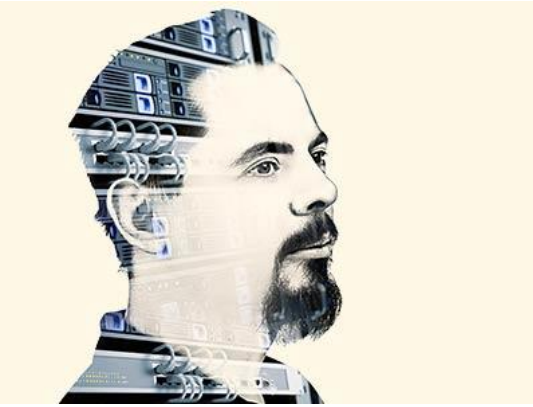
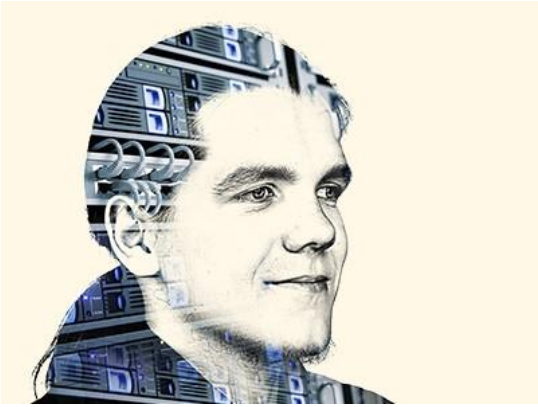
IT-Sicherheit

Über uns



Timo Klein (34)
- Student im Fachbereich Praktische Informatik
- Hilfsarbeiter in der Firma KFK GmbH
- Tätigkeitsbereich: Pentester, Techniker

Hobbys:
- Musik
- Computer
- Filme und Serien
- Lesen



Marcel Schmidt (21)
- Ausbildung zum Fachinformatiker
  im Fachbereich Systemintegration
- Tätigkeitsbereich: Pentester, Techniker

Hobbys:

- Literatur
- Gitarre

KFK

IT von Mensch zu Mensch.

Agenda

- Rechtliche Belehrung
- Intention
- Schematischer Netzwerkaufbau
- Vorgehen
- Mittel und Dauer
- Sicherheit versus Kosten
- Wettlauf zwischen Hersteller und Hacker
- Digitale Spuren hinterlässt jeder
- Social Engineering
- Wifi
- Botnetze/Trojaner und Co
- KFK-QuickCheck / AdvancedCheck
- HP Security Tools

- Q & A

Rechtliche Belehrung

- Straftaten nach Strafgesetzbuch („Hackerparagraph“) sind:
  - §202a Ausspähen von Daten
  - §202b Abfangen von Daten
  - §202c Vorbereiten des Ausspähens und Abfangens von Daten

  Diese werden mit Freiheits- und/oder Geldstrafen verhängt

- Unsere Absicht ist das Aufzeigen von Schwachstellen im System, ohne böswilligen Absichten (Ethical Hacker)

