# DEMANDO - Die IT-Macher

Als erfahrener und zukunftsorientierter Full-Service-IT-Dienstleister mit eigenem Rechenzentrum und fast 100 Mitarbeiter in Kaiserslautern profitieren Sie von den Vorteilen eines der sichersten und modernsten Rechenzentren Europas, dem hohen Know-how unserer IT-Macher und unserem breiten Leistungsspektrum, wie Cloud- oder Managed Services und Themen rund um die IT-Sicherheit.

Wir sind der festen Überzeugung: Nur das Höchstmaß an organisatorischer und technologischer Sicherheit, die höchste Verfügbarkeit und die absolute Integrität der Daten führen zur Basis jeglicher Zusammenarbeit mit unseren Kunden – zu Vertrauen. Als objektiven Beleg für unsere Vertrauenswürdigkeit haben wir im Rahmen unseres Qualitätsmanagements die gesamten Rechenzentrumsdienstleistungen – d. h. über alle Prozesse, Produkte und Services hinweg – nach ISO/IEC 27001:2022 zertifizieren lassen.

Beim Thema IT-Sicherheit gehen wir keine Kompromisse ein. Sie profitieren bei uns von einer umfassenden Absicherung der IT-Systeme und unserem qualifizierten Personal.

Ganz in Ihrem Sinn beachten wir zudem bei allen Projekten den Grundsatz eines offenen und partnerschaftlichen Kontakts zu unseren Kunden: Das Ergebnis sind intelligente Outsourcing-Konzepte, die von Qualität, Sicherheit, Transparenz und einem guten Preis-/Leistungsverhältnis geprägt sind.

**Kümmern Sie sich um Ihr Kerngeschäft, wir kümmern uns um Ihre IT!**

# PenTesting

## Ihr IT-Sicherheitscheck


**Kontaktdaten:**
DEMANDO GmbH
Europaallee 10 · 67657 Kaiserslautern
Telefon: 0631 8001 6000
(Mo-Fr: 7:00 - 17:30 Uhr)
**www.demando.de**

**Ansprechpartner:**
Manfred Stumpf
Leiter IT-Sicherheit, Lizenz-, Partner- und Keyaccountmanagement, Informationssicherheitsbeauftragter
Telefon: 0631 8001 6061
Telefax: 0631 8001 6110
E-Mail: manfred.stumpf@demando.de


TÜV SAARLAND Geprüftes Rechenzentrum Stufe 3 tekPlus tuv-saar.com/id/46236

TÜV SAARLAND Geprüfte Energieeffizienz Systemzertifizierung tuv-saar.com/id/46237

TÜV SAARLAND Geprüftes Rechenzentrum in Anlehnung an DIN EN 50600 Verfügbarkeitsklasse 3 www.tuv-saar.com/ID/46324

DEMANDO

DIE IT-MACHER

# DEM Security PenTesting

Professionelle PenTestings simulieren den Ernstfall und helfen damit, Ihr Unternehmen wirkungsvoll vor Angriffen durch Hacker und andere Cyber-Kriminelle zu schützen. Nur wenn Sie die Schwachstellen in Ihrer IT-Landschaft kennen, können Sie rechtzeitig geeignete Gegenmaßnahmen ergreifen.
Unsere Experten, u.a. Certified Ethical Hacker & Licensed Penetration Tester, dringen mit den Methoden und Werkzeugen der kriminellen Hacker in Ihre IT-Infrastruktur ein. Während es den Kriminellen jedoch darum geht, Informationen zu stehlen oder Schaden anzurichten, identifizieren unsere ethischen Hacker ausschließlich mögliche Schwachstellen.
Regelmäßige PenTestings helfen Ihnen dabei, sensible Informationen wirkungsvoll gegen Hackerangriffe zu schützen. Sie können Ihre IT-Systeme somit rechtzeitig vor Einbrüchen absichern, indem Sie sicherheitsrelevante Schwachstellen rechtzeitig erkennen und beheben können.

Die Sicherheit der IT-Systeme und Anwendungen kann dabei aus zwei Perspektiven geprüft werden:

- Das Angriffsszenario des klassischen Hackers simuliert einen externen Angriff über das Internet oder andere öffentlich erreichbare IT-Systeme.
- Beim Innentäter-Szenario werden Angriffe aus dem eigenen Unternehmensnetzwerk heraus nachgestellt.

