



plenum.red



CIO Advisory

# Offensive Sicherheit

Echte Angriffe, echte Erkenntnisse,  
nachhaltige Resilienz



# Warum Offensive Security heute unverzichtbar ist

Cyberrisiken sind das größte Geschäftsrisiko und gleichzeitig stark unterschätzt

**289 Mrd.**

Schaden entstand für deutsche Unternehmen in 2025.<sup>1</sup>

**11 Mrd.**

Investitionen in Cybersicherheit von deutschen Unternehmen in 2025.<sup>2</sup>

**34%**

der deutschen Unternehmen wurden 2025 Opfer von Ransomware, die Schäden verursacht hat.<sup>1</sup>

**#1 Risiko**

Cybervorfälle gelten als Top 1-Geschäftsrisiko in Deutschland 2025.<sup>3</sup>

## Regulatorische Rahmenbedingungen als Katalysator für nachhaltige Sicherheit

Mit der Umsetzung der EU-Richtlinie **NIS-2** wird der Kreis der betroffenen Unternehmen in Deutschland deutlich erweitert, Schätzungen zufolge um rund **30.000 Organisationen**. Diese Unternehmen sind künftig gefordert, ihre technischen und organisatorischen Sicherheitsmaßnahmen nachvollziehbar zu etablieren und Cyberrisiken strukturiert zu steuern. In der Praxis schafft NIS-2 damit einen nachhaltigen Bedarf an belastbaren Sicherheitsprüfungen, die über formale Selbstbewertungen hinausgehen und einen echten Beitrag zur Risikoreduktion leisten.

Für Betreiber kritischer Infrastrukturen nach **KRITIS**-Verordnung gelten bereits heute klare Anforderungen nach BSIG (§30 und §31). In Sektoren wie **Energie, Gesundheit, Wasser, Finanzen und Transport** sind regelmäßige Sicherheitsnachweise nach §39 BSIG etabliert. Penetrationstests dienen hier nicht nur der formalen Erfüllung, sondern als zentrales Instrument, um die Wirksamkeit von Schutzmaßnahmen nachzuweisen und den stabilen, sicheren Betrieb kritischer Dienstleistungen langfristig abzusichern.

Der **Digital Operational Resilience Act (DORA)** verankert die kontinuierliche Prüfung und Weiterentwicklung der digitalen operativen Resilienz fest in der Governance des Finanzsektors. Der Fokus liegt auf der Wirksamkeit von IKT-Systemen, Prozessen sowie Erkennungs- und Reaktionsfähigkeiten gegenüber Cyberangriffen. Regelmäßige Penetrationstests und realitätsnahe Angriffssimulationen entwickeln sich damit zu einem integralen Bestandteil eines belastbaren Risiko- und Kontrollsystems.

## Der wirtschaftliche Wert realistischer Sicherheitstests

Unsichtbare Risiken verursachen häufig den größten Schaden. Während sichtbare Sicherheitsmaßnahmen in vielen Unternehmen gut etabliert sind, bleiben **reale Angriffspfade, unerkannte Schwachstellen und ungeprüfte Annahmen** über die Wirksamkeit von Kontrollen oft verborgen. Offensive Security macht diese blinden Flecken sichtbar, indem Sicherheitsarchitekturen, Prozesse und Reaktionsfähigkeit unter realistischen Angriffsbedingungen getestet werden – bevor aus Risiken tatsächliche Vorfälle entstehen.

