



#digitalsicher

**AKTIONSTAG: DIGITALE SICHERHEIT IM BETRIEB**

# **SESSION: HACKERANGRIFFEN AUSWEICHEN**

**– WIE SIE SICH ,UND IHRE KOLLEGEN GEGEN CYBERANGRIFFE WAPPEN**

**NRW, 11. MAI 2022, 09:20 – 10:00 Uhr**



**DIGITAL  
SICHER  
NRW**

Kompetenzzentrum für  
Cybersicherheit in der Wirtschaft

Beauftragt vom

Ministerium für Wirtschaft, Innovation,  
Digitalisierung und Energie  
des Landes Nordrhein-Westfalen



A person wearing a grey hoodie is sitting at a desk in a server room, working on a laptop. The room is filled with server racks and multiple computer monitors. The lighting is dim and blue-toned. In the foreground, there are several overlapping orange circles of varying sizes. The text 'Certified Ethical Hacker (CEH)' is centered within the largest of these circles.

Certified  
Ethical Hacker  
(CEH)



## The Ultimate Ethical Hacking Certification

Demanded by **Employers**. Respected by **Peers**.



„Um digitale Angriffe durch Hacker zu bekämpfen,  
muss man wie ein Hacker denken.“

# ANGRIFFSZIELE IN IHREM UNTERNEHMEN:



- Diebstahl sensibler Daten
- Kundendaten zum Verkauf
- Ransomware / Erpressung



**WIE ERFOLGT EIN HACKINGANGRIFF**

**AUF IHR UNTERNEHMEN?**



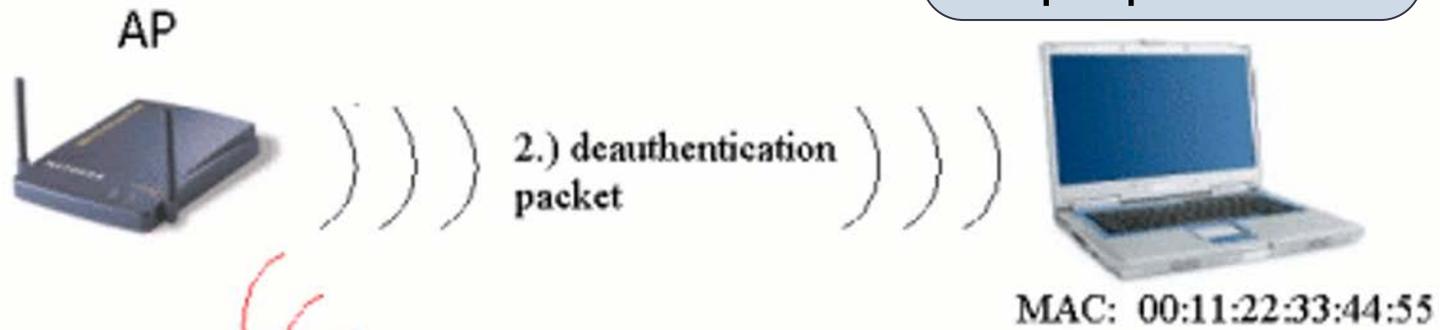
- **Guest WLAN**

**Autohaus WLAN gesichert**

WPA2 verschlüsselt

# DEAUTHENTICATION FLOODING

Mitarbeiter  
Telefone,  
Laptops etc.



1.) deauthentication packet  
MAC: 00:11:22:33:44:55



Wir haben den Handshake aufgezeichnet:

```
sbolinger@kali: ~  
[ 2019-06-06 12:32 ] WPA handshake: 90:61:0C: [REDACTED]  
acons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
95 0 0 3 65 WPA2 CCMP PSK HUAWEI-9B2D_Guest  
79 14 0 3 65 WPA2 CCMP PSK Waldgefluester  
737 654 1 6 270 WPA2 CCMP PSK MagnusHeimdallr  
55 367 17 1 130 WPA2 CCMP PSK SKYbro  
37 4 0 1 270 WPA2 CCMP PSK PL  
49 4 0 11 130 WPA2 CCMP PSK SKYbro  
18 0 0 1 270 WPA2 CCMP PSK PALO  
8 0 0 9 130 WPA2 CCMP PSK PL  
62 1 0 6 195 WPA2 CCMP PSK DN8245W_FC064  
21 3 0 6 130 WPA2 CCMP PSK PL  
  
PWR Rate Lost Frames Probe  
E: [REDACTED] -74 0 - 1 0 18 SKYbro  
B: [REDACTED] -76 0 - 1 0 2  
7: [REDACTED] -38 0 - 1 34 43 MagnusHeimdallr  
C: [REDACTED] -24 0e- 6e 893 935 MagnusHeimdallr
```

loading packets, please wait...

