AKTIONSTAG: DIGITALE SICHERHEIT IM BETRIEB

SESSION: HACKERANGRIFFEN AUSWEICHEN

– WIE SIE SICH ,UND IHRE KOLLEGEN GEGEN CYBERANGRIFFE WAPPNEN

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


Certified
Ethical Hacker
(CEH)

„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

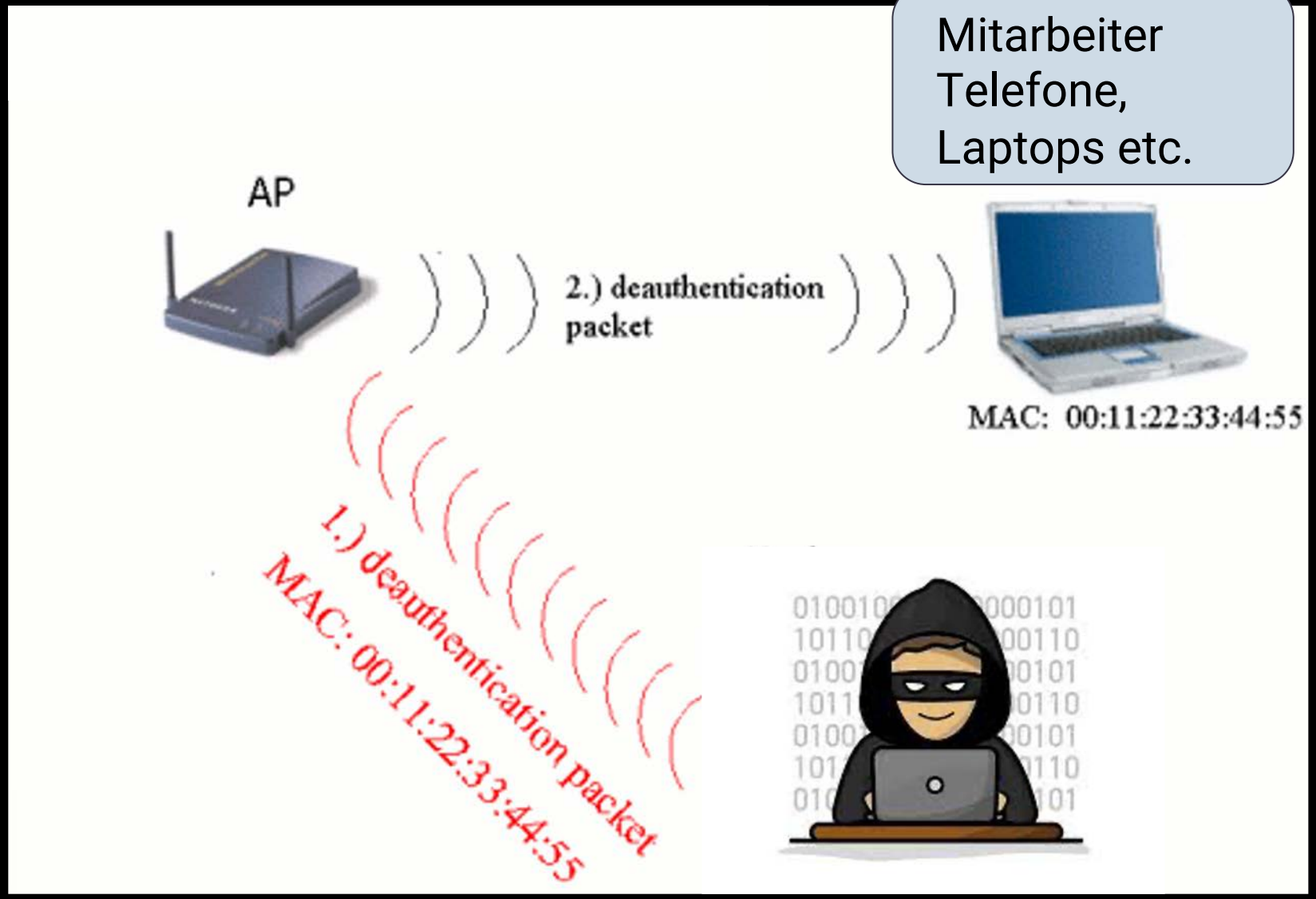
WIE ERFOLGT EIN HACKINGANGRIFF AUF IHR UNTERNEHMEN?

