B² CyberSec
IT SECURITY SOLUTIONS & SERVICES

# Beauftragen Sie Hacker, bevor es Kriminelle tun

Penetrationstests, die aus „Wir glauben, wir seien sicher“ handfeste Nachweise machen — Nachweise, die Sie Ihrem Vorstand vorlegen können.

# Warum diese Broschüre existiert

Weil ein grünes Dashboard keinen roten Alarm verhindert.

Wer je die Kluft gespürt hat zwischen „Alles okay“ im Report und „Wir wurden gehackt“ in der Schlagzeile, weiß: Beruhigende Zahlen sind keine Sicherheit.

Wir zeigen, wie Angreifer tatsächlich eindringen würden – und helfen, diese Wege sofort zu verschließen.

Fazit: Nicht mehr Lärm, sondern ein unabhängiger Test mit echten Beweisen und einem klaren handllings Plan. Wir liefen beides.

# Was ein Penetration Test wirklich ist (ohne Blabla)

Es ist ein legaler, kontrollierter Einbruch.

Wir handeln wie die Angreifer, nur ohne die negativen Folgen.

Menschliche Tester (nicht nur automatische Scanner) verketten kleine Schwachstellen zu realen Angriffspfaden über Identitäten, Anwendungen, Netzwerke, APIs, Cloud und WLAN.

Sie bekommen handfeste Beweise, priorisierte Handlungsempfehlungen und einen umsetzbaren Plan für Ihr Team.

Wenn Angreifer es können, simulieren wir es. Finden wir es, beheben Sie es.

# Warum B2CyberSec (und nicht die anderen zehn, die Sie heute gesehen haben)

| 01 | 02 | 03 | 04 |
|---|---|---|---|
| Unabhängig vom Design. | Wir verkaufen die von uns getesteten Tools nicht. | Wir korrigieren unsere Hausaufgaben nicht selbst. | Glaubwürdigkeit gegenüber Dritten, die Sie bei Audits verteidigen können. |

Senior-geführte, ergebnisorientierte Teams. Kleine Expertenteams, hands-on vom Scoping bis zum Re-Test. Sie wissen immer, wer die Arbeit macht und wie wir Fortschritt messen.

Angriff-informierte Verteidigung. Echte Angreifer-Taktiken, keine reinen Scans. Wir zeigen, was für Ihr Geschäft wirklich zählt, nicht hunderte irrelevante CVEs.

Vorstands-taugliche Klarheit. Berichte in Klartext, Risikobewertung, Angriffspfad-Visualisierungen sowie Kosten-/Aufwand-Abschätzung.

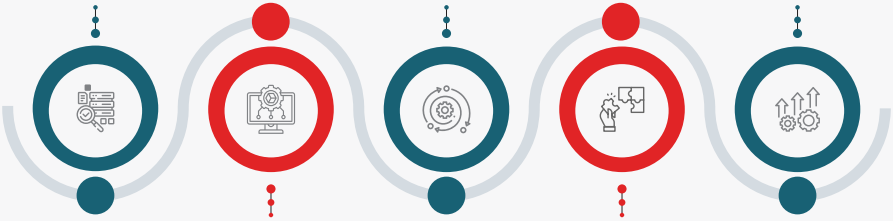
Compliance ohne Kopfschmerzen. Ergebnisse werden auf ISO 27001, NIS2, DORA, PCI DSS abgebildet. Mit echten Nachweisen, die Sie nutzen können. Zusammenarbeit mit Ihrem Team & Partnern, optionaler RenTest zur Beweisführung.

# Der PenTest in 5 Schritten

**Entdeckung und Umfang–** Keine Standardlösung. Wir stimmen Ziele, Assets, Rahmenbedingungen und Regeln des Tests auf Ihre Geschäftsfragen ab.

**Wirkungsorientierte Berichterstattung –** CVE-/CVSS Mapping, Angriffspfad ,Visualisierungen und ein 90-TagenPlan (Quick Wins + strukturelle Maßnahmen).

**Überprüfen und verbessern –** Optionaler Re-Test und Management Debrief. Beweise, keine Versprechen.



**Bedrohungsgesteuerte Simulation –** Freundliche Angreifer, echte Taktiken. Wir verketten Schwachstellen über Ihre gesamte Umgebung. Kritische Probleme melden wir sofort.

**Geführte Sanierung –** Wir setzen uns mit Ihrem Team zusammen, damit schnelle Fixes gelingen – ohne dass der Betrieb gestört wird.

# Was Sie bekommen

- Sie bekommen nicht nur ein Dokument, Sie gehen mit echtem Vertrauen.
- Klare Sicht darauf, wo Sie stark sind und wo Sie verwundbar sind.
- Echten Schutz, weil Maßnahmen priorisiert und praktisch sind.
- Kontrolle, weil Sie wissen, was als Nächstes zu tun ist – und Nachweise, weil jeder Schritt dokumentiert wird.
- Kurz: Weniger Rätselraten, mehr Sicherheit; weniger Überraschungen, mehr Resilienz.

