
**Die Wahrscheinlichkeit eines Brandes liegt bei 1 zu 8000.**
**Die Wahrscheinlichkeit, dass mangelhafte Cybersicherheit**

**Ihr Unternehmen gefährdet, liegt bei 1 zu 5.**

# WO KANN EIN HACKER SIE ANGREIFEN?

## Die Cyber Risk Map bietet Einblick und einen klaren Maßnahmenplan.

Cyberkriminalität stellt eine zunehmend größere Bedrohung für Unternehmen dar. Hacker, Datenlecks und Phishing können Ihre Unternehmensdaten und Ihren Ruf ernsthaft schädigen. Wissen Sie, wie verwundbar Ihr Unternehmen ist? Was tun Sie dagegen – und wo fangen Sie an?

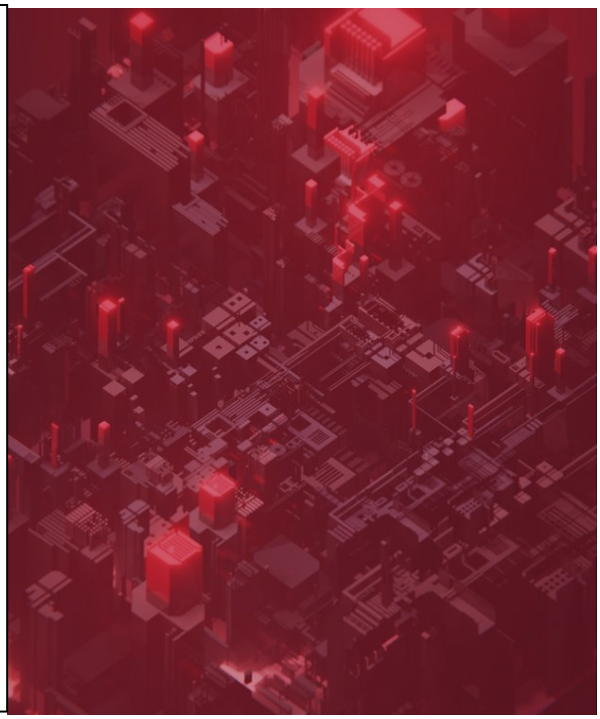
## Die Cyber Risk Map bietet Klarheit – ganz ohne hohe Vorabkosten.

Unsere Cyber Risk Map zeigt, wie Hacker Ihr Unternehmen angreifen könnten, indem sie Ihre vorhandene IT-Landschaft und deren Verbindung zum Internet analysiert. Was sieht ein Hacker, wenn er Ihr Unternehmen ins Visier nimmt? Die Cyber Risk Map ist ein erster, unkomplizierter Schritt, um Risiken sichtbar zu machen – ohne direkt hohe Investitionen tätigen zu müssen.

**Mit der Cyber Risk Map erhalten Sie eine klare Priorisierung und wissen genau, welche Maßnahmen notwendig sind.**
Der nächste Schritt ist eine Hack-Simulation (vollständiger Penetrationstest), bei der wir die Schwachstellen in Ihrer IT-Umgebung gezielt identifizieren, potenzielle Bedrohungen aufdecken und konkrete technische Empfehlungen zur Verbesserung der Sicherheit geben. **Die Kosten der Cyber Risk Map werden Ihnen bei Beauftragung dieser Dienstleistung angerechnet.**

**Unsere Dienstleistungen**

- Phishing-Kampagnen
- Netzwerk-Penetrationstests (intern und extern)
- Überprüfung von Cloud-Konfigurationen
- Penetrationstests von Anwendungen und Websites
- API-Penetrationstests
- Code-Reviews
- Red Teaming
- Bedrohungsgesteuerte Penetrationstests(Threat-Led Penetration Tests)
- Ransomware-Schwachstellenanalysen

