TANGORA // CYSEC

PRIVATE SECTOR OFFENSIVE AGENCY

OFFENSIVE SECURITY
RED TEAMING



HIER KÖNNTE IHRE FIRMA STEHEN

Wenn Ihr Unternehmen hier stehen würde,
wäre es Zeit, genauer hinzusehen.

IT-SICHERHEIT & PENTESTING

SCHWACHSTELLEN FINDEN. RISIKEN MINIMIEREN.
IHRE ZUKUNFT SCHÜTZEN.

TANGORA CYSEC GMBH

ILLUSTRATIVE RECREATION / NOT LIVE DATA

01 / ÜBERBLICK

IT-Sicherheit, die in Angriffswegen denkt.

Das Portfolio verbindet Pentesting, Red Teaming, Ransomware-Simulationen und Awareness. Der gemeinsame Nenner: technische Beobachtungen werden in Angriffspfade, Risiken und konkrete Entscheidungen übersetzt – nicht in Scanberichte.

TECHNISCHE TIEFE

PENTESTING

Black-, White- und Grey-Box-Tests für Webanwendungen, APIs, Infrastruktur und kombinierte Umgebungen. Jede Schwachstelle wird mit Beleg, Auswirkung und Priorität dokumentiert.

SIMULATION

RED TEAMING

Realistische, autorisierte Angriffssimulationen gegen Detection, Response und Resilienz. Die Frage ist nicht „gibt es eine Lücke?", sondern „wie weit kommt ein Angreifer – und merkt es jemand?"

RESILIENCE

RANSOMWARE

Kontrollierte Szenarien für Prävention, Alarmierung, Kommunikation und Wiederanlauf. Geübt wird der Ernstfall – bevor er eintritt.

HUMAN LAYER

AWARENESS

Security Awareness für Entwickler:innen und nicht-technische Teams entlang realer Situationen – statt Folien abzuhaken.

289,2 Mrd €

SCHADEN / JAHR

Datendiebstahl, Spionage und Sabotage in der deutschen Wirtschaft (Bitkom 2025)

87%

BETROFFENE FIRMEN

der deutschen Unternehmen waren in 12 Monaten betroffen

80%

KMU-ANTEIL

der beim BSI angezeigten Ransomware-Angriffe trafen kleine und mittlere Unternehmen

119

LÜCKEN / TAG

neu bekannt gewordene Schwachstellen pro Tag, +24 % zum Vorjahr (BSI 2025)

> „Ich denke nicht in Findings.
> Ich denke in Angriffswegen."
>
> MAXIMILIAN KRETSCHMER / OFFENSIVE SECURITY

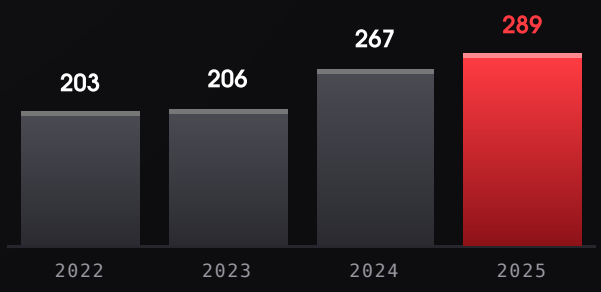
02 / BEDROHUNGSLAGE DEUTSCHLAND

Die Zahlen hinter dem Risiko.

Cyberangriffe sind für deutsche Unternehmen kein Randthema mehr, sondern die größte Einzelquelle wirtschaftlicher Schäden. Die Studien von Bitkom und BSI zeichnen seit Jahren dasselbe Bild – mit steigender Tendenz.