Aircrack-ng 1.2 rc4

[07:04:13] 11977037/92621076 keys tested (102.05 k/s)

Time left: 9 days, 3 hours, 37 minutes, 7 seconds

12.93%

KEY FOUND! [ XXXXXXXXXX ]

Master Key : 8B 4D AD 42 C6 93 67 BC 4C D3 94 BE 47 5D 49 CA  
6C 75 FC B1 98 B4 29 C3 2A 56 4F 1E C0 78 4C 7D

Transient Key : 69 18 1E 80 BC 13 4F E3 88 A9 B8 C9 90 7C 6F 91  
72 95 3A 5F 3F 27 F1 8C DB FB 8B EC 04 C2 C1 76  
43 F0 61 A8 EB F2 39 6A 30 3F 07 43 AA BB C9 BA  
3C 71 BA 88 91 E4 32 F3 C4 E6 A9 29 53 93 B0 9F

EAPOL HMAC : 69 E0 52 9B 46 F6 8A 68 5D 9D 8D D7 D2 FF 2A D5

**“AutohausSalinger2015!”**

Netzwerk Scan  
zeigt einen  
Windows 7  
Rechner im Haus.



```
not shown. 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:A7:2F:E1 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cp
:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o
ndows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows
Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vist
ws 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 14.04 seconds
```

Angriff auf den Rechner mit einem Exploit.