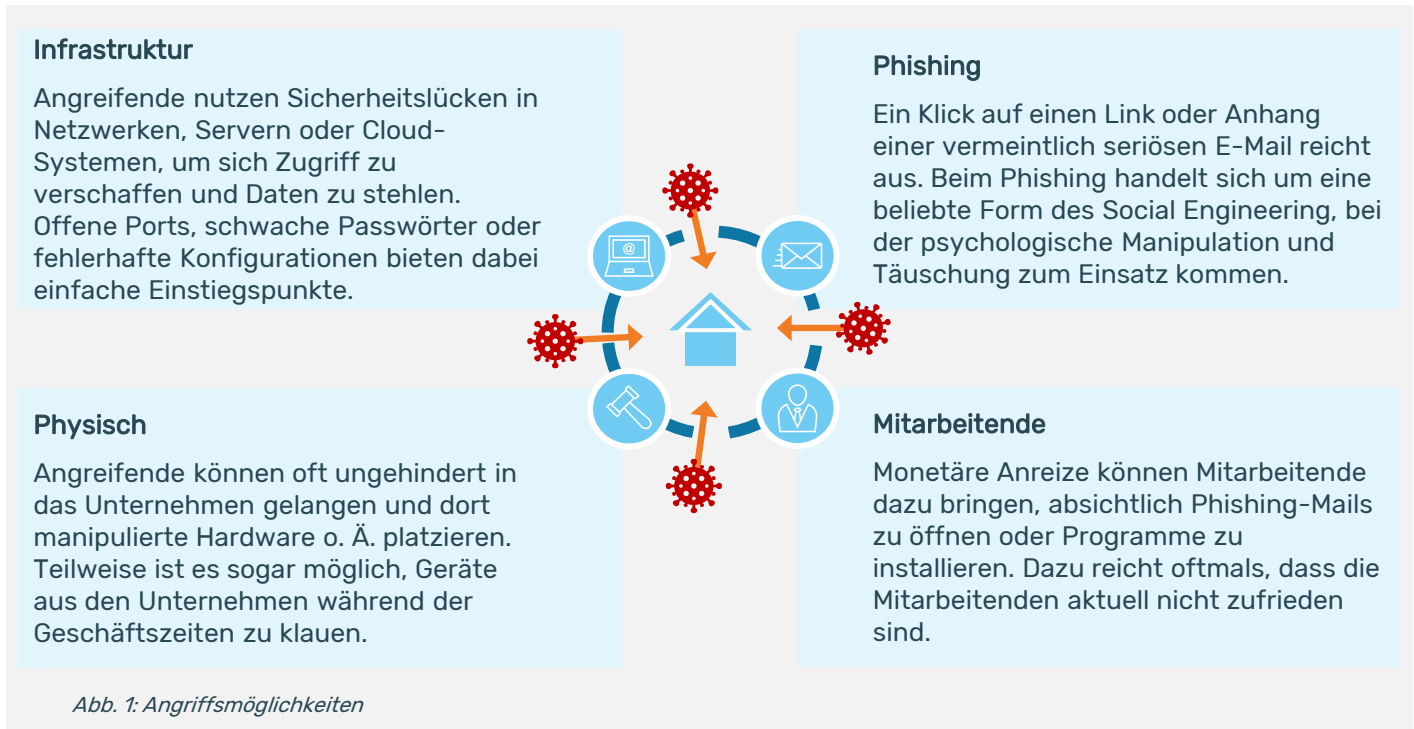
Offensive Security erzeugt keinen direkten Umsatz, liefert jedoch einen **messbaren wirtschaftlichen Nutzen** durch die Vermeidung realer Schäden. Jeder identifizierte und behobene Schwachpunkt reduziert das Risiko von Lösegeldzahlungen, senkt Kosten für Incident Response und Wiederherstellung und hilft, Umsatz- sowie Vertrauensverluste zu vermeiden. Damit wird der sonst schwer greifbare Wert von Sicherheit konkret messbar und leistet einen nachhaltigen Beitrag zur digitalen Resilienz.

<sup>1</sup> Bitkom – Wirtschaftsschutzstudie 2025, <sup>2</sup> Bitkom – IT-Sicherheitsmarkt 2025, <sup>3</sup> Allianz – Risk Barometer 2024



# Resilienz durch Kombination von Pentesting und Red Teaming

Angriffsziele: Infrastruktur, Cloud und Mitarbeiter, vielseitig und kritisch



## Penetests und Red Teaming testen Sicherheit unter realistischen Bedingungen

**Penetrationstests** identifizieren gezielt technische Schwachstellen in Netzwerken, Systemen und Anwendungen und machen potenzielle Einstiegspunkte für Angreifende transparent. **Red Teaming** ergänzt diesen Blick um reale Angreifer-Taktiken und prüft unter praxisnahen Bedingungen, ob Angriffe erkannt werden, wie schnell das Unternehmen reagiert und wie wirksam die vorhandenen Abwehr- und Reaktionsmechanismen tatsächlich sind.

**Gemeinsam liefern beide Testformen ein vollständiges und realistisches Bild der digitalen Resilienz**, indem technische, organisatorische und menschliche Faktoren zusammengeführt werden und eine fundierte Priorisierung von Sicherheits- sowie Detection- und Response-Maßnahmen ermöglichen.

Pentest			Red Teaming	
<b>Scope</b>	Applikation oder Netzwerk	VS	<b>Scope</b>	Gesamtorganisation
<b>Angriffsart</b>	Offen	VS	<b>Angriffsart</b>	Verdeckt
<b>Zeitraum</b>	Tage/Wochen	VS	<b>Zeitraum</b>	Wochen/Monate
<b>Ziel</b>	Schwachstellen identifizieren	VS	<b>Ziel</b>	Detection und Response verbessern