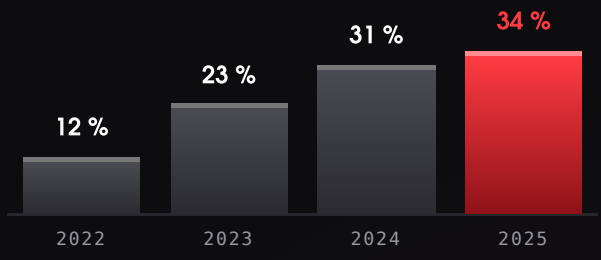
GESAMTSCHADEN DEUTSCHE WIRTSCHAFT

Diebstahl, Spionage, Sabotage – in Mrd. Euro pro Jahr (Bitkom Wirtschaftsschutz)



VON RANSOMWARE GESCHÄDIGT

Anteil der Unternehmen mit Ransomware-Schaden in den letzten 12 Monaten

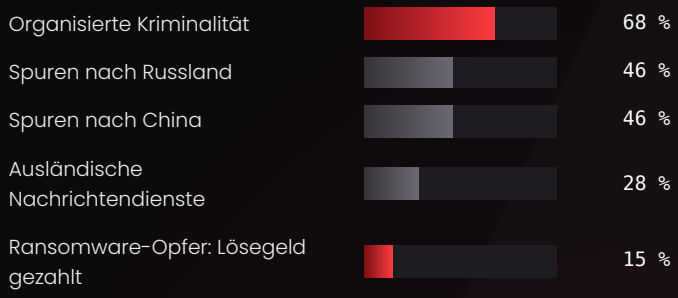


DAS DUNKELFELD BEI KMU

Das BSI zählt im Lagebericht 2025 rund **950 angezeigte Ransomware-Angriffe – etwa 80 % davon gegen kleine und mittlere Unternehmen**. Angezeigt wird nur ein Bruchteil: Viele Betriebe melden Vorfälle aus Sorge um Reputation und Kundenbeziehungen nicht. Expertenschätzungen gehen von einem Dunkelfeld **um das Zehnfache** aus.

Warum der Mittelstand? Angreifer wählen nach Aufwand und Ertrag: KMU sind zahlungsfähig, oft versichert, aber selten mit Security-Team, 24/7-Monitoring oder geübtem Notfallplan ausgestattet. Automatisierte Angriffe unterscheiden nicht zwischen 20 und 2.000 Mitarbeitenden.

WER GREIFT AN?



Der Anteil der Unternehmen, die staatliche Akteure als Täter nennen, hat sich seit 2023 vervierfacht. Kriminelle Gruppen und staatliche Auftraggeber arbeiten zunehmend Hand in Hand – gut finanziert, arbeitsteilig, professionell.

202,4 Mrd €
CYBER-ANTEIL
70 % des Gesamtschadens entfallen auf Cyberangriffe

950
ANGEZEIGT
Ransomware-Angriffe im BSI-Berichtszeitraum – Dunkelfeld ca. 10×

280 Tsd.
MALWARE / TAG
neue Schadprogrammvarianten pro Tag laut BSI

3×
SEIT 2022
Anteil der Ransomware-geschädigten Unternehmen fast verdreifacht

Quellen: Bitkom, Studie „Wirtschaftsschutz 2025" (Sept. 2025, n > 1.000 Unternehmen); BSI, „Die Lage der IT-Sicherheit in Deutschland 2025" (Nov. 2025, Berichtszeitraum Juli 2024 – Juni 2025). Zwischenwerte 2023/2024 gerundet aus den jeweiligen Vorjahresstudien.

03 / ANATOMIE EINES ANGRIFFS

So läuft ein Ransomware-Angriff wirklich ab.

Ransomware „passiert“ nicht plötzlich. Ein Angriff ist ein Projekt mit Phasen und Entscheidungspunkten – vom ersten Zugriff bis zur Verschlüsselung dauert es oft Tage bis Wochen. In jeder Phase gibt es Signale. Die Frage ist, ob jemand sie sieht.

PHASE 01 · TAG 0

Initial Access

Phishing-Mail, gestohlene Zugangsdaten aus Leaks, ungepatchter VPN-Zugang, exponiertes RDP – oder ein fertiger Zugang, gekauft bei „Initial Access Brokern“.

PHASE 02 · TAG 0–2

Persistenz & Rechteausweitung

Der Angreifer verankert sich, sammelt Passwörter, nutzt Fehlkonfigurationen im Active Directory und arbeitet sich zum Domänen-Admin vor.

PHASE 03 · TAG 2–14

Lateral Movement & Aufklärung

Bewegung von System zu System, Suche nach Backups, Fileservern, Buchhaltung, Kundendaten. Backups werden gezielt zerstört.