# Module unserer PentTestings

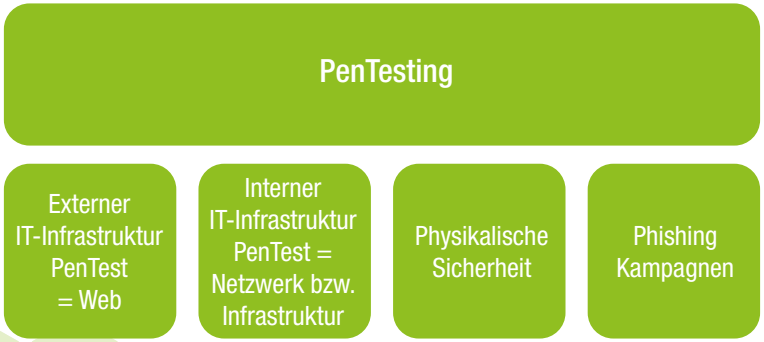


Abbildung 1: Module des PenTesting

**Selbstverständlich können die Module auch kombiniert werden!**

# Unser standardisiertes Vorgehensmodell

Unsere PenTestings folgen einem standardisierten, sechsstufigen Vorgehensmodell:

1. **Kick-Off:** In einem Kick-Off-Gespräch werden alle organisatorischen Fragen wie Ort und Zeitpunkt des PenTestings und auch die konkreten Ziele und der Umfang der individuellen Prüfungen abgestimmt. Dabei erläutern unsere Experten, wie der Penetrationstest durchgeführt wird und welche Angriffsszenarien geprüft werden.

2. **Angriff:** Mit manuellen und automatisierten Verfahren und den entsprechenden Werkzeugen werden nun die ausgewählten Ziele entsprechend der zuvor vereinbarten Angriffsszenarien penetriert. Dabei arbeiten unsere Experten so, wie es auch kriminelle Hacker tun würden – nur so erhält der Auftraggeber ein realistisches Bild des aktuellen Sicherheitsniveaus.

3. **Dokumentation:** Die identifizierten Schwachstellen werden von unseren erfahrenen Experten (u.a. Certified Ethical Hacker (CIEH) bzw. Licensed Penetration Testern (LIPT)) bewertet und dokumentiert.

4. **Maßnahmenplan:** Um den Auftraggeber optimal bei der Behebung der identifizierten Schwachstellen zu unterstützen, wird ein individueller Maßnahmenplan erstellt. Dabei werden die Maßnahmen entsprechend der Kritikalität priorisiert.

5. **Bericht:** In einer kurzen Präsentation werden die Ergebnisse des durchgeführten PenTestings vorgestellt. Dabei werden die identifizierten Schwachstellen benannt und anhand des Maßnahmenplans aufgezeigt, wie das Sicherheitsniveau zukünftig weiter ausgebaut werden kann.

6. **Re-Test:** Nach der Umsetzung der Maßnahmen erfolgen zielgerichtete Prüfungen auf die jeweiligen Schwachstellen. So lässt sich feststellen, ob die Schwachstellen tatsächlich vollständig behoben wurden und das Schutzniveau optimiert werden konnte.

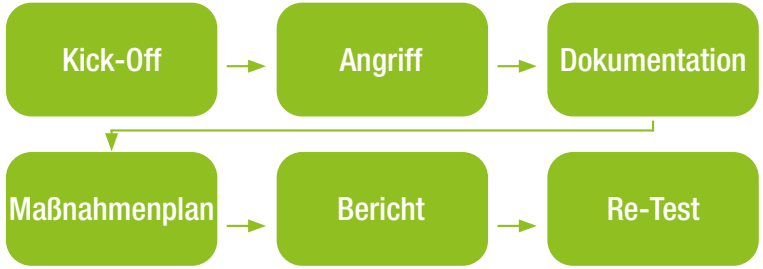


Abbildung 2: Vorgehensmodell

**Gerne erstellen wir Ihnen ein Angebot. Der Preis richtet sich nach Ihren individuellen Anforderungen.**