*Abb. 2: Unterschiede Pentest und Red Teaming*



# Unser USP und Leistungsangebot

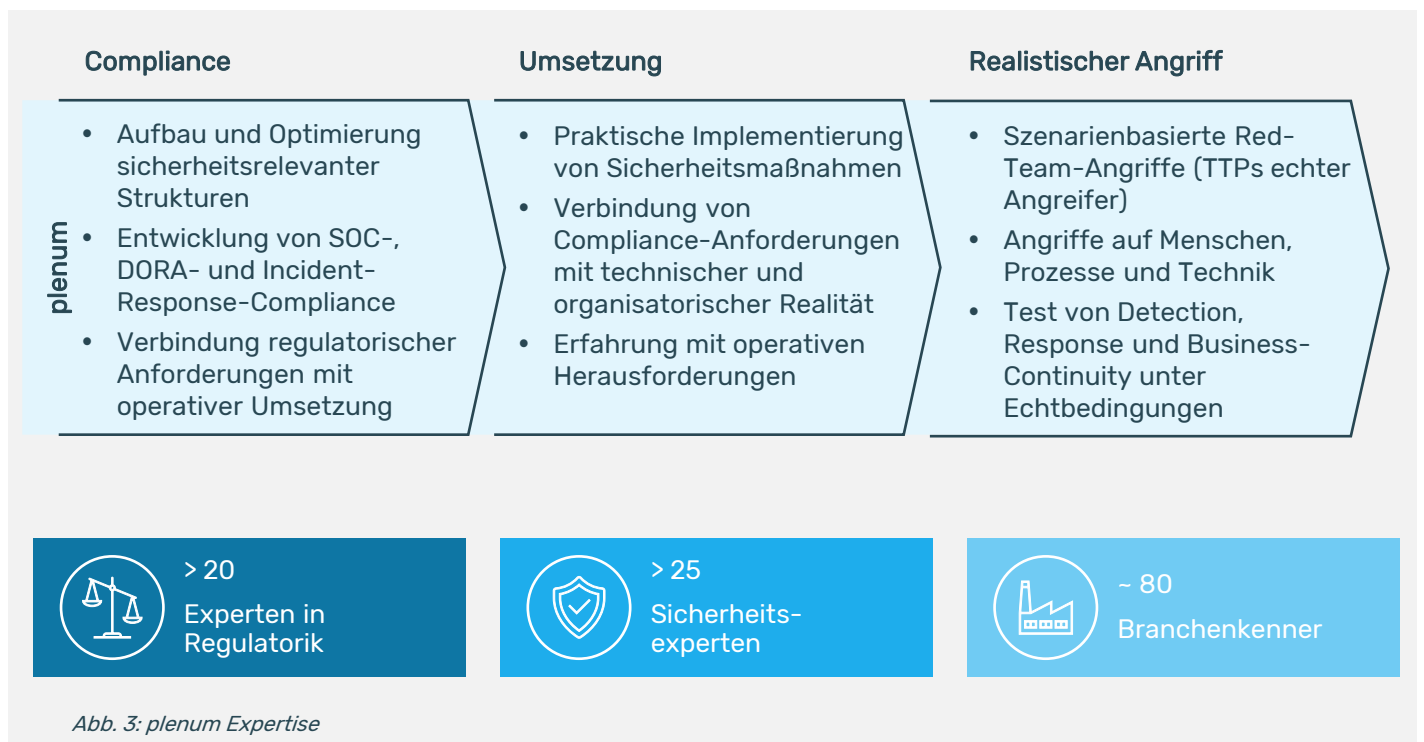
## Schluss mit „Security-Theater“ – Wir testen Ihre echte Resilienz

**Echte Angriffe, keine Checklisten:** Wir simulieren echte Bedrohungen. Keine Vulnerability-Scans mit Firmenlogo, sondern manuelle Exploits und komplexe Angriffspfade.

**Fokussierte, ehrliche Beratung:** Wir empfehlen ausschließlich Maßnahmen, die wirksam sind und Ihre Cyberresilienz erhöhen. Wir blähen keine Tagessätze auf und verkaufen keine Buzzwords.

**Sicherheit zuerst, Compliance inklusive:** Natürlich erfüllen wir alle Anforderungen nach DORA, NIS2 oder BAIT. Doch für uns ist Compliance das natürliche Nebenprodukt exzellenter Sicherheit – und nicht der alleinige Endzweck.

## Wir vereinen Management-Kompetenz und reale Angriffserfahrung



## Ein modulares Offensive-Security-Portfolio für reale Angriffsszenarien

plenum.red bietet ein modular aufgebautes Offensive-Security-Portfolio – von gezielten Penetrationstests für Infrastrukturen, Webanwendungen und KI-Systeme bis hin zu umfassenden Red-Team-Engagements. Assumed-Breach-Szenarien, Full-Scope-Red-Teamings und realitätsnahe Angriffssimulationen ermöglichen eine fundierte Bewertung von Erkennungs-, Reaktions- und Abwehrfähigkeit unter echten Angriffsbedingungen. Das Leistungsangebot richtet sich an Organisationen mit hohem Risikoprofil ebenso wie an Unternehmen mit regulatorischen Anforderungen und wird durch individuell zugeschnittene Projekte, etwa im Bereich physischer Sicherheit oder spezialisierter technischer Umgebungen, ergänzt.