PHASE 04 · TAG 7–21

Datenexfiltration

Hunderte Gigabyte wandern unauffällig zu Cloud-Speichern – Druckmittel für die zweite Erpressung, falls Backups funktionieren.

PHASE 05 · TAG X, MEIST NACHTS / WOCHENENDE

Verschlüsselung

Innerhalb weniger Stunden werden Server, Clients und Hypervisoren verschlüsselt. Produktion, Logistik, E-Mail und Telefonie stehen still.

PHASE 06 · AB TAG X

Erpressung & Leak-Site

Lösegeldforderung, Countdown auf der Leak-Site, Anrufe bei Kunden und Presse. „Double Extortion“: zahlen für den Schlüssel – und nochmal fürs Schweigen.

PROFILE	LOCKBIT
MODELL	Ransomware-as-a-Service
AKTIV SEIT	2019 · v3.0 „Black“ ab 2022
ROLLEN	Kernteam + Affiliates
SPLIT	~80/20 Affiliate/Betreiber
OPFER	> 2.000 weltweit (US-DoJ)
LEAK-SITE	Tor · Countdown · Samples
TAKEDOWN	Op. Cronos, Feb. 2024
STATUS	Nachfolger weiter aktiv

LOCKBIT ALS LEHRSTÜCK

LockBit war über Jahre die aktivste Ransomware-Marke der Welt – nicht wegen genialer Technik, sondern wegen eines skalierbaren Geschäftsmodells: Das Kernteam liefert Verschlüsseler, Leak-Site und Verhandlungsportal; hunderte „Affiliates“ übernehmen den Einbruch und behalten den Großteil des Lösegelds.

Die Leak-Site zeigte, wie Datenexfiltration und Verschlüsselung mit Veröffentlichungsdruck kombiniert werden. Im Februar 2024 übernahmen Ermittler im Rahmen von **Operation Cronos** Teile der Infrastruktur. Das Ökosystem hat sich neu sortiert – das Geschäftsmodell ist geblieben.

DOUBLE EXTORTION · RAAS · AFFILIATE-MODELL · LEAK-SITE · INITIAL ACCESS BROKER

FAZIT 01

Jede Phase ist eine Chance. Zwischen Erstzugriff und Verschlüsselung liegen Tage. Wer die Signale erkennt, unterbricht die Kette.

FAZIT 02

Backups allein reichen nicht. Erst stehlen, dann verschlüsseln: Ein Backup verhindert den Stillstand – nicht die Veröffentlichung.

FAZIT 03

Der Weg ist bekannt. Genau diese Kette prüft ein Pentest oder Red-Team-Einsatz kontrolliert – bevor es jemand anderes unkontrolliert tut.

04 / SCHADEN IM ERNSTFALL

Was ein Vorfall wirklich kostet.

Das Lösegeld ist meist der kleinste Posten. Die eigentlichen Kosten entstehen durch Stillstand, Wiederaufbau, Meldepflichten, verlorene Aufträge – und durch Wochen, in denen die Geschäftsführung nichts anderes mehr tut.

KOSTENBLÖCKE EINES RANSOMWARE-VORFALLS

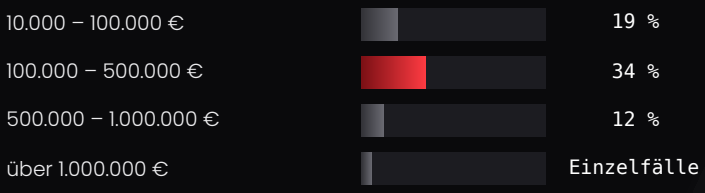
Typische Verteilung bei mittelständischen Unternehmen (Erfahrungswerte, indikativ)



- Betriebsstillstand / Umsatzausfall ~35 %
- Wiederherstellung, Forensik, IT-Neuaufbau ~25 %
- Recht, DSGVO-Meldung, Bußgeldrisiko ~15 %
- Kundenverlust, Reputation, Vertragsstrafen ~15 %
- Lösegeld (falls gezahlt) ~10 %

GEZAHLTE LÖSEGELDER IN DEUTSCHLAND

Anteil der Unternehmen, die auf Forderungen eingegangen sind, nach Höhe (Bitkom 2025)



BSI und BKA raten von Zahlungen ausdrücklich ab: Wer zahlt, finanziert den nächsten Angriff – häufig auf das eigene Unternehmen – und hat keine Garantie auf funktionierende Entschlüsselung oder Löschung gestohlener Daten.