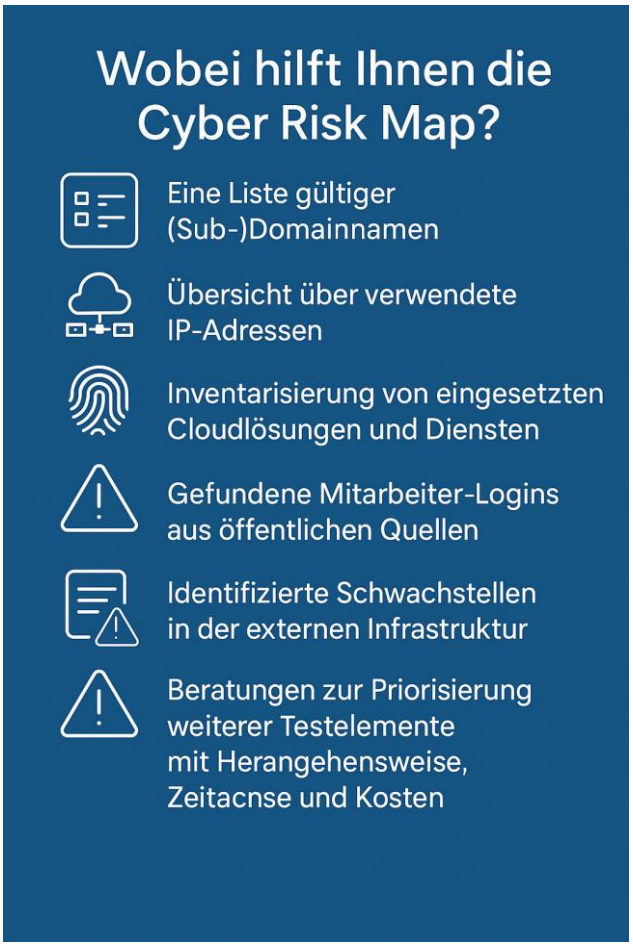


## Warum die Cyber Risk Map wählen?

- ✅ Erfahrene Cybersecurity-Spezialisten
- ✅ Praktische und umsetzbare Empfehlungen ohne hohe Vorabkosten
- ✅ Vermeidung teurer Schäden und Reputationsverluste

## Exklusiver Rabatt

Entscheiden Sie sich nach der Analyse dafür, die Risiken mit einer echten Hack-Simulation (Penetrationstest) weiter zu untersuchen?
Dann erhalten Sie Ihre Investition von 2.000 € zurück bei einer Beauftragung ab 10.000 € – oder Sie bekommen 10 % Rabatt, wenn der Gesamtbetrag darunter liegt!





## Kontaktieren Sie uns!

Möchten Sie wissen, wo Ihre Cyberrisiken liegen?
Nehmen Sie noch heute Kontakt mit uns auf oder buchen Sie ein kurzes Meeting!

# Wie erstellen wir eine Cyber Risk Map?

Wir tun zwei Dinge: Wir führen ein Gespräch und führen einen externen Test durch, inklusive eines OSINT-Checks (Open Source Intelligence – das Sammeln und Analysieren öffentlich zugänglicher Informationen, um Einblicke in Personen, Organisationen oder Situationen zu gewinnen).

**Gespräch**

Wir führen ein etwa einstündiges Gespräch mit dem IT-Verantwortlichen (ggf. auch mit dem CISO) und besprechen, welche IT-Strukturen die Organisation intern und extern besitzt.

- Wie sieht das interne Netzwerk aus? Gibt es On-Premises-Server? Gibt es interne IoT-Geräte? Oder besteht das Netzwerk nur aus ein paar Laptops und Access Points?
- Handelt es sich um ein flaches Netzwerk oder gibt es mehrere VLANs?
- Wie werden Arbeitsplätze und Server verwaltet? Gibt es eine Windows-Domäne oder werden Laptops über Intune verwaltet?
- Wo werden die Daten gespeichert? Gibt es interne Server oder liegt alles in OneDrive und SharePoint?
- Entwickelt die Organisation eigene Webanwendungen oder gibt es Anwendungen, von denen sie stark abhängig ist und die man auf Sicherheit prüfen sollte?

**External Attack Surface Assessment**

Wir untersuchen die extern erreichbaren Zugangspunkte der Organisation. Zunächst führen wir ein OSINT-Assessment durch, um internetzugängliche IT-Assets wie Domains, Subdomains und IP-Adressen zu identifizieren – inklusive Cloud-Ressourcen (Azure, AWS, GCP).

Nach Freigabe der gefundenen Assets führen wir einen Scan durch, um erreichbare Systeme und Dienste zu analysieren. Danach werden Schwachstellenscans mit Tools wie Nuclei und Nessus durchgeführt, wobei erkannte False Positives manuell verifiziert werden.

Zusätzlich prüfen wir, ob gültige Zugangsdaten von Mitarbeitenden oder Services öffentlich zugänglich sind. Wenn ja, versuchen wir, Zugriff auf Verwaltungsportale oder Cloud-Umgebungen zu erhalten. Alle kritischen Erkenntnisse werden selbstverständlich zuerst mit der Organisation besprochen.

# BE SURE

SECURANCE


**The Netherlands**
Reactorweg 47 (4th floor)
3542 AD Utrecht, The Netherlands
Tel: +31(0)30 280 08 88
Mail: info@securance.com

**Sweden**
Sidenvävargatan 17
75319 Uppsala, Sweden
Tel: +46(0)703040656
Mail: info@securance.com

**United Kingdom**
63-66 Hatton Garden
Londen EC1N 8LE, United Kingdom
Tel: +44 (0)20 351 446 56
Mail: info@securance.com

**Germany**
Josef-Orlopp-Strasse 54
10365 Berlin, Germany
Tel: +49 (0)30439716860
Mail: info@securance.com