CYBERTELL / CHECKLIST PER L'AVVIO DI CYBERTELL

Checklist per l'avvio di CyberTell

Cosa prepara la vostra azienda prima della configurazione. Con queste informazioni il setup si completa in una sola sessione.

Passo dopo passo · 8 passaggi

01 Designare un referente e il primo amministratore

Una persona che gestisce CyberTell per l'azienda: nome, cognome e un indirizzo e-mail aziendale personale. L'accesso avviene tramite link via e-mail e passkey, senza password.

02 Creare una casella security@

Creare una casella o un inoltro **security@vostro-dominio.ch** che riceva e-mail in modo affidabile e venga letta regolarmente. CyberTell invia lì la conferma del vostro dominio. L'indirizzo funge anche da punto di contatto per gli incidenti di sicurezza.

> ! Senza una casella security@ funzionante il dominio non può essere confermato.

03 Preparare dominio e DMARC

Stabilire il dominio principale dell'azienda e chiarire l'accesso alla gestione DNS. Per l'analisi DMARC, creare un record TXT su **_dmarc.vostro-dominio.ch** con CyberTell come destinatario dei report:

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

04 Invio e-mail per le simulazioni di phishing

Le e-mail di phishing simulate passano dal vostro server di posta. Tenere pronti: host SMTP, porta (di solito 587), utente, password, indirizzo e nome del mittente. Per il dominio mittente devono essere impostati SPF e DMARC; DKIM è consigliato.

05 Consentire le simulazioni nel filtro di posta

Affinché le e-mail di test arrivino, consentire nel filtro il vostro server SMTP e il dominio mittente: in Microsoft 365 tramite «Recapito avanzato» (simulazione di phishing), in Google Workspace tramite una lista di autorizzazione. Opzionale: un dominio di tracking proprio con record TXT **_cybertell-verify.vostro-dominio.ch** e un CNAME verso la destinazione indicata nel portale. Consentire anche questo dominio.

06 Elenco dei collaboratori in CSV

Tutti i collaboratori con nome, cognome e indirizzo e-mail aziendale, lingua opzionale (de, en, fr, it). Formato: punto e virgola come separatore, UTF-8, max. 2 MB. Ogni indirizzo e-mail deve essere univoco.

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

07

Profilo aziendale e ambiente IT

Logo, sito web e una breve descrizione dell'azienda. Per la prima valutazione dei rischi annotare: sistemi in uso (Windows, Active Directory, Microsoft 365, macOS, Linux), firewall e protezione degli endpoint, fornitori principali e dove vengono trattati i dati personali.

08

Opzionale: integrazioni

Per il collegamento al SOC: credenziali del firewall (Sophos, Firewalla, pfSense) o una registrazione app in Microsoft Entra ID per Defender. Inoltre un webhook Slack per gli avvisi e un piano per distribuire l'app CyberTell sui dispositivi dei collaboratori.

Pronti a partire quando …

- ☐ il primo amministratore è designato e il suo indirizzo e-mail funziona
- ☐ security@vostro-dominio.ch riceve e-mail
- ☐ l'accesso alla gestione DNS è chiarito
- ☐ le credenziali SMTP per le simulazioni sono disponibili
- ☐ l'elenco dei collaboratori è pronto in CSV