HanseSecure

Exploit Hunter

# Weniger Cyber, mehr Grundlagen

## Alles halb so wild ;-)

vom 29.04.2021

# Inhaltsverzeichnis

1. Wer
2. Warum
3. Was

# 1. Wer

# Wer

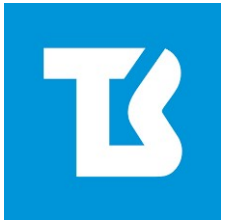
- 21 CYBERSECURITY TWITTER ACCOUNTS YOU SHOULD BE FOLLOWING

  (https://www.sentinelone.com/blog/21-cybersecurity-twitter-accounts-you-should-follow/)

*“Florian is a redteamer, pentester and exploit hunter, as well prolific tweeter and blogger. @HanseSecure is one of the best sources for tweets and retweets of technical write-ups, links to scripts, plug-ins, exploit kits and other new tools, along with how-to’s and tips for anyone interested in redteaming and pentesting.”*

- Modern red teaming: 21 resources for your security team

  (https://techbeacon.com/security/modern-red-teaming-21-resources-your-security-team)



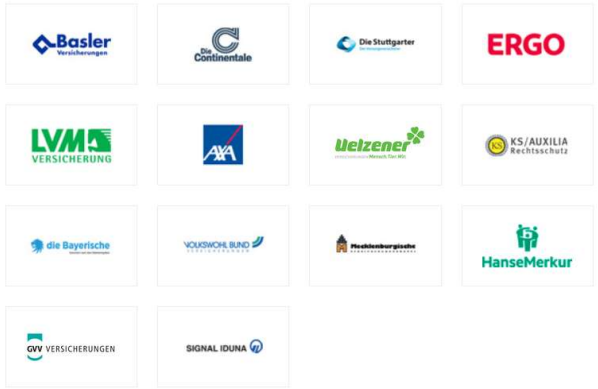
*“Hansemann is an ethical hacker and penetration tester. His tweets and blog focus on tools and techniques of interest to red team members. For example, he covers Tokenvator—a tool to elevate privilege with Windows tokens—and how to write a payload for process injection in Windows.”*

# Wer

- Über **25.000** Follower auf Twitter

  95% der Top 100 Security Experten folgen @CyberWarship

- *Speaker, z.B. „IT-Sicherheitsmanagement in Versicherungen“*




- KeyNote Speaker, z.B. auf der ISX2021
- Speaker at Best of The World in Security 2021

# Wer

- Disclosure CVE-2020-13912
  (https://hansesecure.de/2020/06/vulnerability-in-monitoring-software/?lang=en)

- Microsoft SmartScreen Bypass
  (https://hansesecure.de/2019/05/smartscreen-bypass/)

- Disclosure CVE-2018-7272
  OpenAM Unauthorized Access
  (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7272)

- Disclosure CVE-2018-16231
  Remote DoS in Personal FTP-Server
  (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16231)

- Intel Vulnerability
  (https://hansesecure.de/2019/05/intel-unquoted-service-path/)

- Artikel: IT-Sicherheit professionell unter die Lupe nehmen
  (https://www.security-insider.de/it-sicherheit-professionell-unter-die-lupe-nehmen-a-852288/)

# 2. Warum

# Warum

Das FBI hackt infizierte Exchange-Server und entfernt Hintertüren - ohne Zustimmung der betroffenen Unternehmen. Mit der Begründung, dass es die Unternehmen selbst wohl nicht können. Der ungefilterte Wah ... mehr anzeigen


**FBI nuked web shells from hacked Exchange Servers without telling owners**

bleepingcomputer.com • Lesedauer: 3 Min.

Schlagzeilen

DER SPIEGEL

Daten von 530 Millionen Nutzern veröffentlicht: Bundestag warnt Abge…

vor 4 Stunden

Tagesspiegel Background

Facebook-Leak, SMS-Spam: So schützt man sich

vor 9 Stunden


it-daily.net

Facebook Datenleak: Das steckt hinter dem Angriff

vor 7 Stunden

Die Sicherheitslücken und der Trubel um #Hafnium sind noch nicht lange her, da gibt es schon die nächsten Sicherheitslücken in #Microsoft #Exchange.

... mehr anzeigen

⚠ Gefälschter Zoom-Download (ZoomPortable.exe). Angreifer haben hier die legitime Zoom-App manipuliert. Man kann Zoom installieren und starten. Allerdings verbindet sich die App dann mit der Infrastruktur der ... mehr anzeigen

# Warum

# 3. Was

# Was

Next Generation Firewall

Advanced Threat Protection

KI


0Day-Schutz

BlockChain

AI

# Was

# Was

- **Assetmanagement**
  Wo und wie ist dieses gespeichert? -> Excel Tabellen ist nicht die beste Antwort ;-)

- **Patchmanagement**
  Wie wird der Patchstand der Systeme überwacht? Wie und wie oft wird Drittanbietersoftware [nicht Microsoft] gepacht? Was ist mit den Systemen, welche nicht in der Domain sind?

- **Office Macros**
  Können Macros deaktiviert werden?

- **Email Security - Spoofschutz/ Awareness**
  Wird SPF, DKIM oder/und DMARC* genutzt?
  Wann war die letzte Mitarbeiterschulung?

# Was

- **Administrator-Rechte**
  Kann ich selber Software installieren? -> oh Gott xD

- **Laptops**
  Verschlüsseln wir die Festplatten? -> Nein = unnötige Gefahr (zumal die Lösung kostenfrei ist…)

- ***Backups***
  Von was und wie oft werden diese durchgeführt? Wie oft wird die Herstellung überprüft? Gibt es einen Schutz vor Ransomware?

HanseSecure

Exploit Hunter

# Danke für Ihre Zeit!


**Florian Hansemann**

Principal Security Consultant

Web hansesecure.de
Mail info@hansesecure.de
Twitter @CyberWarship