~21
TAGE AUSFALL
durchschnittliche Betriebsunterbrechung nach Ransomware, Erfahrungswert aus IR-Einsätzen

72 h
DSGVO-FRIST
Meldung an die Aufsichtsbehörde bei Verlust personenbezogener Daten (Art. 33)

24 h
NIS2-ERSTMELDUNG
Frühwarnung für betroffene Einrichtungen nach dem NIS2-Umsetzungsgesetz

2×
ERPRESSUNG
Schlüssel und Nicht-Veröffentlichung werden getrennt „verkauft"

KRITISCHE FOLGEN FÜR UNTERNEHMEN

- **Produktion & Lieferfähigkeit:** Maschinen, ERP und Logistik stehen; Kunden wechseln zum Wettbewerber, Vertragsstrafen greifen.
- **Liquidität:** Rechnungen können weder gestellt noch bezahlt werden; Löhne und Lieferanten warten – bei KMU existenzbedrohend.
- **Haftung der Geschäftsführung:** Fehlende Vorsorge kann als Organisationsverschulden gewertet werden; Versicherer prüfen die Obliegenheiten genau.
- **Datenabfluss:** Verträge, Kalkulationen, Personaldaten und Kundendaten auf einer Leak-Site – dauerhaft, unwiderruflich.
- **Nachwirkungen:** Monate Neuaufbau, Audits, verlorene Zertifizierungen, erschwerter Versicherungsschutz.

RECHNUNG

PRÄVENTION VS. VORFALL

Ein fokussierter Pentest oder eine Ransomware-Simulation kostet einen Bruchteil eines einzigen Ausfalltages. Selbst bei konservativer Annahme – ein Vorfall in fünf Jahren, Schaden im mittleren sechsstelligen Bereich – rechnet sich regelmäßiges Testen um ein Vielfaches.

Wichtiger als die Rechnung ist die Entscheidung: **Welche Angriffspfade sollen es nach dem Projekt nicht mehr geben?**

Quellen: Bitkom Wirtschaftsschutz 2025; BSI Lagebericht 2025; DSGVO Art. 33; NIS2-Umsetzungsgesetz (in Kraft seit Dez. 2025). Kostenverteilung und Ausfalldauer sind Erfahrungswerte aus Incident-Response-Praxis und branchenüblichen Auswertungen, keine amtliche Statistik.

05 / PENTESTING

Technisch tief. Praktisch verwertbar.

Ein Penetrationstest beantwortet eine konkrete Frage: Welche Schwachstellen hat diese Anwendung, diese API, dieses Netzwerk – und was kann ein Angreifer damit anfangen? Das Ergebnis sind belegte Findings, verkettete Angriffspfade und eine Priorisierung, mit der Ihr Team sofort arbeiten kann.

01
DISCOVER
Assets, Dienste, Schnittstellen, Angriffsfläche erfassen

02
MAP
Vertrauensbeziehungen, Rollen, Berechtigungen abbilden

03
VALIDATE
Schwachstellen manuell verifizieren und verketten

04
PRIORITIZE
Eintrittswahrscheinlichkeit × Auswirkung bewerten

05
REPORT
Beleg, Angriffspfad, Entscheidung, Maßnahme

06
RETEST
Gleiche Frage, neue Antwort: Ist der Pfad wirklich zu?

TEST MODE
BLACK BOX
Angreiferperspektive. Ohne Vorwissen, wie ein externer Angreifer. Zeigt, was von außen tatsächlich erreichbar und ausnutzbar ist.

TEST MODE
GREY BOX
Realistisch und fokussiert. Ausgewählter Kontext – Testaccounts, Architekturskizze – verbindet Effizienz mit Tiefe. Der häufigste Modus.

TEST MODE
WHITE BOX
Maximale Tiefe. Mit Quellcode, Konfiguration und Architektur. Findet Logikfehler, die von außen unsichtbar bleiben.

