
RAPID7
Kennen Sie Ihre Schwächen?
Veraltete Software?
Schwache Prozesse?
Fehlende Sicherheitspatches?
Unsicherer Umgang mit Passwörtern?
Fehlkonfigurationen?
WIR HABEN ANTWORTEN.
"UNDER THE HOODIE 2019"
bringt Licht ins Dunkel.

**UNDER THE HOODIE 2019**
Ein Bericht von RAPID7 Global Consulting

# TYPISCHE SCHWACHSTELLEN

die **180** Penetrationstests in den Jahren 2018 und 2019 zeigten

Netzwerk-Schwachstellen


Schwache Verschlüsselungsstandards


Unsicherer Umgang mit Passwörtern

Fehlende Sicherheitspatches

Veraltete Software

Fehlkonfigurationen

In Klartext gespeicherte Anmeldedaten

Offener Zugang zur Datenbank

# TESTBEREICHE

- Externe Netzwerkgefährdung
- Interne Netzwerkgefährdung
- Elektronisches Social Engineering
- Physisches Social Engineering
- Untersuchung des Anwendungscodes
- Red Team Angriffssimulation

# PENETRATIONSTESTS

# DAS WICHTIGSTE ZUERST

## DIE GUTEN NACHRICHTEN


der extern durchgeführten Tests konnte Zugang zum internen LAN erlangt werden


der Angriffe, die über Webanwendungen gestartet wurden, führten zu einer Gefährdung auf der gesamten Website

## DIE SCHLECHTEN NACHRICHTEN


der Netzwerk- und Anwendungstests offenbarten mindestens eine für Angreifer offene Schwachstelle


der Aufträge mit Bezug auf die Sicherheit der Anmeldedaten wurde mindestens ein Passwort offengelegt

**DEFINIERT**

MEHR DETAILS AUF DER INNENSEITE

# IST IHR UNTERNEHMEN GEGEN DIESE SICHERHEITSRISIKEN GESCHÜTZT?


ERKLÄRT UND

# JETZT BERICHT LESEN

**www.rapid7.de/research/under-the-hoodie**

**SPRECHEN SIE MIT EINEM RAPID7-EXPERTEN**
+49 (0)89 97 007 007

# FÜNF REALE FALLBEISPIELE

In den realen Fallbeispielen im Bericht betrachten Sie Ihr Netzwerk durch die Augen der Hacker.

- ✔ Deine Maus ist meine Tastatur
- ✔ Nachricht für Doktor Hackerman
- ✔ Ihre Daten, frei und ungeschützt
- ✔ Sie haben da etwas übersehen
- ✔ Nerds in der NERC

?

- Welche Unterschiede gibt es zwischen den unterschiedlichen Arten von Penetrationstests?
- Welche externen Schwachstellen treten am häufigsten auf?
- Wie kann ein Hacker vom externen zum internen Netzwerk gelangen?
- Welche Lateral Movement-Techniken werden am häufigsten verwendet?
- Welches sind die häufigsten Schwachstellen bei Web-Anwendungen?
- Welche Social Engineering-Techniken funktionieren am besten?
- Wie gelangen Hacker an Anmeldedaten?

# QUANTIFIZIERT

RAPID7

Entdecken Sie in unserem neuesten Bericht "Under the Hoodie 2019" die geheime Welt der Penetrationstester.

Wie testen wir Ihre Abwehrmaßnahmen? Welche Probleme finden wir? Wo liegen Ihre Schwachstellen wirklich? Das und viel mehr erfahren Sie bei "Under the Hoodie 2019".

## BERICHT JETZT LESEN

**www.rapid7.de/research/under-the-hoodie**

**SPRECHEN SIE MIT EINEM RAPID7-EXPERTEN**

+49 (0)89 97 007 007

# BEREIT, IHRE SICHERHEIT ZU VEREINFACHEN?

### SOFTWARELÖSUNGEN

- Schwachstellen-Management
- Incident Detection and Response
- Application Security
- Security Automation and Orchestration
- Log-Management

### DIENSTLEISTUNGEN

- Managed Detection and Response
- Managed Vulnerability Management
- Managed Application Security
- Consulting
- Incident Response
- Penetration Testing
- IoT Security
- Training und Zertifizierung