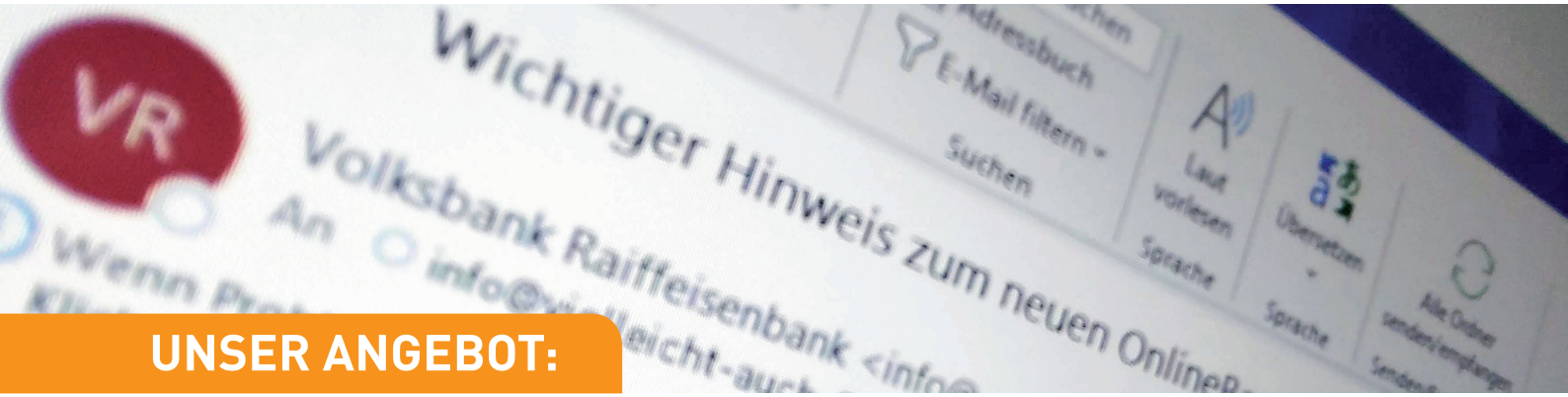
STEP Pentesting



UNSER ANGEBOT:

Bringen Sie Ihre IT-Sicherheit mit **Pentesting** auf ein neues Level

Beim Pentesting (Kurzform für Penetration Testing) werden IT-Systeme, Netzwerke oder Ihre Mitarbeiter wie bei einem realen Angriff durch echte Hacker getestet, um Schwachstellen zu identifizieren und das allgemeine Potenzial einer Gefährdung zu analysieren und zu dokumentieren.

Die Ergebnisse eines solchen Tests sind dann Grundlage für eine Beseitigung eventueller Schwachstellen sowie für eine Härtung der Unternehmens-IT. Auch die Überprüfung der Unternehmensorganisation und ihrer Widerstandsfähigkeit gegenüber sogenanntem „Social Engineering“ fällt in diesen Bereich.

STEP Computer- und Datentechnik GmbH

Standort Lörrach
Im Entenbad 20
D-79541 Lörrach

Telefon +49 76 21 40 57-0
Telefax +49 76 21 40 57-50
welcome@stepnet.de

Öffnungszeiten:
Mo–Fr 7:30–16 Uhr u.n.V.

Telefonische Erreichbarkeit:
Mo–Fr 7:30–18 Uhr

STEP Computer- und Datentechnik GmbH

Standort Schönau
Oberfeldstraße 1–5
D-79677 Schönau

Telefon +49 7673 88 09 1-0
Telefax +49 761 40 57-50
schoenau@stepnet.de

Öffnungszeiten:
Mo–Fr 7:30–16 Uhr u.n.V.

Telefonische Erreichbarkeit:
Mo–Fr 7:30–18 Uhr

STEP Business Solutions AG

Standort Basel
Steinentorstrasse 19
CH-4002 Basel

Telefon +41 61 511 20 70
Telefax +41 61 511 20 80
welcome@step-bs.ch

Öffnungszeiten:
Mo–Fr 7:30–16 Uhr u.n.V.

Telefonische Erreichbarkeit:
Mo–Fr 7:30–18 Uhr

STEP Pentesting

Typische Szenarien für Penetration Tests

Externer Penetrationtest

Hier agieren die Tester als anonyme Angreifer und versuchen Schwachstellen in der von außen sichtbaren Infrastruktur zu finden (inkl. VPN, Clouddienste etc.).

Interner Penetrationtest

Hier identifizieren die Tester Schwachstellen der von innen sichtbaren Infrastruktur (inkl. WLAN, Clients, Server etc.) aus Sicht eines Innentäters.

Social Hacking

Durch zwischenmenschliche Beeinflussungen versuchen die Tester, vertrauliche Informationen zu erlangen. Bekannte Methoden sind allgemeines Social Engineering, Pretexting, Tailgating und Media Dropping.

Penetrationtest von Anwendungen

Anwendungssoftware wie z. B. Ihr Web-Shop, Ihr CMS, Ihre Webserver und Ihre Android- oder iOS-Apps werden auf Schwachstellen untersucht.

Wie läuft ein Pentesting ab?

1. Vorbereitung

In der Vorbereitung werden wesentliche Kriterien wie Typ und Ziel des Audits sowie organisatorische Maßnahmen besprochen.

2. Information

Die Informationsbeschaffung dient der Sammlung relevanter Informationen in frei verfügbaren, offenen Quellen, um durch Analyse der unterschiedlichen Informationen verwertbare Erkenntnisse zu gewinnen.