PRÜFUMFANG

BEREICH	TYPISCHE FRAGEN
Webanwendungen	Auth, Session, Injection, Zugriffskontrolle, Business-Logik – OWASP Top 10 und darüber hinaus
APIs	Objekt- und Funktionsberechtigungen, Massenabfragen, Token-Handling, Rate Limits
Infrastruktur / AD	Exponierte Dienste, Patchstand, Kerberos, Delegationen, Pfade zum Domänen-Admin
Cloud / M365	Identitäten, Conditional Access, Fehlkonfigurationen, öffentlich erreichbare Speicher
Kombiniert	Wie greifen Web, Identität und Netzwerk ineinander? Wo wird aus „mittel" „kritisch"?

DELIVERABLES

DELIVERY
TECHNISCHER BERICHT
Findings mit Reproduktionsschritten, Beleg, Auswirkung, CVSS-Einordnung und Empfehlung.

DELIVERY
ANGRIFFSPFAD
Mehrere Schwachstellen als Kette – vom Einstieg bis zur Wirkung.

DELIVERY
MANAGEMENT SUMMARY
Die wichtigsten Risiken und Entscheidungen auf einer Seite – für die Geschäftsführung.

DELIVERY
RETEST
Prüfung, ob Schwachstelle oder Kette tatsächlich geschlossen wurden – nicht nur das Ticket.

06 / RED TEAMING

Angreiferlogik gegen Verteidigungslogik.

Ein Red-Team-Einsatz untersucht nicht, ob ein einzelner Fehler existiert. Er prüft Kombinationen aus Exposure, Identität, Vertrauen und Detection – und fragt, wie weit ein kompromittierter Pfad in Ihrer Organisation führen könnte, bevor jemand eingreift.

```
mk://       red-team-operation · CONTROLLED · AUTHORIZED
MISSION     Detection + Response unter realistischen Bedingungen testen
BOUNDARY    customer-owned / schriftlich autorisiert / Rules of Engagement
PHASES      recon → access → identity → path → objective → detection → debrief
QUESTION    Kann die Organisation den Pfad beobachten, verstehen und eingrenzen?
OUTPUT      Attack Narrative / Detection-Lücken / Response-Timeline / Remediation
```

ATTACK PATH
SURFACE
Welche Angriffsfläche ist außen und innen relevant – technisch wie menschlich?

ATTACK PATH
IDENTITY
Wo entstehen privilegierte Beziehungen, die ein Angreifer übernehmen kann?

ATTACK PATH
DETECTION
Welche Signale existieren – und werden sie rechtzeitig gesehen und verstanden?

ATTACK PATH
RESILIENCE
Wie schnell kann die Organisation einen Angriff eingrenzen und den Betrieb halten?

PENTEST ODER RED TEAM?

	PENTEST	RED TEAM
Frage	Welche Lücken hat System X?	Erreicht ein Angreifer Ziel Y – unbemerkt?
Umfang	Definierte Systeme, breit	Ganze Organisation, zielorientiert
Prüft	Technik	Technik, Mensch, Prozess, Detection
Dauer / Reife	Tage; Basis, regelmäßig	Wochen; für Teams mit SOC / MDR

WARUM BEIDES WICHTIG IST

Pentests schließen Türen. Red Teaming prüft, ob jemand merkt, wenn eine trotzdem aufgeht. Zusammen beantworten sie die Frage von Geschäftsführung und Versicherern: **Sind wir vorbereitet – und woher wissen wir das?**

Ransomware-Gruppen arbeiten genau entlang dieser Kette. Wer sie kontrolliert durchspielt, kennt seine schwächsten Glieder, bevor ein Affiliate sie findet.

MESSBARE KPIS NACH DEM EINSATZ

MTTD
TIME TO DETECT
Wie lange bis zur ersten Alarmierung?

MTTR
TIME TO RESPOND
Wie lange bis zur Eingrenzung des Pfads?