Intention

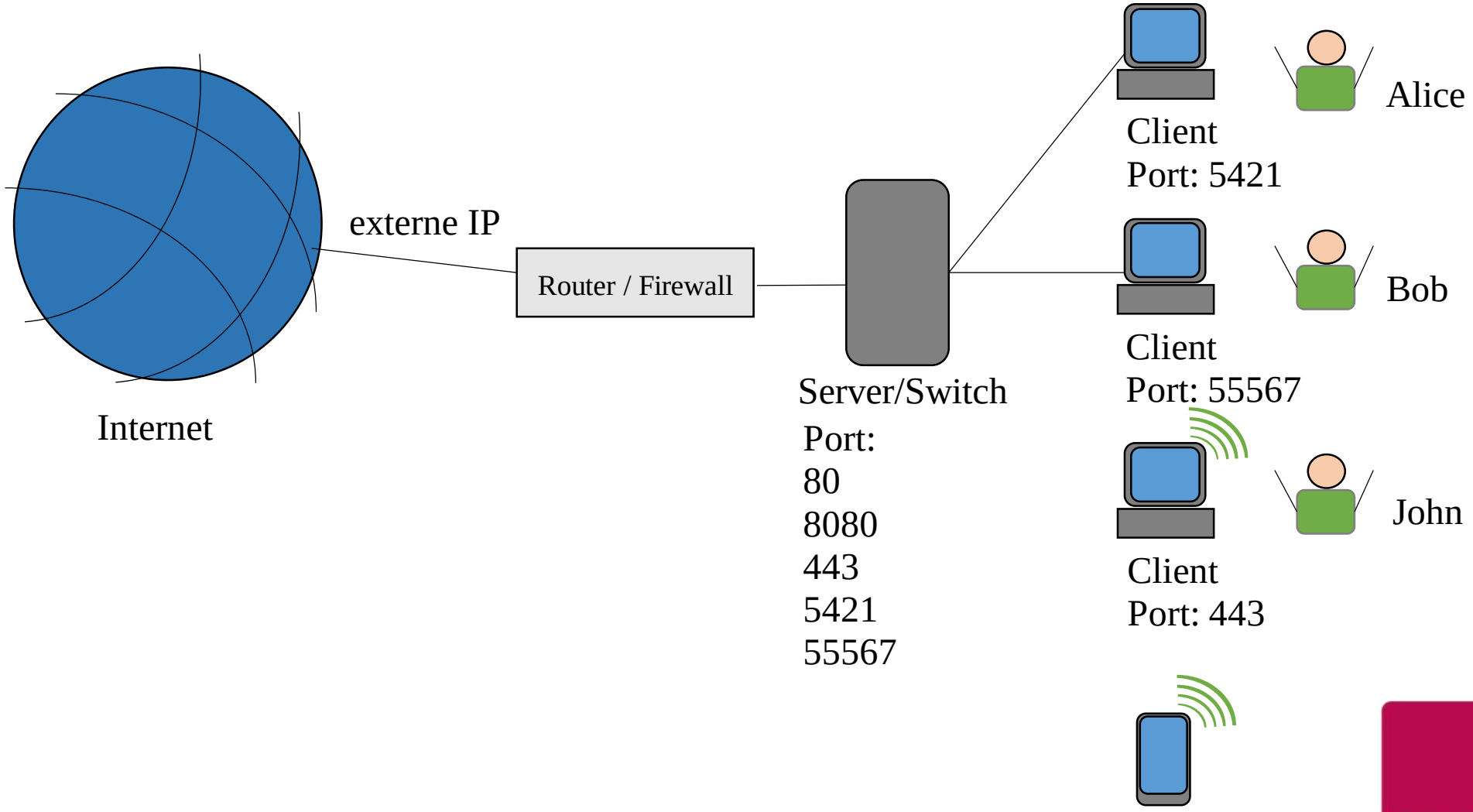
- Schwachstellen und Lücken in der verwendeten Hard- und Software aufzeigen
  - Software nicht regelmäßig aktualisiert
  - Hardware nicht mehr zeitgemäß

- Mitarbeitersensibilisierung
  - Keine Datenweitergabe, besonders nicht über Telefon und Email
  - Identitätsdiebstahl

- Datenschutz verbessern
  - durch Mitarbeiterschulung
  - Welche Daten sind sensibel?
  - Welche Daten sollen / dürfen an die Öffentlichkeit?

- Gegenmaßnahmen einleiten
  - Software / Firmware aktualisieren
  - Sicherheitslücken beheben
  - Sicherheitsstrategien entwickeln

Schematischer Netzwerkaufbau



Angriffsansätze

- Whitebox
  - Interne Informationen / Strukturen sind bekannt
    z.B. externe IP, Firewall, Anzahl der Clients, …

- Blackbox
  - Informationen müssen erst recherchiert werden
    z.B. über Facebook, Google und Co. , …
- Greybox
  - Informationen sind teilweise bekannt
    z.B. verwendete Software, interne Strukturen, …

- Social Engineering / Social Hacking
  - Ausspähen von Mitarbeitern
  - Anwendung von psychologischen Methoden zur Informationsbeschaffung

Vorgehen

- Koordination mit den betroffenen Abteilungen
  - durch den Angriff kann es zu einem Neustart der Hardware / Software kommen
  - Zeitliche Abstimmung des Pen-Test
  - während des Pen-Test müssen zuständige Mitarbeiter der IT-Abteilung erreichbar sein

- Angriffsvektor
  - welche Systeme sollen / dürfen nicht getestet werden
  - welche Angriffsstrategien sollen zum Einsatz kommen (Whitebox, Blackbox, Greybox)

- Pen-Test
  - Angriff auf die Systeme

- Nachbesprechung
  - gefundene Schwachstellen / Sicherheitslücken erläutern
  - Konzepte erarbeiten, um das System vor Angriffen zu schützen

Mittel und Dauer

- Dauer
  - ist abhängig von Anzahl der Mitarbeiter / Komponenten und Sicherheit der IT

- Tools
  - Boardmittel des Linuxkernels (z.B. ping, traceroute, arp, whois, …)
  - nmap
  - Metasploit
  - Wireshark
  - Aircrack
  - firmeneigene Skripte und Software
  - Geolocator

