Red Teaming

Ein Jahr Red Teaming

Vergleiche, Erfahrungen und Berichte

Stuttgart 25.02.2019

Referent

B.Sc.
Christoph Ritter
Senior IT-Security Consultant
Penetration Tester
Head of Red Teaming

Dozent an der HS Aalen

+49 7071 – 40785658
christoph.ritter@syss.de
www.syss.de

Agenda

- Was ist Red Teaming
- Vorgehen
- Red Teaming vs. Pentesting
- Vorteile von Red Teaming
- Erfahrungsbricht

Definition Red Team

Als **Red Team** oder als **Rotes Team** wird eine unabhängige Gruppe bezeichnet, welche eine Organisation zur **Verbesserung der Effektivität** bringen soll, indem sie als Gegner auftritt. Ziel ist es dabei immer Sicherheitslücken aufzuspüren, bevor ein externer Dritter diese ausnutzen kann. Es ist besonders effektiv in Organisationen mit starren Strukturen und eingefahrenen Verfahrensweisen.

Vgl. https://de.wikipedia.org/wiki/Red_Team

Red vs. Blue

Pentesting vs. Red Teaming

Zielsetzung eines Penetrationstests ist es in einem klar definierten engen Rahmen alle Schwachstellen, zu finden welche das Zielobjekt hat und diese zu dokumentieren.

Zielsetzung von Red Teaming ist es einen validen Weg zur Erreichung der Zielsetzung zu finden unter Zuhilfenahme von frei wählbaren Angriffsvektoren. Dabei ist der Rahmen sehr weit gefasst und der Angreifer hat einen hohen kreativen Freiraum. Ein eingesetztes Blue Team hat die Aufgabe die Angriffe das Red Teams zu detektieren und zu verhindern. Dabei wird das Blue Team und dessen Maßnahmen getestet und weiter ausgebaut.

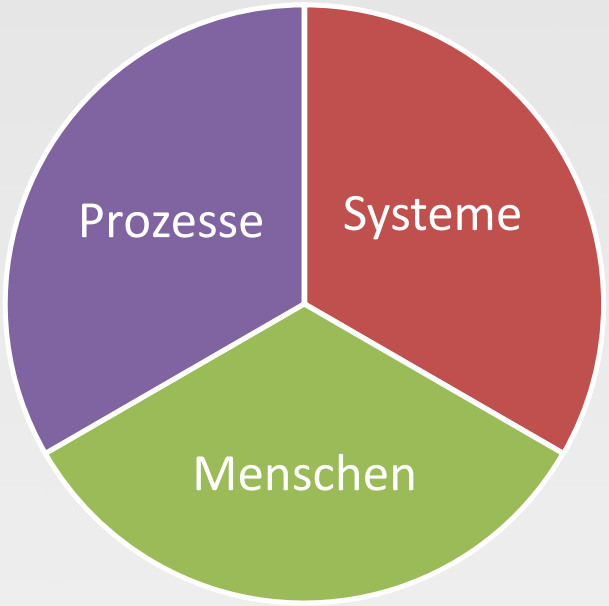
Pentesting vs. Red Teaming

Quelle: https://twitter.com/privesque

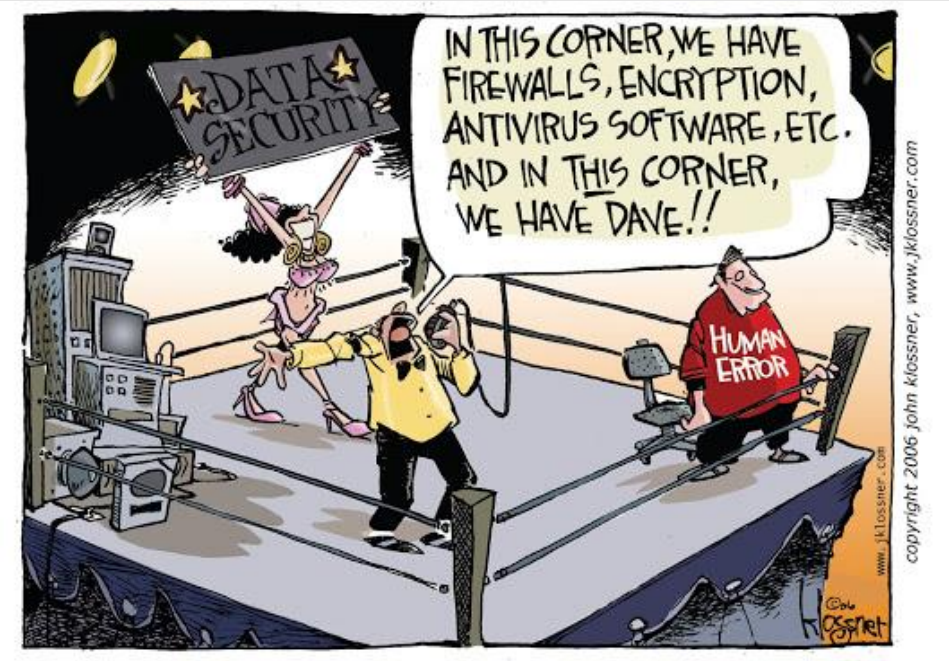
	Vulnerability Scan	Penetrationtest	Red Teaming
Erforderliches Skill-Level	Kurze Einweisung	Schulung erforderlich	Langjährige, breitgefächerte Berufserfahrung erforderlich
Techniken	Vollautomatisierte softwarebasierte Erkennung von bekannten Schwachstellen	Manuelles Ausnutzen von automatisiert/manuell gefunden Schwachstellen	Kreative Teamarbeit, weitestgehend rein manuell unter Einbeziehung des Faktors Mensch
Bedrohungs-Simulation	-------	Punktuell	Advanced Persistent Threat Simulierung
Gefundene Schwachstellen	Oberflächliche Schwachstellen meist durch ausgegebene Versionsnummern erkannt Ziel: Minimalaufwand viele Ergebnisse	Schwachstellen mit erweiterten Angriffsvektoren und nachgelagerte Schwachstellen Ziel: Möglichst alle Schwachstellen in einem dedizierten Bereich zu finden	Schwachstellen mit erweiterten Angriffsvektoren und nachgelagerte Schwachstellen Ziel: Schwachstellen zu finden welche die Erreichung des Ziels zuträglich sind
Abschlussbericht	Vollautomatisiert	Teilautomatisiert, manuelle Nachbearbeitung/ Aufbereitung	Vollständig individuell, zeitliche Reihenfolge als Struktur