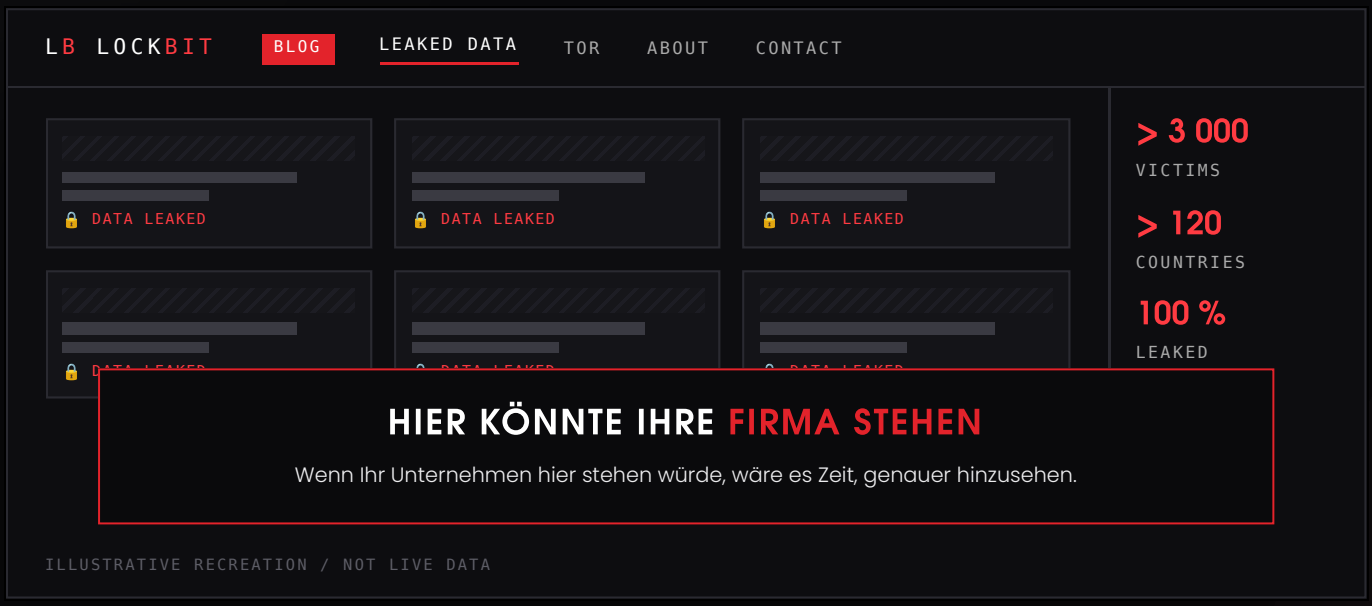
PATHS
ANGRIFFSPFADE
Gefunden / geschlossen / im Retest bestätigt

COV
DETECTION COVERAGE
Anteil der Techniken, die Signale erzeugt haben

07 / RANSOMWARE-SIMULATION

Was passiert, wenn die Grenze versagt?

Ransomware-Simulationen sind kontrollierte Szenarien. Geprüft werden nicht nur technische Schutzmechanismen, sondern Alarmierung, Kommunikation, Entscheidungswege, Abhängigkeiten und Wiederanlauf – alles, was im Ernstfall über Tage oder Wochen entscheidet.



WAS SIMULIERT WIRD

- **Technik:** Erkennt EDR/AV die Vorbereitung? Wird Massen-Verschlüsselung gestoppt? Sind Backups erreichbar – auch für den Angreifer?
- **Alarmierung:** Wer wird wann informiert – nachts, am Wochenende? Funktionieren Telefonketten, wenn E-Mail und Teams weg sind?
- **Entscheidung:** Wer darf Systeme abschalten? Wer spricht mit Versicherung, Anwalt, Behörde, Presse? Wird verhandelt?
- **Wiederanlauf:** Welche Systeme zuerst? Wie lange dauert Restore wirklich? Was ist der manuelle Notbetrieb?

FORMATE

FORMAT A

TABLETOP

Halbtägige Übung mit Geschäftsführung, IT und Fachbereichen entlang eines realistischen Szenarios. Kein Risiko für den Betrieb.

FORMAT B

TECHNISCHE SIMULATION

Kontrollierte Ausführung von Ransomware-Techniken in abgestimmter Umgebung – ohne echte Verschlüsselung, mit echten Erkenntnissen.

