# IT-Sicherheitskurs – Tag 2

VORTRAGENDER:
GR Thomas Rupprecht, B.Sc

# Über mich

- Thomas Rupprecht. B.Sc
- 27 Jahre
- Gemeinderat seit 2015
- Schule: HTL Mödling → FH Wr. Neustadt
- Webentwickler
- Hobbies: Programmieren, Feuerwehr, Tanzen, Politik
- Großes Interesse für IT-Security

# Agenda – Tag 2

- Social Engineering & Phishing
- Privatsphäre & Datenschutz / DSGVO
- Überwachung
- Tor & Darknet
- Botnetz & DDoS
- Sichere Kommunikation
- Sicheres Surfen
- Kinderschutz

# Disclaimer

Nicht alles ist bzw funktioniert genauso wie erklärt. So wird es aber einfacher und verständlicher.

# Rückblick

- Wer hat alle Updates installiert?
- Wer hat seine Passwörter geändert?
- Wer hat ein AV-Progamm (de)installiert?
- Wer hat ein Backup angelegt?
- Wer hat sich Linux angesehen?
- Wer hat sein Smartphone abgesichtert?
- Wer hat sein WLAN überprüft?
- Wer hat sein SmartHome abgebaut?

# Frage Office Verschlüsselung

- Bei MS Office 2016 sicher
- MS Office 2010 – 2013 halbwegs sicher
- MS Office 2007 und älter unsicher
- Open/LibreOffice sind sicher

# Social Engineering & Phishing

# Social Engineering?

- Ziel
  - Verhaltensweise beeinflussen
  - Ködern von privaten Informationen
- Arten
  - Phishing: Nachrichten, Telefonat, ...
  - Dumpster Diving: Mülltonne durchsuchen
  - Baiting: USB-Stick mit Virus „verlieren“

# Phishing

- Durch Kontakt Informationen ködern
  - Gefälschte Webseiten
  - E-Mails
  - SMS, WhatsApp, ...
  - Telefonat
- Informationen
  - Passwörter, intene Infos, Kontodaten, ...

# Phishing erkennen

- Rechtschreib-/Grammatik-Fehler
- Frage nach Passwort
- Dringlichkeit (z.B. Sie haben 2 Tage Zeit)
- Angebliche Verwandte oder Kunden
- Persönliche Anrede
- URL überprüfen
- Keine Teilnahme/Kein Mitglied
- Achtung beim Anhang in E-Mails

# Privatsphäre & Datenschutz

# Warum?

- Allgemeine Erklärung der Menschenrechte
- Artikel 12
  - „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.“

# Wozu?

- Ich hab doch nichts zu verbergen...
- Jeder hat etwas zu verbergen!
  - Passwörter
  - Gehalt / Vermögen
  - Krankheiten
  - Postverkehr
  - ...

# Wovor schützen?

- Staat
  - Geheimdienste (Massenüberwachung)
- Firmen
  - Kredit-Rating
  - Verkauf von Vorlieben / Interessen
  - ...
- Kriminellen
  - Betrug, ...

# Datenschutz-Grundverordnung

# DSGVO

- EU-Verordnung
- Gilt mit: 25. Mai 2018
- Datenschutz-Anpassungsgesetz 2018
- Privacy by Design, Privacy by Default
- SEHR hohe Strafen
  - 20 Mio € oder 4% weltweiten Jahresumsatzes
  - Bsp: Apple 185 Mrd € → bis 7,4 Mrd € pro Fall
- NGO (NOYB - Max Schrems)

# Rechte

- Auskunft
- Richtigstellung
- Recht auf Vergessen (Löschung)
- Datenübertragbarkeit
-
- Frist: max 1 Monat (+2 Monate)

# Überwachung

# Wer sind die Überwacher?

- Five Eyes
  - USA: NSA, CIA, FBI
  - Australien: ASIS, ASD, ASIO
  - Canada: CSE, CSIS
  - Neuseeland: GCSB, NZSIS
  - Vereinigtes Königreich: MI5, MI6, GCHQ
- Andere
  - Deutschland: BND, MAD, BfV
  - Österreich: BVT,  HNaA, AbwA

# Königswarte (HNaA)

# Was wird überwacht?

- (fast) ALLES
  - Telefonate
  - SMS/MMS
  - E-Mails
  - Websurfen
  - Standortdaten (Handy)
  - Kontakte
  - Kameras

# Ein paar Zahlen

- NSA
  - Täglich 6 Mrd Metadaten
    - Email, SMS, Telefon
- GCHQ
  - Täglich 50 Mrd Metadaten (Stand 2012)
    - Emails, Telefonate, SMS, Suchabfragen, Telefonstandorte, ...
  - Metadaten: bis 6 Monate gespeichert
  - Inhaltsdaten: bis 30 Tage gespeichert

# Wer wird überwacht?

- (fast) JEDER
  - Politiker
  - Behörden
  - Firmen
  - Einzelpersonen
  - Massenüberwachung

# Warum wird überwacht?

- Terrorismus
- „einfache“ Verbrechen
- Industriespionage
- Bessere Verhandlungsposition
- Erpressung
- Konfliktabschätzung

# Womit wird überwacht?

- Anzapfen von Seekabel
- Anzapfen von Rechenzentren (DE-CIX)
- Abhören von Satellitenkommunikation
- Vorratsdatenspeicherung
- Verwendung von IMSI-Catchern
- Verwendung von „Stillen-SMS“
- Installation von Trojanern
- Brechen von Verschlüsselung
- Schwächung von Sicherheitsstandards