Red Teaming

Unternehmenssicherheit



Menschen

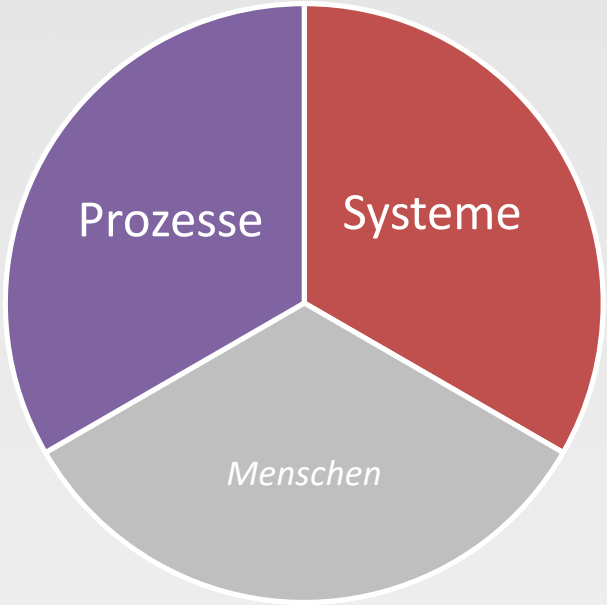

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
copyright 2006 john klossner, www.jklossner.com

Prozesse

Systeme


U.S.
CYBERSECURITY
STOP
Lisa ©2015 6-9 Dist. by Wash. Post Writers Group
Copyright Lisa Benson

Red Teaming Light



let Success_Social_Engineering_Attack = true

→ Simulierte SE Angriffe auf eingeweihten Mitarbeiter, dieser repräsentiert den Durchschnitt und klickt immer.

Vorgehen

1. Initial Reconnaissance – Information Gathering
2. Initial Compromise – Exploiting
3. Establish Foothold – Persistieren
4. Escalate Privileges – Laterale und horizontale Rechte-Eskalation
5. Internal Roconnaissance – Identifizierung der Zieldaten
6. Complete Mission – Zieldaten-Extrahierung

Red Teaming Prozess

Red Teaming: Vorteile für den Kunden

- → Tatsächliche Auswirkungen von Schwachstellen werden sichtbar
- → Schwachstellen in Segmenten welche man für normale Pentests nicht im Blick hat werden aufgedeckt
- → Internes Blue Team wird weiter geschult/getestet
- → Prozesse werden getestet
- → Mitarbeiter werden sensibilisiert
- → Awareness der Mitarbeiter wird getestet
- → Aktive Schutzmaßnahmen werden getestet

Red Teaming: Herausforderungen für den Kunden

- → Social Engineering (SE) kann zur Unzufriedenheit bei Mitarbeitern führen
- → Umsetzung von Funden im Bereich SE
- → Umgang mit den Betroffenen von SE Angriffen
- → Exkludieren von Systemen/Personen Ja/Nein
- → Projektlaufzeiten
- → Umgang mit kritischen Schwachstellen in der Projektlaufzeit
- → Informierter Personenkreis
- → Genehmigungen

Red Teaming: Herausforderungen für das Testteam

- → Ethisches Social Engineering ?
- → Identifikation von exkludierten Personen
- → One –Shot
- → Identifikation von Kundensystemen
- → Breites Knowhow erforderlich
- → Projektmanagement
- → Diverse Testsetups erforderlich
- → Flexibilität/Arbeitszeiten

Highlights Red Teaming

- → VPN Hardwaretoken wurde nach Spear-Phishing Mails zugeschickt
- → In der Kaffee-Ecke sitzen, Kaba trinken und Domänenadministrator werden
- → Wochenlanger Zugriff per RDP was über eine Webshell getunnelt wurde
- → Eine Woche, direkter „Kampf“ gegen das Blue Team

OWASP
Open Web Application
Security Project

Fragen ?

Gerne auch per Mail an:

christoph.ritter@syss.de