- Analyse und Auswertung
  - gesammelte Informationen werden auf sicherheitsrelevante Punkte überprüft und aufarbeitet
  - Erstellung eines Prüfberichtes (dokumentieren, dokumentieren, dokumentieren)

Sicherheit versus Kosten

- Hardware- und Softwarehersteller
  - starker Konkurrenzkampf
  - Zeitplanung
  - kostengünstiges Produkt
  - Bedienerfreundlichkeit
  - Sicherheitsstrategie

Beispiel:

IP-Kameras, deren Software/Firmware nicht mehr vom Hersteller aktualisiert werden

Wettlauf zwischen Hersteller/Entwickler und Hacker

Sicherheitslücken (Exploits) in Software / Hardware

- fehlende Abfragestrukturen
- unerwartete Zustände
- Fehler in der Software- / Hardwarearchitektur

Wird eine Sicherheitslücke in einer Software gefunden, dauert es in der Regel Monate bis sie geschlossen wird. Manche Sicherheitslücken benötigen Jahre bis sie behoben werden und in seltenen Fällen ist es nicht möglich Sie zu schließen.
Wird eine neue Sicherheitslücke gefunden und wurde sie noch nicht gemeldet, nennt man diese Zero-Day-Expoit. Da die Reaktionszeiten der Hersteller / Entwickler sehr hoch sind, lassen sie sich durch Hacker hervorragend ausnutzen.

Digitale Spuren hinterlässt jeder!

- Jeder Internetnutzer hinterlässt im World Wide Web digitale Spuren
  - IPv4 / IPv6-Adresse
  - Cookies / Trackingcookies und Trackingpixel
  - Browserdaten
  - Betriebssysteminformationen
  - Bildschirmdaten
  - GPS-Daten (Smartphone)

Diese Daten fallen ohne das zutun des Internetnutzers an.

Alle Datenpakete werden über den Hauptknotenpunkt DE-CLIX in Frankfurt geleitet.
Seit 01.01.2017 darf der Bundesnachrichtendienst in diese Pakete reinschauen (Deep Packet Inspection) und speichern.

Social Engineering / Social Hacking

Social Engineering
- Eine Sammlung von psychologischen Tricks, die dem Angreifer ermöglichen das Verhalten von Menschen (zu seinem Vorteil) zu beeinflussen

Mögliche Formen des Social Engineerings:
- Ausspionieren des Anwenders
- „Visual Hacking“
- Kontaktaufnahme über Social Media
- Identitätsdiebstahl in sozialen Netzwerken
- Vorgaukeln einer Autoritätsposition
- …etc

WiFi

WiFi-Jamming

- Stören des WLAN-Signals, um das WLAN-Netz zum Absturz zu bringen

WiFi-Hacking (AirCrack)

- Sobald das WLAN-Passwort entschlüsselt ist hat der Angreifer drahtlosen Zugang zum firmeninternen Netz

ManInTheMiddle

- Der Angreifer-PC gibt sich als Router aus und fängt somit sämtliche Kommunikation zwischen den Anwendern, dem Server und dem Internet ab