3. Analyse

Die gesammelten Informationen werden nach sicherheitsbezogenen Problemen analysiert und über direkte Angriffssimulationen verifiziert.

4. Bericht

Zum Abschluss eines Audits werden alle Informationen detailliert zusammengefasst. Jede Schwachstelle wird nach ihrem Gefahrenpotenzial gewichtet und mit einem entsprechenden Vorschlag für ihre Behebung ausgewiesen.

STEP Pentesting

UNSER ANGEBOT:

Initialer Perimeter-Check (Penetrationstest extern)

Ein Security-Analyst versucht als anonymer Angreifer aus dem Internet, Schwachstellen in der von außen sichtbaren Infrastruktur zu finden.

Beim initialen Perimeter-Check geht es darum, mögliche Angriffsziele zu identifizieren und Schwachstellen der erreichbaren Dienste aufzulisten. Dabei werden auch die Level der implementierten Sicherheitskontrollen und Konfigurationen der eingesetzten Komponenten identifiziert. Der Check beinhaltet im Detail:

- **Firewall-Check, VPN-Check**
- **Verfügbare Dienste identifizieren**
- **Autorisierung und Authentifizierung überprüfen**
- **Augenscheinliche Fehlkonfigurationen aufzeigen**
- **Schwachstellen automatisiert scannen**
- **Manuelle Prüfung (Stichproben)**
- **Ergebnisse auswerten**

Bei einem initialen, externen Penetrationstest werden alle gefundenen Schwachstellen analysiert und klassifiziert, jedoch nur die fünf kritischsten Schwachstellen ausgeführt, verifiziert und detailliert dokumentiert.

Initialer Penetrationstest intern		Preis
SMALL	< /24 (256 IP-Adressen/Hosts) (~ 5 Server, 20 IT-Seats)	1.500,00 €
MEDIUM	< /22 (1.024 IP-Adressen/Hosts) (~ 20 Server, 100 IT-Seats)	3.500,00 €
LARGE	< /18 (< 16.384 IP-Adressen/Hosts) (~ 100 Server, 1.000 IT-Seats)	7.500,00 €

STEP Pentesting

UNSER ANGEBOT:

Initialer Penetrationtest intern

Sind Sie sicher, dass vertrauliche Informationen in Ihrem Unternehmen auch vertraulich bleiben und nicht unbemerkt abfließen können?

Bei diesem Test prüfen wir, ob ein interner Angreifer oder ein Trojaner im internen Netzwerk auf einfache Weise mehr Privilegien erlangen kann oder Zugriff auf sensitive Systeme oder Daten erhält. Dabei suchen wir nach Schwachstellen in der internen IT-Infrastruktur, beispielsweise durch:

- **Asset-Discovery**
- **Schwachstellenscan**
- **Rechteerweiterung (Privilege Escalation)**
- **Ausbreitung im Netzwerk (Lateral Movement)**
- **Zugriff auf Daten und Systeme prüfen**

Bei einem initialen, internen Penetrationstest werden alle gefundenen Schwachstellen analysiert und klassifiziert, jedoch nur die fünf kritischsten Schwachstellen ausgeführt, verifiziert und detailliert dokumentiert.

Initialer Penetrationstest intern		Preis
SMALL	< /24 (256 IP-Adressen/Hosts) (~ 5 Server, 20 IT-Seats)	1.500,00 €
MEDIUM	< /22 (1.024 IP-Adressen/Hosts) (~ 20 Server, 100 IT-Seats)	3.500,00 €
LARGE	< /18 (< 16.384 IP-Adressen/Hosts) (~ 100 Server, 1.000 IT-Seats)	7.500,00 €

STEP Pentesting

UNSER ANGEBOT:

Awareness Training / Live-Hacking

Cyberkriminalität hat viele Gesichter – schulen Sie jetzt Ihre Mitarbeiter spielerisch, effektiv und nachhaltig, um die Techniken der Täter zu erkennen.

Angriffsszenarien in IT-Umgebungen erleben und verstehen: Das ist das Motto dieses Sicherheitstrainings. Den Teilnehmern wird praktisches Hintergrundwissen für ein besseres Verständnis und eine höhere Akzeptanz von IT-Sicherheit vermittelt, sowohl für den Beruf als auch privat. Hauptziel ist es, die Risiken über das **„Einfallstor Mitarbeiter"** zu minimieren und das Bewusstsein für Gefahren im Umgang mit IT-Systemen zu sensibilisieren und zu steigern.

Bei einem **Awareness Training** werden die Teilnehmer für **Gefahren im Umgang mit IT-Systemen** sensibilisiert, indem wir mögliche Angriffsszenarien durch Live-Hacking demonstrieren und Ihre Mitarbeiter so auf Bedrohungen aufmerksam machen. Des Weiteren ist ein Impulsvortrag Bestandteil dieses Moduls. Dabei werden **alle Angriffsszenarien ausführlich erläutert** und **live demonstriert**. Das Training wird von einem TÜV-zertifizierten (PersCert) „Security-Awareness-Koordinator" durchgeführt.

Inhouse-Veranstaltung
(max. 20 Teilnehmer pro Vortrag, Preise je Block à 20 Teilnehmer), zzgl. Reisekosten

Awareness Training / Live-Hacking		Preis
Paket SMALL	bis 20 Mitarbeiter / 1 Vortrag	2.500,00 €
MEDIUM	21–40 Mitarbeiter / 2 Vorträge	4.000,00 €
LARGE	41–80 Mitarbeiter / 4 Vorträge	6.000,00 €