Dauer des gesamten Angriffs: ca. 15 Minuten.

```
lWyuua+b1b1tPoZwInPsnGevmbC+MLjTRYES5HoBMUFAoMo+Q+ZnmU+4Pvnb33EZEW91ZNayFjWQUqcWvjUBQUyV/FuFyLPCdp1jHAC
i/CCbmpHye5RUaeOT/G6yPezgzFEfqS2CE8nz9GBt+ab3Pbo9On2MmyGn1h1zTnyZIBOKb0lFqQFbsXCMgCKz4b+iQwIAtv6z1TFMba
:ws6UJEA/4jdrS1390q8q1cwm0J7LYvvQThyzBt61KDPEXm6vBRGz27RY+6ntXFqS901XNREF3kiJnaKwiKzBSbvW1eTXn12Hxt/ghl
'Db+geLNkXIR5T5BDR9ZLdr2sOM5wZXGp7j05EFFFqisVjX0/K0pL4Iqouzo1lthHjFn1SBPugoF/3GhmMyOC9dGo708qzx+v5e9/75
:sFC/8myp//VPLFK0wx2sqA+SGbYLj9KAFveev5vD/PnWgZE3NPwXT0v9b1zeCzhuTc+n7vkxi/pkmUASyTBeHUG7OKTQt2tIQDM5/\
:ct6yWJl1EjUI3ilKrjue2Aj5ZiacGpRap14KEhFRhf1z6wgYJ1Y30axSQKGoHMPFsQ9b4AtTFIbgZtu1QGjftVoq+jdZeAWBfcZ/LI
I7bhyiRKih8FuawqegyYLtSSD18PYKvtSWBFZ+1IZ0pjqqoD7wbqa4ndvpUuOwDftdtG5yGMHbMdZRz/hYv0IAprhi6kBosCdfE9x>
ijeqNVgFLj4gcoEodaKww10cp40uSed7IGV/y6Pzhqv8Buc2VBVG/JzpQkz2ythFc5i2zHpbFcGwTpTtwqF0v7jAHMmj2yg715n1dfv
TPW5Fu2yyXC79YaasImkxc9XSe1u63G3Kx0k3m08drtbhheQf4rm9TDLVqtEM2T2ntB15Hvnk8ThZ4OZ7F6Crnghtqzk0x1Ragnke
z0tP1Smgx1/BEeRB4PkBG6fSuFCOK/wgcDHexCuyeHxoS+jtL/nkN14xTkseSCYMGyDsCzrpDGFEiMeGcXtBW0+R0bqunp4fMyk7U+
rk1k4Pi86uz3z67CY10DIgxoFyA3aws7TdvDv3/boP+qGA0wB+PGXPniC9Tio26P3PFBUSrflGCcxelojkmfYncAAzqDh0rkFo4M0
:KgIr0yqv2/urVgMXg4lXi5Tc4xDdAza+45Nw34PwvxcUPRJngubbsxvbTanJWLQvAd06xU2N8m8jwYA/03hd8ikaIQjT+y43q/zzG1
'Ayg9Wmudfg00HLhT4Gwj/6qLe0ofclkhjY6756JQADkMxKDubmCTL6UGAMoeF2P5GXYQh31cb04n1Cy4Ua3D3Ujjsge5U/YozY6e0c
waVPZT/Z6wow/G8I1aak003Rqo8tL+HqyIHNCrMIu10pDEB+6XPzXqkUhnfptYRzSGsv9Zphi/h/emNfljxamtM6y/iZOx3d49reDT
H+Mpmi+pLq0pC9gJjg38H6PuUZS0UOXlTgbeLnx9u0Tb88vo7ZrVjmdMrehvZ1FI+wiPlgRT3SuVlzz6rgc47pD6M3GvG4Vcm0MOF5V
:h4itLiX009JevudvwLoLUjZ0VzGro8Ufn9G3Av7Eo7nJfLqYBit54HPF9TVXSIEGykkHnt2wuqfQd9FJjmgynvpsRiB3Su4Ez7mmf
.SD8BkuBqEB1Qv0qkv0tfjHa0078kovcdkzbEDY/TpedLxfBJEJcyU6zhyWCzX7zSXX5xc7mhq0BStc0B7aE29Kogtvrf/iRuILJLyI
.wiRXMPcFcgnagGglZBsJbZTG+qoCKDo3NjlIzmJpvnLp7fnZjZyuFP5bjvb4jbfS6s1lRnZh19Fd1f6SdnZSH+Nw8xCL9j4pBj5ok
:PiBVCdq4UuLEawlVXLaZe24FAEdbpDNGJT4Bqt0ArcvXHU0sttU1qsARquD0Zmyf5a9YnByQGTI6rrICRiAFzj1+teNjia2T3ntTME
+JCATd0UyHx13Ks/tCyIA6BBMW6NVg/VLknfFzycPdkZfRLa7WujVqgXhASRXys7xR9677mp37+nEaFdbrrwIiN9hhG6HSJ9Ykv6ts
:zonnJHpp2GhLf8Fvkvx7NZw1ak/7U6
'Ajs/FsgXHmK7+ftt tNsOpte/9xnTsmE
ibYE7lyIid/n0yn93 jwnYGpwQyKfLxLc
:TOJBly3IuPXETYS5 cQyps2dyg3eCy3s
:R/vo8ye+4HPMLshv iADFPjPvhc6kkke
Ivd5TF571b42TK263 +PL7HSy7v155SFy
'fk86q06AyaIb1vrj09dV5TzjL6XyygF4xiYjlgxkMCuyQZ9/d5ehMUPLo4c4hIXAXUKHFUUVHvtXv2qdhbEGn1VycsYP9jrmxfqNnyI
i6e8vtLynWmJ2sdoR141lhZYP9TgwJF00K2pCeQo4c8VpdtZNeqdUaYPT3LtnJm17kAaf0Fg9iXoKqnvoYmBg1NGUUTqHTK30xi2frs
Pw8tCglH+QuqY/blmWgsAoFF835uZrmyCS7z9WNSfa0RptYkiZS6J6/RRtUmqHiKu8utg56F1Tcheko1B9umUgfga4Udm4QS90oZHF
M3+6yLRTTrQXToXNDzLuqixNB7N1kUC+5vI/CxgGeZuzcuEGWv9Sb0ofr4DcdRoYtQQY1wvQmfki1QrCTMwDBiWc1qx+4tdgV4g4k6A
'nxf/Ga/ov1YwocGd0YkrDow8NhTnsriKH0i7XaRvz9azrFm1BoP7uH7uKU/19Sa/imwvvtuGrf1sfv0wtMR078R8811H8v0fai+af
```