**Sie erhalten außerdem:**

- Executive Summary & Risikoscore (nachvollziehbar Vorher/Nachher bei Re-Test)
- Technische Findings & Proof of Exploitation (Screenshots, Logs, PoCs)
- Priorisierter Maßnahmenplan (wer/was/wann, Aufwand vs. Wirkung)
- Compliance Mapping (ISO/NIS2/DORA/PCI DSS)
- Optionaler Re-Test Report zur Bestätigung der Schließung

# Faszinationen Lesen Sie das und sehen Sie, ob Sie danach wirklich keinen Test buchen wollen.

Die sieben „höflichen Türen“, die Angreifer im Mittelstand lieben – und warum sie auf Dashboards unsichtbar sind.

Die eine Fehlkonfiguration, mit der ein Tester von der MarketingnSeite zur Gehaltsabrechnung in drei Klicks springt.

Warum „starke Passwörter“ immer noch scheitern (und was wir stattdessen ausnutzen).

Wie ein flaches Netzwerk und ein ServicenAccount aus einem Laptop das ganze Unternehmen machen.

Der saubere, compliancenkonforme Weg, unabhängige Tests nachzuweisen – ohne mit Ihrem MSP zu streiten.

# Warum Sie den Unterschied spüren (Psychologie trifft Sicherheit)

**Verlustangst, kontrolliert.**
Wir zeigen Ihnen, wie Geld, IP und Vertrauen verloren gehen könnten – und geben Ihnen die Lösung.

**Gewinnstreben, legitim.**
Weniger Risiko, schnellere Audits, schnellere Deals – weil Sicherheit kein Fragezeichen mehr ist.

**Komfort & Klarheit.**
Ein Dokument, mit dem CFO, CTO und CISO arbeiten können.

**Anerkennung & Status.**
Sicherheit, die Sie beweisen können, überzeugt Partner, Kunden und Aufsichtsbehörden.

# Häufige Einwände (schnell erledigt)

***„Wir haben schon Tools."***

Angreifer auch. Unsere Aufgabe ist es zu zeigen, wie sie kleine Lücken verketten, die Ihre Tools übersehen.

***„Wir haben ein Audit bestanden."***

Audits prüfen meistens Abläufe. Angreifer nutzen andere Wege. Wir finden die und machen sie unwiederbringlich dicht.

***„Wir können keine Ausfälle riskieren."***

Darum testen wir sicher, mit klar definierten Spielregeln und Echtzeit-Kommunikation, sobald ein kritischer Fall auftritt.

***„Unser MSP kann das."***

Nein. Tests müssen unabhängig sein, um glaubwürdig zu sein.Wir kooperieren mit MSPs aber MSPs können niemals eigene Arbeit selbst kontrolieren.

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

# Beweise, die Sie auditieren können

Unsere Praktiker halten Zertifizierungen wie CRTO, SWIFT CSP Assessor, Burp Suite Certified Practitioner, eCCPT, eJPT, CPSA, CEH, CHFI, OSCP, OSMR, PNPT. Unsere Methoden richten sich nach OWASP und NIST; Ergebnisse werden auf ISO/NIS2/DORA/PCI DSS abgebildet

# Zwei Wege von hier

## Pfad A: Nichts tun.

Hoffen, dass die grünen Lichter grün bleiben. Akzeptieren, dass Sie vielleicht erst durch eine Lösegeldforderung von einer Lücke erfahren.

## Pfad B: Den Angriff simulieren.

Wissen, wo Sie verwundbar sind, beheben Sie das Wichtige und gehen Sie mit Nachweisen in Ihr nächstes Audit (oder Board Meeting).

## Wählen Sie B.

Wir gehen den Weg gemeinsam.

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

# Starten Sie hier:
# 30 Minuten austausch, null Verpflichtung.

Buchen Sie ein kostenloses 30-minütiges Cyber Risiko Assessment.

Wir stellen gezielte Fragen zu Ihrer Umgebung, skizzieren wahrscheinliche Angriffspfade undempfehlen den passenden Umfang für Ihren PenTest.

Kein Druck. Nur Klarheit und ein Plan.


info@b2cybersec.com

+49 (0) 821 90 789 500

Werner-von-Siemens-Str. 6
86159 Augsburg, Deutschland

www.b2cybersec.com


book free 30min call

b2cybersec.com

*Wichtiger Hinweis: Wir limitieren die Anzahl der PenTests pro Monat, damit SeniornExperten bei jedem Auftrag eingebunden sind.*

Wenn Ihr Zeitplan eng ist, buchen Sie jetzt Ihren Termin.