HIER KÖNNTE IHRE FIRMA STEHEN

Der Witz funktioniert am besten, wenn Sie dort NICHT stehen.

Security testen, bevor fremde Leute Ihre Angriffsgeschichte erzählen.

08 / AWARENESS

Security Awareness ohne Security-Theater.

Awareness soll Menschen in realen Situationen handlungsfähig machen: erkennen, innehalten, verifizieren, melden. Nicht, weil Mitarbeitende das „schwächste Glied" sind – sondern weil sie der erste Sensor sind, den ein Angreifer auslöst.

DEV / APPSEC

DEVELOPERS

Threat-aware Development: Secrets, Dependencies, Identity, Input-Handling und die Angriffsmuster, die in echten Pentests immer wieder auftauchen – am eigenen Code erklärt.

HUMAN / REPORT

EMPLOYEES

Social Engineering, verdächtige Anfragen, Identitätsdruck („der Chef braucht das sofort"), ungewöhnliche MFA-Prompts, QR-Phishing. Ziel: melden ohne Angst vor Fehlern.

RISK / DECISION

LEADERS

Cyberrisiko organisatorisch einordnen, Haftung verstehen, Entscheidungen für Resilienz treffen – inklusive der Frage, was ein Ausfalltag wirklich kostet.

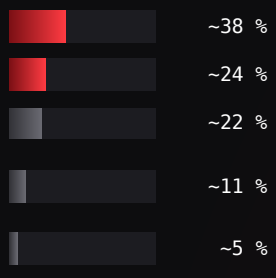
SOC / IR

SECURITY TEAMS

Von Awareness zu Detection: Was sieht das Team, wenn ein Angreifer Phase 2 erreicht? Übergang von Meldung zu Triage, Reporting und Response.

WO ANGRIFFE BEGINNEN

Häufige Einstiegsvektoren bei Ransomware-Vorfällen (indikativ, gerundet)



Mehr als die Hälfte der Vorfälle beginnt beim Menschen – mit einer Mail, einem Anruf oder einem wiederverwendeten Passwort.

WIE EIN PROGRAMM AUSSIEHT

- ☐ **Kick-off-Workshop** je Zielgruppe, 2–4 Stunden, an echten Beispielen aus Pentests und Vorfällen.
- ☐ **Kontrollierte Phishing-Kampagnen** mit Auswertung nach Klick-, Eingabe- und Meldequote – ohne Bloßstellung Einzelner.
- ☐ **Meldeweg testen:** Kommt eine Meldung in unter 10 Minuten bei der richtigen Stelle an?
- ☐ **Quartalsweise Kurzformate** zu aktuellen Maschen: Deepfake-Anrufe, MFA-Fatigue, QR-Codes, gefälschte Lieferantenrechnungen.

Meldequote
KPI 01
Anteil gemeldeter Test-Phishings – der wichtigste Wert

Time to Report
KPI 02
Minuten von Zustellung bis erster Meldung

> Menschen müssen nicht Hacking lernen.
> Sie müssen gute Entscheidungen treffen können.

09 / RESEARCH & NACHWEIS

Öffentliche Security-Arbeit mit nachvollziehbaren Quellen.

Offensive Security lebt von Nachweisbarkeit. Die hier ausgewiesenen Anerkennungen stammen aus öffentlichen Responsible-Disclosure- und Hall-of-Fame-Programmen und sind an der Originalquelle überprüfbar.

PUBLIC / EVIDENCE

BUNDESWEHR / VDPBW

9 gemeldete Schwachstellen auf der offiziellen Danksagungsseite des Vulnerability Disclosure Programms der Bundeswehr.

PUBLIC / EVIDENCE

EUROPÄISCHE UNION

Anerkennung im Rahmen des EU-Programms für die koordinierte Meldung von Schwachstellen in Institutionen der Union.

PUBLIC / EVIDENCE

DEUTSCHE TELEKOM

Hall-of-Fame-Anerkennung im öffentlichen Bug-Bounty- / Responsible-Disclosure-Programm der Deutschen Telekom.

PUBLIC / EVIDENCE

HEISE

Öffentlich ausgewiesenes Finding mit Hall-of-Fame-Eintrag beim Heise-Verlag.

