FÜR IT-VERANTWORTLICHE IN FIRMEN

Eine Plattform statt vieler.

CyberTell bündelt **Awareness, Security-Operations und Compliance** in einer Schweizer Plattform — für KMU ohne dedizierte Security-Stelle.

Die Ausgangslage

In vielen KMU läuft Sicherheit **nebenbei** — verteilt auf mehrere Werkzeuge, ohne dedizierte Stelle und ohne durchgängigen Nachweis. Awareness, Monitoring und Compliance laufen getrennt, und niemand führt die Ergebnisse zusammen.

16 %

der Sicherheitsverletzungen beginnen mit Phishing; bei **60 % ist ein Mensch beteiligt** — durch Klick, Fehler oder Social Engineering (Verizon, Data Breach Investigations Report 2025).

33,1 %

der Mitarbeiter klicken ohne Training auf eine simulierte Phishing-Mail; nach zwölf Monaten Training sind es 4,7 % — **Branchen-Benchmark, nicht unsere Messung** (KnowBe4, Phishing by Industry Benchmarking Report 2025).

108 Kontrollfragen

Der IKT-Minimalstandard des Bundes ist eine **Selbstbewertung in fünf Funktionen und 23 Kategorien**. CyberTell führt durch 108 Kontrollfragen, bewertet den Reifegrad von 0 bis 4 und hält Massnahmen und Nachweise fest.

Was das für die IT heisst: **eine einzige Konsole für Mensch, Technik und Nachweis** — weniger Werkzeuge zu pflegen, weniger Lücken zwischen den Systemen, Berichte und Nachweise als PDF.

WARUM AUS DER SCHWEIZ

Datenhoheit — Hosting in der Schweiz.

Schweizer Hosting, **verschlüsselt gespeichert**. Die Daten Ihrer Mitarbeiter und Systeme werden in der Schweiz gespeichert und unterliegen Schweizer Recht. Einzelne Funktionen (KI-Analyse, Leak-Abfragen, Zahlung, Push) laufen über die in der Datenschutzerklärung genannten Dienste, teils in den USA.

DREI DOMÄNEN – ÜBER 30 MODULE

Awareness · Human Layer

Der Mensch ist oft der Einstiegspunkt. CyberTell trainiert das Team und wertet jede Kampagne pro Person aus.

- Phishing-Simulationen — 17 Vorlagen plus KI-Generator
- Simulationen — Krisen-Dialoge mit KI-Gegenspieler
- 13 Online-Kurse mit Prüfung
- Tabletop-Übungen, per KI je Firma erstellt

Operations · Detection & Response

KI-gestützte Phishing-Analyse, regelmässiger Abgleich mit Leak-Datenbanken und ein klarer Ablauf für den Ernstfall — ohne eigene Security-Stelle.

- Phishing-Analyse & DMARC-Prüfung
- Dark-Web-Abgleich (HIBP, DeHashed, LeakCheck)
- Incident-Response & War Room
- Asset-Register mit Risk-Score

Compliance · Governance

Pflichten und Nachweise laufend gepflegt — als Berichte und PDF-Exporte statt einmaliger Selbstdeklaration.

- IKT-Minimalstandard & ISMS nach ISO-27001-Struktur
- DSG / DSGVO — VVT, TOMs, Verträge
- Lieferanten-Management
- Policy-Rollout & Nachweise

EINFÜHRUNG & BETRIEB

SaaS. Schweizer Betrieb.

Kein eigener Server nötig, optionale Desktop-Clients für Windows, macOS und Linux — zentral administriert. Auf Wunsch eigene Instanz oder On-Premises.

BEREITSTELLUNG
SaaS
Kein eigener Server · optionale Desktop-Clients · 30 Tage Test

HOSTING
Schweizer RZ
Hosting in der Schweiz, Auslieferung über Cloudflare

VERWALTUNG
Zentral
Eine Admin-Konsole für Mitarbeiter, Geräte & Nachweise