simulierte Phishing-Mails gehen über Ihren eigenen Mailserver. Bereithalten: SMTP-Host, Port (meist 587), Benutzer, Passwort sowie Absenderadresse und -name. Für die Absenderdomain müssen SPF und DMARC gesetzt sein, DKIM wird empfohlen.

05 ### Simulationen im Mailfilter freigeben

Damit Test-Mails ankommen, im Mailfilter den eigenen SMTP-Server und die Absenderdomain zulassen, in Microsoft 365 über «Erweiterte Zustellung» (Phishing-Simulation), in Google Workspace über eine Zulassungsliste. Optional eine eigene Tracking-Domain: TXT-Record **_cybertell-verify.ihre-domain.ch** und ein CNAME auf das im Portal angezeigte Ziel. Diese Domain ebenfalls freigeben.

06 ### Mitarbeiterliste als CSV

Alle Mitarbeiter mit Vorname, Nachname und geschäftlicher E-Mail-Adresse, optional Sprache (de, en, fr, it). Format: Semikolon als Trennzeichen, UTF-8, höchstens 2 MB. Jede E-Mail-Adresse muss eindeutig sein.

```
firstname;lastname;email;language
Max;Muster;max.muster@example.ch;de
```

07

Firmenprofil und IT-Umgebung

Logo, Website und eine kurze Beschreibung der Firma. Für die erste Risikoeinschätzung festhalten: eingesetzte Systeme (Windows, Active Directory, Microsoft 365, macOS, Linux), Firewall und Endpoint-Schutz, wichtige Lieferanten und wo Personendaten bearbeitet werden.

08

Optional: Integrationen

Für die Anbindung im SOC: Zugangsdaten zur Firewall (Sophos, Firewalla, pfSense) oder eine App-Registrierung in Microsoft Entra ID für Defender. Dazu ein Slack-Webhook für Alarme und ein Plan, wie die CyberTell-App auf die Geräte der Mitarbeiter kommt.

Bereit für den Start, wenn …

- [ ] der erste Admin feststeht und seine E-Mail-Adresse erreichbar ist
- [ ] security@ihre-domain.ch E-Mails empfängt
- [ ] der Zugang zur DNS-Verwaltung geklärt ist
- [ ] die SMTP-Zugangsdaten für Simulationen vorliegen
- [ ] die Mitarbeiterliste als CSV bereitliegt