# Zielführend?

- Nadel im Heuhaufen
- Unschuldige betroffen
- Terroristen schon meist bekannt
- Keine Beweise auf Wirksamkeit
- Bruch von Menschenrechten
- Hohe Kosten

# Was tun?

- Whistelblower (Edward Snowden)
- Druck auf Politik aufbauen
  - Keine Überwacher wählen
  - Demonstration
- NGOs unterstützen (Epicenter.Works)
- Verschlüsseln
- Weiter erzählen

# Filme/Dokus/Links

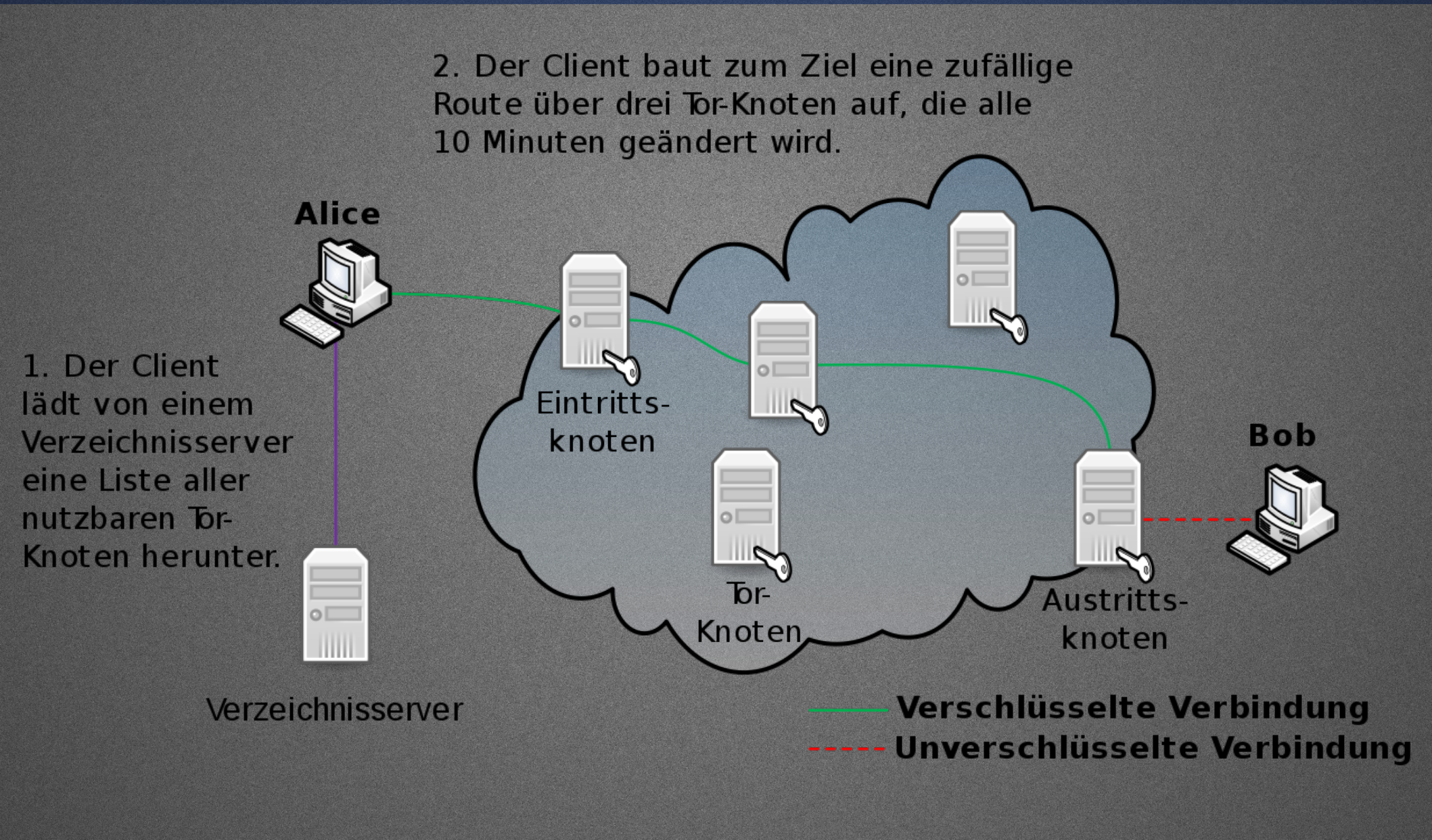
- Snowden (Geschichte Verfilmt)
- Citizenfour (Doku)
- ARD Doku - Jagd auf Snowden
- Heise.de - Geheimakte NSA-Ausschuss
- Heise.de - NSA-Skandal: Was bisher geschah - Zeitleiste

# Tor & Darknet

# Tor?

- Akronym: The Onion Router
- Finanzierung: 60% US-Regierung
- Anonymisierungs-Netzwerk
- Möglichkeiten
  - Anonymes Surfen
  - Versteckte Dienste (Darknet)
- Nachteile: Langsam, nicht 100% anonym

# Tor - Funktionsweise



# Wozu Tor?

- Umgehung von Zensur/Websperren
- Schutz gegen Überwachung (NSA)
- Schutz für Whistleblower (Snowden)
- