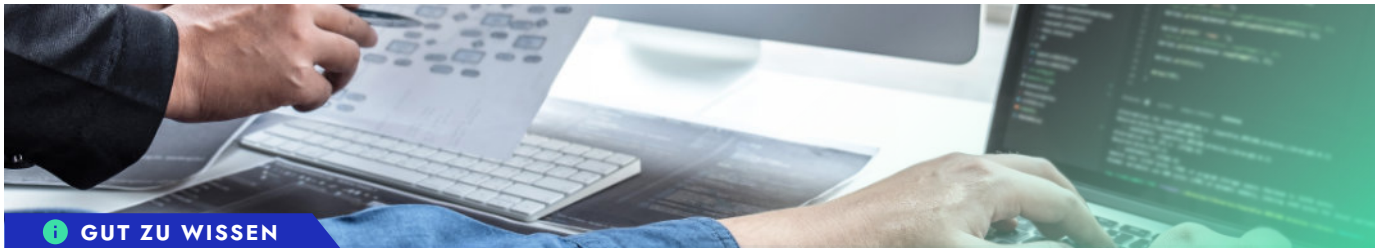


# Penetrationstests

Identifizieren Sie Stärken und Schwächen Ihrer IT-Systeme



## GUT ZU WISSEN

Penetrationstests sind mit Ihnen abgestimmte und von unseren Experten durchgeführte Eindringungsversuche in Ihr IT-System. Ziel ist es, externe Angriffsversuche in realer Härte zu simulieren, ohne dabei die Schutzziele Ihrer IT (Verfügbarkeit, Vertraulichkeit, Integrität) zu verletzen. Am Ende erhalten Sie einen konkreten Systemreport mit Wissensvorteilen über das Schutzniveau Ihrer IT-Infrastruktur zur zukünftig besseren Abwehr echter Angriffe.

## Darum geht's

Die **Anzahl der IT-Angriffe** in deutschen Unternehmen **steigt**. Dabei werden längst nicht mehr nur große Unternehmen Opfer digitaler Raubzüge: Knapp **die Hälfte aller Unternehmen mit 10 - 50 Mitarbeitern berichten von Attacken** in den zurückliegenden 12

Monaten. Laut einer repräsentativen Studie des Kriminologischen Forschungsinstituts Niedersachsens e.V. können **Hacking-Angriffe, Phishing, Spyware und Co.** „gerade für kleine und mittlere Unternehmen ein **bestandsgefährdendes Ausmaß** annehmen“.

## Warum Penetrationstests für Sie das Richtige sind

Keine bösen Überraschungen: **Beugen Sie Schaden durch Cyberangriffe vor** und bewahren Sie sich vor Datenverlusten, Erpressungen und sensiblen Leaks. Dies gelingt durch eine genaue **Definition Ihres IT-Schutzniveaus als Ergebnis** eines Penetrationstests. Diese **Penetrationstests sind kostengünstiger als die durchschnittlichen Schäden**, die durch den Verzicht auf derartige Tests entstehen (Verlust, Wiederherstellung von Daten). Als KRITIS-Klient profitieren Sie von einer **engmaschigen Betreuung**, sowie einem einzigartigen, kosteneffizienten Abomodell für sich wiederholende Penetrationstests zu (un)bestimmten Zeitpunkten. Nachhaltige Sicherheit-as-a-Service.

## Ideale Szenarien für Penetrationstests

Einhaltung vorgeschriebener  
Sicherheitsrichtlinien inkl.  
DIN ISO 27001



Schutz Ihrer Daten,  
der Daten Ihrer Kunden,  
Partner und Mitarbeiter



Konzipierung relevanter  
Sicherheitsmaßnahmen (Nullmessung)



Ausfallzeiten im Netzwerk  
reduzieren (Folgekosten sparen)



Identifikation versteckter  
Sicherheitslücken im  
gesamten IT-Netzwerk



Marken-Image vor  
Schäden bewahren



## Ihr Weg zum Penetrationstest

### **1. Kickoff**

Gemeinsam führen wir ein digitales oder vor-Ort-Kickoff durch, indem wir Ihre zu testenden Systemmodule definieren.

### **2. Penetrationstest**

In stetiger Kommunikation mit Ihrer IT nehmen wir die Eindringungsversuche in Ihr System vor, ohne dass Mitarbeiter oder Kunden davon Notiz nehmen.

### **3. Reporting**

Alle Phasen und Ergebnisse jedes Penetrationstests werden dokumentiert und in Ihrem eigenen IT-Report zusammengefasst.

### **4. Auswertung**

Sie erhalten ein Management-Resümee des Penetrationstests inkl. geeigneter Reaktionsmaßnahmen als Entscheidungsvorlage.

### **5. Behebung**

Sie kommen den Schwachstellen nach und beheben identifizierte Einfallstore in Ihre IT-Systeme

### **6. Erfolgsmessung**

In einem erneuten, schwerpunkt-basierten Penetrationstest wird der Erfolgsgrad der Schwachstellenbehebung festgestellt.

## Produkttypen

### Black Box Penetrationstest

In diesem Testverfahren stehen uns keine internen Systeminformationen, Daten oder Schwerpunkte zu Verfügung. Der Test kann verdeckt stattfinden. Ihr System wird einer realitätsnahen, externen Angriffssimulation ausgesetzt, mit dem Ziel dieses zu infiltrieren.

### Grey Box Penetrationstest

**Empfehlung:** Diese Methodik sieht eine engere Kommunikation zwischen Klient und Testern vor. Schwerpunkte („Perimeterkennung“) können Ihrerseits kommuniziert oder von uns vorab identifiziert werden. Allgemein zeichnet sich dieses Verfahren durch erhöhte Variabilität aus.

### White Box Penetrationstest

Im Vorfeld dieser Tests werden umfangreiche Informationen vorab an uns übermittelt. Dies kann insbesondere für bereits bestehende Verdachtsmomente wertvoll sein, und erlaubt eine umfassendere Prüfung in der dafür zur Verfügung stehenden Zeit.



## Den ersten Schritt haben Sie bereits gemacht. - Jetzt helfen wir Ihnen.

Unser Expertenteam ist gerne für Sie da. Nehmen Sie unverbindlich Kontakt auf, lassen Sie uns Rückfragen klären und Ihren Bedarf ermitteln.

[kontakt@kritis-cyber.de](mailto:kontakt@kritis-cyber.de)

[kritis-cyber.de/kontakt](https://kritis-cyber.de/kontakt)

### Weitere KRITIS Produkte

#### Informationssicherheit nach ISO 27001 & Audit

*Stärken Sie das Vertrauen Ihrer Stakeholder und senken Sie Ihr Haftungsrisiko.*



#### Digitale Forensik

*Erhalten Sie Beweise für digitale Rechtsverstöße, gerichtsverwertbar.*



#### Externer CTO

*Überlegenes technisches Know-how für die Geschäftsführung - für kurz- und langfristige Projekte.*