**RANSOMWARE**

# WIE ERFOLGT EIN HACKING-ANGRIFF AUF IHR UNTERNEHMEN?

● Unsichere IT / Webserver / Netzwerke

● 68 - 93 Prozent der erfolgreichen Angriffe sind auf ein Fehlverhalten durch unwissende Mitarbeiter zurückzuführen

# TÄUSCHUNG DER MITARBEITER

- Übernahme von Mailkonten / Identitätsdiebstahl
- Gefälschte Portale
- Einschleusen von Trojanern durch infizierte Dateien wie PDF, EXCEL oder WORD Dokumente



**SPOOFING**



# SPOOFING

[www.paypal.com](http://www.paypal.com)

# SPOOFING

www.paypal.com

# SPOOFING

www.google.de

# SPOOFING

www.google.de

**ABWEHR-  
MASSNAHMEN**



# UNSICHERE IT / WEBSERVER / NETZWERKE

Abhilfe:

- Fest eingestellter IT Administrator
- geschultes Personal im IT Bereich
- Vertrag mit einem externen IT Dienstleister
- Intrusion Detection Systeme
- aktuelle Betriebssysteme / Firewall / Security Gateway etc.

# **68 - 93 PROZENT DER ERFOLGREICHEN ANGRIFFE SIND AUF EIN FEHLVERHALTEN DURCH UNWISSENDE MITARBEITER ZURÜCKZUFÜHREN**

## Abhilfe:

- Awareness Schulungen des GESAMTEN Personals
- Sichere Passwort Politik
- Regelmäßige Kontrolle des Mitarbeiterverhaltens (Weblogs etc.)
- Verwendung einer Sandbox zum Öffnen von PDFs etc.

Nur **regelmäßig geschulte** und **aufmerksame** Mitarbeiter können diese Angriffe erkennen und vermeiden / melden.

# Security Awareness



**WIE LÄSST SICH DIES UMSETZEN?**

# 1. DIE GESCHÄFTSFÜHRUNG MUSS DAS PROBLEM ERKENNEN



Nur wenn die Geschäftsführung die Gefahren erkennt und dem Thema eine hohe Priorität gibt lassen sich Prozesse verändern

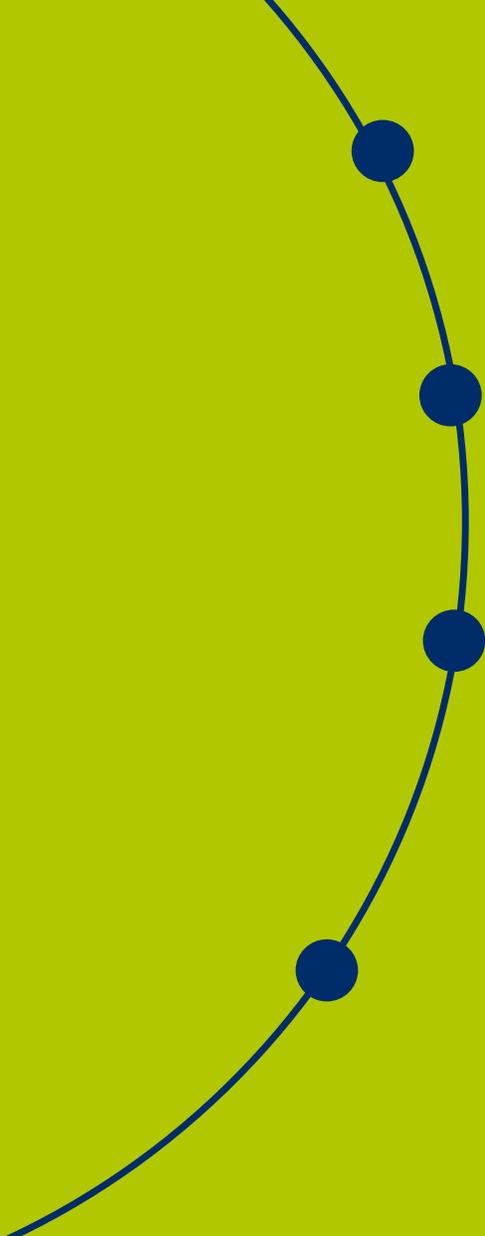
## 2. ERNENNEN SIE EINEN VERANTWORTLICHEN



Dieser Person muss der “Rücken gestärkt werden”, in Form von Zeit für Schulungen, Zeit zum analysieren von Prozessen, Zeit für Awareness - Trainings.

