

# Gezielter Ausnahmezustand – Penetrationstests

## Cusanuswerk Fachschaftstagung Ingenieurwissenschaften 2023

Jens Liebchen  
RedTeam Pentesting GmbH  
kontakt@redteam-pentesting.de  
<https://www.redteam-pentesting.de>

2. Oktober 2023, Xanten

## RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Unternehmenssitz Aachen



**Wir testen hacken**





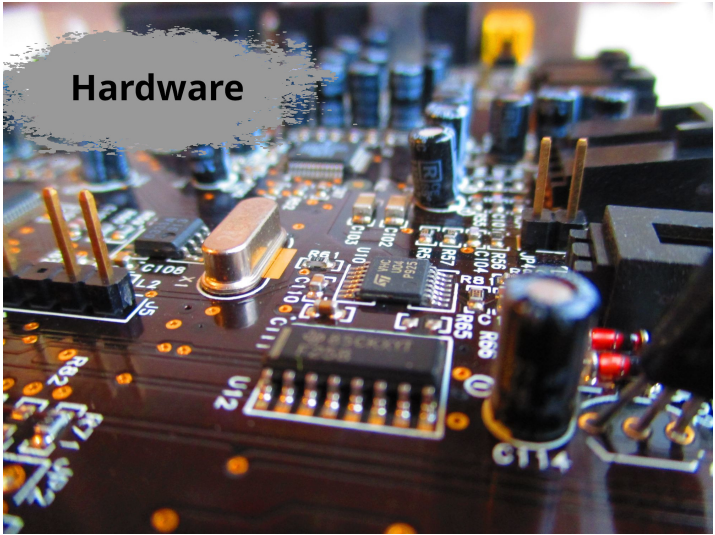
# Webanwendungen





**Apps**







**(Fast) Alles &  
überall...**



# RedTeam Pentesting

## Unser Alltag

Das tun, was man normalerweise nicht darf! Fast alles ist erlaubt!

## Was ist ein Penetrationstest?

- ★ Angriff auf ein IT-System (z.B. Netzwerk oder Produkt) im Auftrag des Betreibers
- ★ Fragestellung: Wie weit können Angreifer vordringen?
- ★ Durchgeführt aus der Angreiferperspektive, gleiche Methoden
- ★ Angriff und keine Simulation!





# RedTeam Pentesting

- ★ Hochspezialisiert durch ständige Durchführung von Penetrationstests
- ★ Unabhängig und objektiv (kein Angebot von Sicherheitslösungen)
- ★ Kreativität! (Teamwork, unkonventionelle Ideen)

## Angreiferperspektive

- ★ Sicherheit muss ein Gesamtkonzept sein, denn Angreifer suchen sich die schwächste Stelle
- ★ Pentester sehen Dinge aus einer anderen Sichtweise
- ★ Wie kann man ein System für eigene Zwecke nutzen/missbrauchen?
- ★ „Was wäre wenn?“



# Beispiel aus dem ÖPNV

★ Was sehen Sie hier?



# Beispiel aus dem ÖPNV

- ★ Was sehen Sie hier?
- ★ Was sieht ein Angreifer hier?
- ★ Wie kritisch sind die Anzeigetafeln im ÖPNV?



# Beispiel aus dem ÖPNV

- ★ Was sehen Sie hier?
- ★ Was sieht ein Angreifer hier?
- ★ Wie kritisch sind die Anzeigetafeln im ÖPNV?
- ★ Was würde in einer Stadt passieren, wenn alle Anzeigetafeln vor einem Amoklauf warnen und die Bevölkerung auffordern, die Stadt schnellstmöglich zu verlassen?



# Beispiel aus dem ÖPNV

Thesen | Wetter | Newsticker | RSS-Feeds | Spiele | N24-Mobil-Portal |

**N24** | NACHRICHTEN | SPORT | WISSEN |

POLITIK | PANORAMA | WIRTSCHAFT | NETZWELT | N24-NETZREPORTER | WISSENSCHAFT

Start > Nachrichten > Panorama > San Francisco warnt vor Godzilla-Angriff

Anzeigetafel gehackt

## San Francisco warnt vor Godzilla-Angriff



Diese Anzeigetafel warnte Autofahrer vor dem Film-Monster Godzilla. (Foto: Twitter)

In San Francisco hat sich ein Unbekannter an einem Verkehrsschild zu Schaffen gemacht. Statt vor Stau warnte dieses kurzzeitig vor dem Riesenmonster Godzilla. Steckt ein Werbegig dahinter?

Abbildung: [N24.de, 18. Mai 2014]

DONERSTAG, 05. JAN. 2009

 Merkur-Online.de

Menu | Multimedia | Gehackte Straßenschilder warnen vor Untoten



Achtung vor freilaufenden Zombies: In Austin haben sich Hacker einen Spaß erlaubt. © Screenshots: rebelcat.net

Aktualisiert: 30.01.2009 - 15:18

## Achtung Autofahrer: Zombies in Austin

Straßenschilder in Austin haben in dieser Woche vor Zombies gewarnt. Wer die Anzeigetafel manipuliert hat, ist unbekannt.

Abbildung: [Merkur-Online.de, 30. Januar 2009]

## Beispiel für Kritische Infrastrukturen

Aus der Angreiferperspektive:

- ★ Atomkraftwerk
- ★ Kohlekraftwerk
- ★ Pumpspeicherkraftwerk



# Katastrophenschutz?

Auch im Katastrophenschutz spielt IT eine Rolle:

- ★ Leitstellen-IT, Digitalfunk (TETRA), Sirenen...
- ★ Informations-/Warnsysteme wie NINA, Katwarn, MoWaS...
- ★ Steuerungs- und Automatisierungstechnik
- ★ Systeme für den Aufbau von Ad-hoc-Infrastruktur
- ★ ...



# Warum überhaupt Penetrationstests?

# Warum überhaupt Penetrationstests?



## Warum überhaupt Penetrationstests?

- ★ Realistischer Angriff statt Checkliste
- ★ Versteckte Schwachstellen identifizieren
- ★ Trainieren, um Angriffe überhaupt zu verstehen
- ★ Sichtweise von Angreifern in die Arbeit von abwehrenden Teams integrieren
- ★ Verschiedene Ebenen des Unternehmens an einen Tisch bekommen und Entscheidungen für die Zukunft gemeinsam finden

## Penetrationstests?

- ★ Die Ergebnisse von Penetrationstests sind oft kritischer, als die meisten glauben
- ★ Wir sehen hinter die Kulissen
- ★ Wir liefern die Grundlagen für kritische Geschäftsentscheidungen
- ★ Wir begleiten unsere Kunden in absoluten Ausnahmesituationen
- ★ Aber kaum jemand redet über Penetrationstests...

# Diskussion



# Diskussion



<https://www.redteam-pentesting.de>

<https://blog.redteam-pentesting.de>

<https://jobs.redteam-pentesting.de>