B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

Hire Hackers Before Criminals Do

Penetration Testing that turns “we think we’re secure” into proof you can show your board.

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

Why this brochure exists

Because green dashboards don't stop red-handed attackers.

If you've ever felt that uneasy gap between reports that say OK and a headline that says breached, this is for you.

We reveal exactly how attackers would get in, then help you close the door. Fast.

Bottom line: you don't need more noise. You need an independent test that produces evidence and a plan. We do both.

What a Penetration Test really is (No Fluff)

It's a legal, controlled break-in.

We act like the bad guys, without the bad outcomes. Human testers (not just scanners chain small weaknesses into real-world attack paths across identities, apps, networks, APIs cloud and Wi-Fi. You get proof, priorities, and a 90-day action plan your team can execute.

If attackers can do it, we simulate it. If we find it, you can fix it.

Why B2CyberSec (and not the other ten you've seen today)

01	02	03	04
Independent by design.	We don't sell the tools we test.	We don't mark our own homework.	Third-party credibility you can defend in audits.

Senior-led, outcome-driven. Small expert teams, hands-on from scoping to re-test. You always know who's doing the work—and how we measure progress.

Offense-informed defense. Real attacker tactics, not just automated scans. We surface what matters to your business, not a hundred low-value CVEs.

Board-ready clarity. Plain-English summaries, risk scoring, attack-path visuals, and cost/effort guidance.

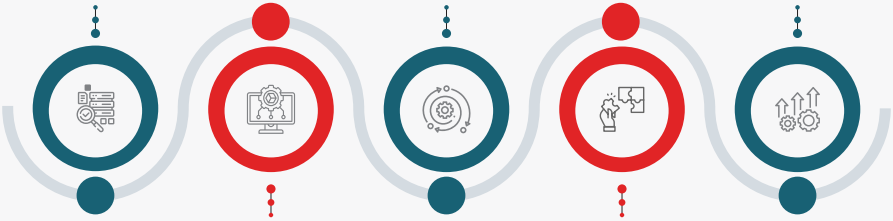
Compliance without the headache. Findings mapped to ISO 27001, NIS2, DORA, PCI DSS, evidence you'll actually use. Action to closure. Working sessions with your team and partners. Optional re-test to prove fixes.

The PenTest in 5 moves

Discovery & Scoping – No cookie-cutter. We align goals, assets, constraints, and rules of engagement to answer your business question.

Impact-Focused Reporting – CVE/ CVSS mapping, attack-path visuals, and a 90-day plan (quick wins + structural fixes).

Verify & Improve – Optional re-test and management debrief. Proof, not promises.



Threat-Led Simulation – Friendly attackers; real tactics. We chain weaknesses across your stack. Critical issues are flagged immediately.

Guided Remediation – We sit with your teams to land fixes fast, without breaking operations.

What you get

- You don't just get a document, you leave with confidence.
- Clear visibility into where you're strong and where you're exposed.
- Real protection because fixes are prioritized and practical.
- Control because you know what to do next, and proof because every step is documented for boards and auditors.
- In short: less guesswork, more certainty; fewer surprises, more resilience.

You also get:

- Executive Summary & Risk Score (board-ready; before/after if re-test)
- Technical Findings & Proof of Exploitation (screenshots, logs, PoC where applicable)
- Prioritized Remediation Plan (who/what/when, effort vs. impact)
- Compliance Mapping (ISO/NIS2/DORA/PCI DSS)
- Optional Re-Test Report confirming closure

Fascinations (Read these and try not to Book a Test)

The seven *"polite doors"* attackers love in mid-sized finance and how they look invisible on your dashboards.

The one misconfiguration that lets a tester jump from your marketing site to payroll in three clicks.

Why *"strong passwords"* still fail (and what we actually exploit instead).

How a flat network and a helpful service account turn one laptop into your whole company.

The clean, compliant way to prove independence of testing without fighting your MSP.

Why you'll feel the difference (Psychology meets Security)

Fear of loss, controlled.
We show you the real ways money, IP, and trust could drain away, then give you the fix.

Greed for gain, legit.
Lower exposure, smoother audits, faster deals because security isn't a question mark anymore.

Comfort & clarity.
One document your CFO, CTO, and CISO can all act on.

Approval & status.
Security you can demonstrate wins partners, customers, and regulators.

Common Objections (killed quickly)

"We already have tools."

Great! So do attackers. Our job is to show how they chain small gaps your tools miss.

"We passed an audit."

Audits check process. Attackers exploit paths. We map those paths and close them.

"We can't risk downtime."

We test safely, under clear rules of engagement, with real-time comms for criticals.

"Our MSP can do this."

Testing must be independent to be credible. We collaborate with MSPs; we don't test our own work.

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

Proof you can audit

Our practitioners hold certifications including CRTO, SWIFT CSP Assessor, Burp Suite Certified Practitioner, eCCPT, eJPT, CPSA, CEH, CHFI, OSCP, OSMR, PNPT. Methods align with OWASP and NIST; results map to ISO/NIS2/DORA/PCI DSS requirements.

Two paths from here

Path A: Do nothing.

Hope the green lights stay green. Accept that the first time you learn about a gap may be in a ransom note.

Path B: Simulate the attack.

Know where you're exposed, fix what matters, and walk into your next audit (or board meeting) with evidence.

Choose B.

We walk the path together

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

Start Here: 30 Minutes, zero obligation

Book a free 30-minute cyber risk assessment call.

We'll ask targeted questions about your environment, outline likely attack paths, and recommend the right scope for your PenTest.

No pressure. Just clarity and a plan.

info@b2cybersec.com

+49 (0) 821 90 789 500

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

www.b2cybersec.com

book free 30min call

b2cybersec.com

Quality over quantity: we limit the number of PenTests we run each month to keep senior experts on every engagement.

If your timeline is tight, book your slot now.