Botnetze, Trojaner und Co

- Trojaner / Ransomware
  - Ausspähen
  - Verschlüsselung
  - Erpressung

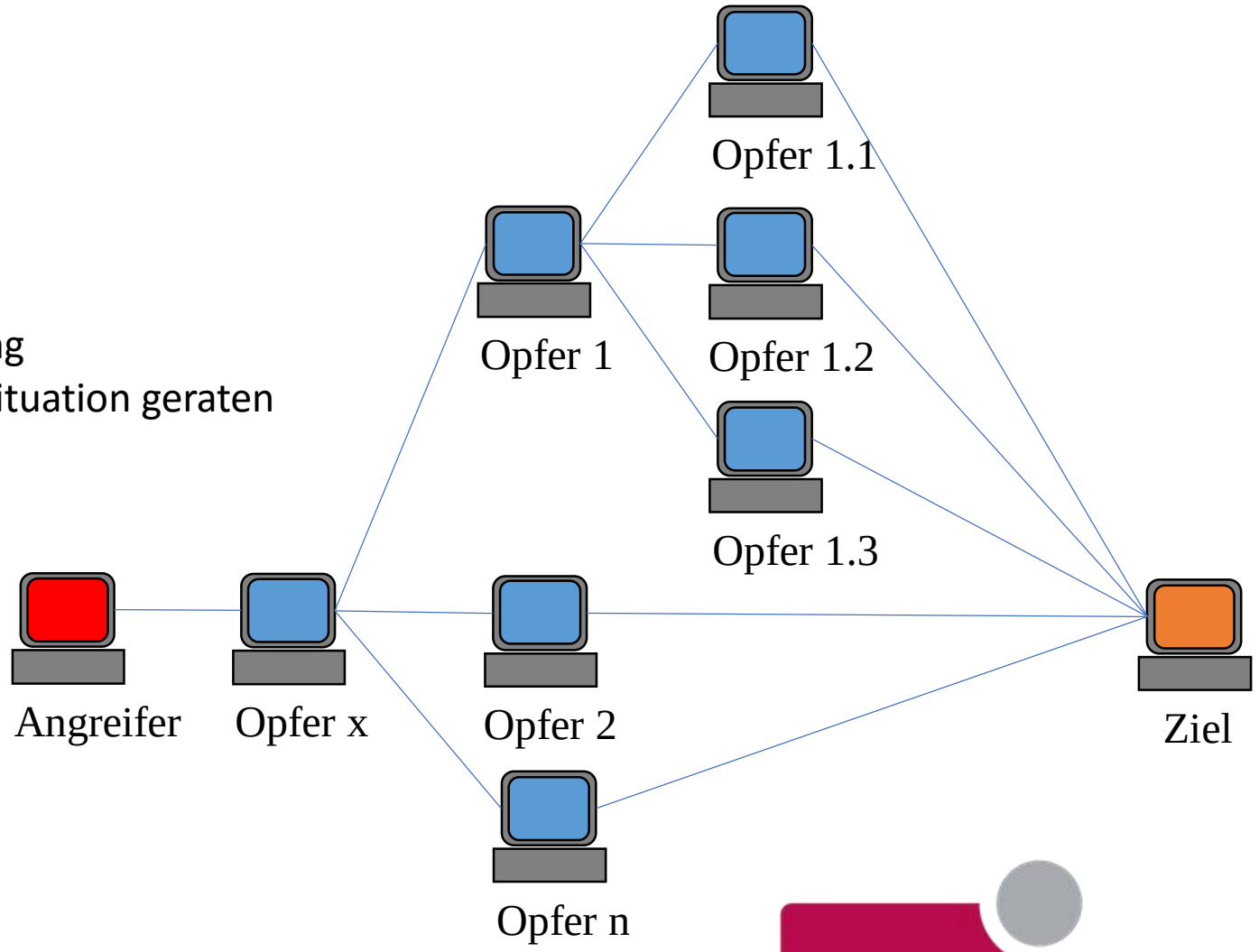
Die Abbildung zeigt den sogenannten „Bundestrojaner“, welcher genutzt wurde, um ahnungslose Anwender zu erpressen

KFK

IT von Mensch zu Mensch.

Botnetze, Trojaner und Co

- Botnetze
  - Angreifer-Identität wird verschleiert
  - Netzwerk von gekarperten Opfer-PCs
  - viel Rechenleistung steht zur Verfügung
  - Opfer können in eine unangenehme Situation geraten



Wie schütze ich mich?

Der KFK QuickCheck und AdvancedCheck

QuickCheck
- passive Analyse
- 100 Punkte Auswertungssystem
- eigene Scripte (ca. 700 Zeilen Code)
- modular erweiterbar
- Auswertung zusammengefasst in einem Prüfbericht

AdvancedCheck
- simulierter Angriff auf Ihr IT-System
- mehrstufige maßgeschneidert
- moderne Angriffsstrategie

HP Client Security

- HP Multi-Factor-Authenticate
  - Um Zugang zu dem System zu bekommen wird nicht nur ein Benutzername/Passwort abgefragt, sondern mindestens ein weiterer Faktor (PIN, Fingerabdruck, etc)
- HP SpareKey
  - Dienstprogramm, um verlorene Systemkennwörter wiederherzustellen
  - Abfolge von 3 zuvor festgelegten Identifizierungsfragen
- HP Device Access Manager
  - Ermöglicht das Abschalten auf Hardwareebene von Geräten

HP Security Tools

- HP Image Assistant
  - Abgleich/Analyse von Images
  - Empfehlungen für
    - BIOS-Version
    - Treiber
    - Software
- HP Secure Erase
  - Ermöglicht das schnelle und sichere Löschen von Speichermedien
- HP Sure Start Gen3
  - Sicherheitsmechanismus auf BIOS-Ebene
  - Überprüft das HP-BIOS auf Manipulation und flasht OriginalBIOS – automatisch („Selbstheilendes BIOS“)

LIVE-DEMO

Question and Answer

Danke!

TKL und MSC

Nächster Workshop

01.06.17 – Alexander Huckert
WLAN: Troubleshooting / Ausleuchtung

IT von Mensch zu Mensch.