METHODE

01
EVIDENCE
Jede Aussage hat einen reproduzierbaren Beleg – Screenshot, Request, Log.

02
ATTACK PATH
Einzelfunde werden zur Kette: Was wird aus „mittel" in Kombination?

03
DECISION
Welche Entscheidung muss die Organisation jetzt treffen – und welche nicht?

04
REMEDIATION
Konkrete, priorisierte Maßnahmen, abgestimmt mit dem umsetzenden Team.

05
RETEST
Dieselbe Frage nochmal stellen. Nur ein bestätigter Fix ist ein Fix.

GRUNDSÄTZE

- ☐ **Autorisierung zuerst.** Kein Test ohne schriftliche Freigabe, klaren Scope und Rules of Engagement.
- ☐ **Keine Kollateralschäden.** Produktivsysteme werden nicht gefährdet; kritische Aktionen nur nach Rückfrage.
- ☐ **Vertraulichkeit.** Ergebnisse gehören dem Auftraggeber. Kommunikation auf Wunsch verschlüsselt (PGP / Threema).
- ☐ **Primärquellen.** Technische Aussagen werden mit offiziellen Programmen oder Originaldokumenten belegt.

PORTFOLIO	tangora.io
SEKTIONEN	Pentesting / Red Teaming / Research / Awareness / Contact
LOCKBIT	Europol / NCA – Operation Cronos (Feb. 2024)
LEAK-SITE	öffentliche Dokumentation der LockBit-3.0-Site (PCrisk u. a.)
STATISTIK	Bitkom Wirtschaftsschutz 2025 · BSI Lagebericht 2025
RECHT	DSGVO Art. 33 · NIS2-Umsetzungsgesetz

10 / PROJEKTANFRAGE

Nicht noch ein Scanbericht. Eine belastbare Antwort.

Ein gutes Erstgespräch beginnt mit der Frage hinter dem Auftrag: Welche Umgebung? Welches Ziel? Welche Autorisierung? Und welche Entscheidung soll nach dem Projekt klarer sein als davor?

SO LÄUFT EIN PROJEKT

SCHRITT 01
Erstgespräch (kostenfrei)
30–45 Minuten. Ziel, Umgebung, Reifegrad, Zeitfenster. Ergebnis: ein Vorschlag, welches Format tatsächlich passt.

SCHRITT 02
Scope & Autorisierung
Schriftliche Freigabe, Systeme, Ausschlüsse, Notfallkontakte, Rules of Engagement.

SCHRITT 03
Durchführung
Laufende Abstimmung. Kritische Funde werden sofort gemeldet – nicht erst im Bericht.

SCHRITT 04
Bericht & Debrief
Technischer Bericht, Management Summary, gemeinsamer Termin mit IT und Geschäftsführung.

SCHRITT 05
Retest
Nach Umsetzung: Sind die Pfade wirklich zu? Erst dann ist das Projekt abgeschlossen.

CHECKLISTE FÜR IHRE ANFRAGE

- ☐ Welche Systeme / Anwendungen sollen geprüft werden – oder welches Ziel soll ein Angreifer nicht erreichen?
- ☐ Gibt es Vorgaben von Kunden, Versicherung, NIS2, ISO 27001, TISAX?
- ☐ Gab es bereits Tests oder Vorfälle?
- ☐ Wer entscheidet, wer setzt um, wer ist im Notfall erreichbar?
- ☐ Wann muss das Ergebnis vorliegen?

KONTAKT

TANGORA CYSEC GMBH

Maximilian Kretschmer / Offensive Security

MAIL kontakt@maximiliankretschmer.de
THREEMA ID ZANKU3VH
PGP 857A 126D 1E03 9D55 D1E6 AFE6 9BC4 E6F1 6D35 83C6
WEB tangora.io
ORT Hamburg / Deutschland

RED TEAMING · PENTESTING · RANSOMWARE-SIMULATIONEN · AWARENESS

SICHERHEIT IST EIN ZUSAMMENSPIEL AUS TECHNIK, MENSCH UND PROZESS.

Testen Sie es, bevor es jemand anderes tut.