Ca 30% der Arbeitszeit sollten als “unproduktiv” für diese Person eingeplant werden.

### 3. AWARENESS ALS PROZESS ANSEHEN



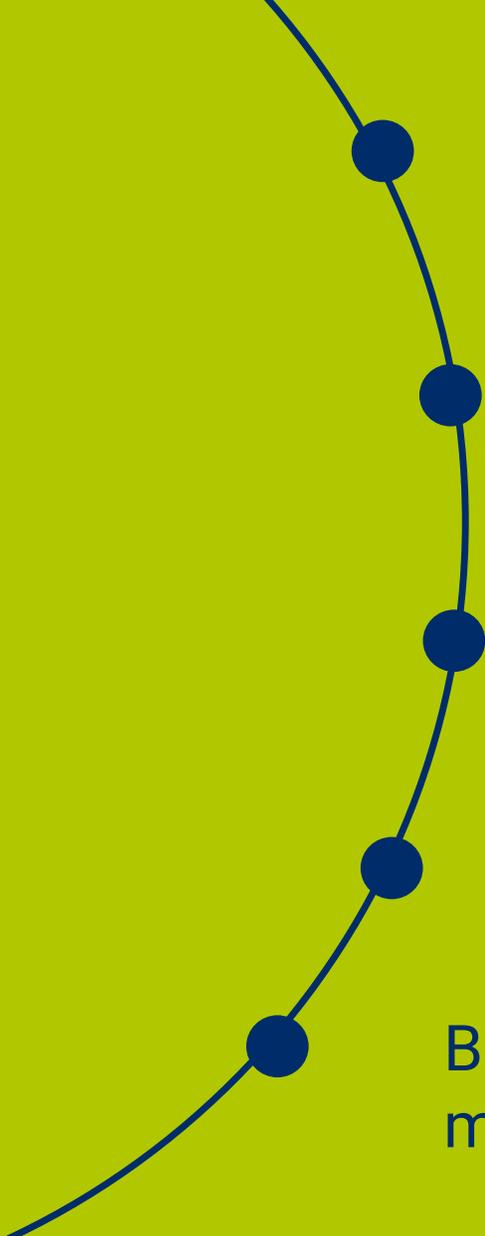
Basis für Verständnis für das Thema bei den Mitarbeitern schaffen und auf Dringlichkeit hinweisen

Beispiele von erfolgreichen Hacking Angriffen aufzeigen

Erklären, warum Awareness ein wichtiges Thema für jeden Einzelnen ist und wie die Trainings aussehen werden

Mitarbeiter einbeziehen: Wie fühlen sie sich mit den Trainings? Wie kann man Hilfestellungen geben um Stress zu vermeiden?

## 4. MITARBEITER MITNEHMEN / ABHOLEN



Alle Mitarbeiter sollten mind. einmal pro Quartal geschult werden

Vorstellung neuer Attacken und Phishing Methoden durch Beauftragten

Regelmäßiges Versenden von Phishing Mails zur konstanten Überwachung des Mailverkehrs

Tipps für den privaten Gebrauch geben

Beraten, nicht belehren. Bleiben Sie auf Augenhöhe mit ihren Mitarbeitern

## 5. FEHLERKULTUR LEBEN



Es ist okay wenn Fehler gemacht werden. Davor muss niemand Angst haben - im Gegenteil. Desto eher ein Fehler gemeldet wird, desto schneller kann man eingreifen.

Belohnungssystem für das Finden von Fehlern einführen

Querverweise zu privatem Datendiebstahl (Facebook, Instagram etc.)

und eventuellen Folgen für den Betrieb (Social Engineering)

## 6. INFORMATIONSMATERIAL BEREITSTELLEN



Anleitung für Homeoffice mitgeben

Checkliste für Konfiguration heim W-LAN mitgeben, mit den Mitarbeitern gemeinsam durchgehen und Unterstützung bei der Umsetzung anbieten