- **Guest WLAN**

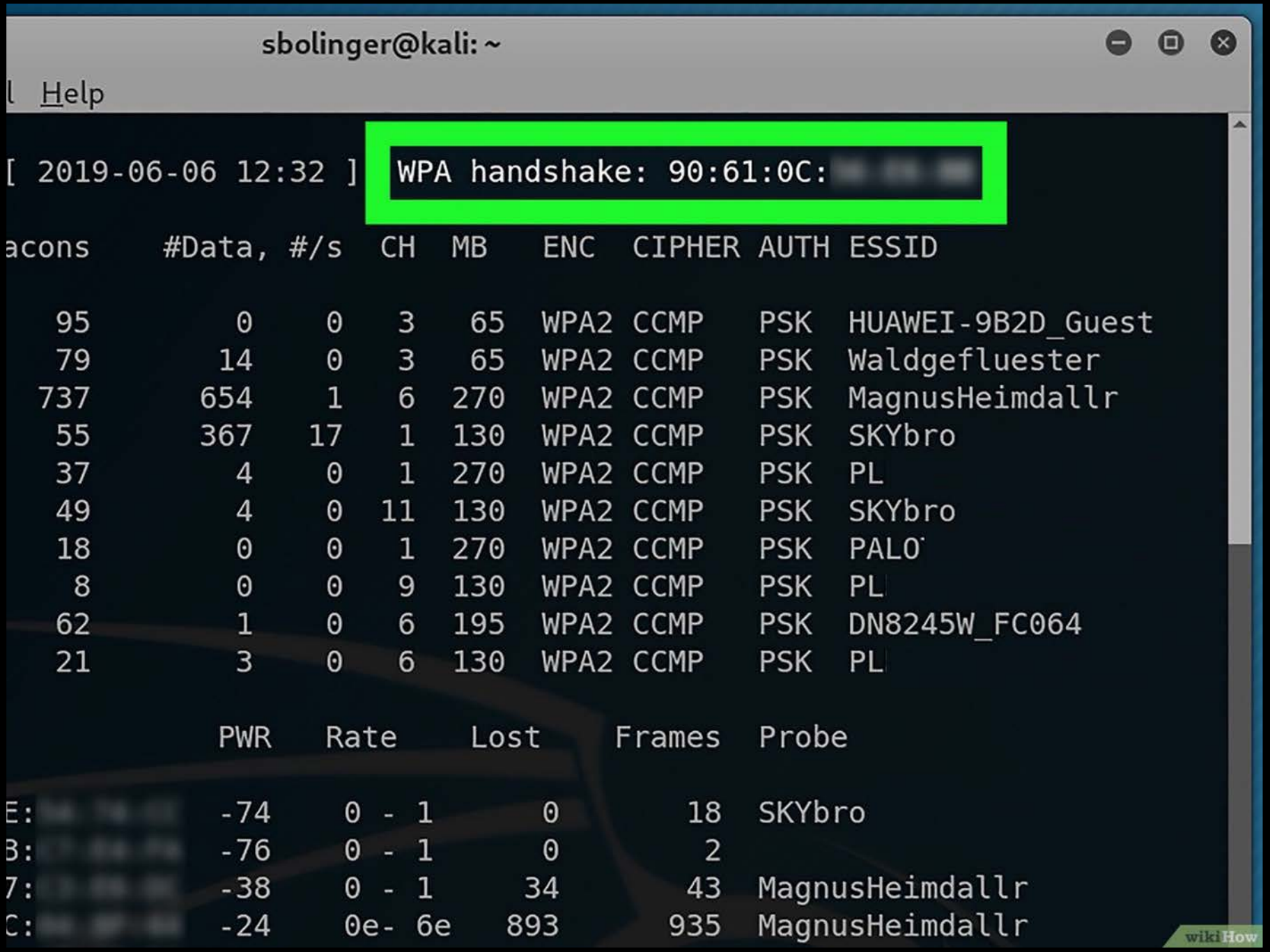
Autohaus WLAN gesichert

WPA2 verschlüsselt

DEAUTHENTICATION FLOODING



Wir haben den Handshake aufgezeichnet:

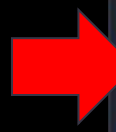


Command Prompt

```
eading 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! [ [redacted] ]


     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: 993 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  icslap
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.

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

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.

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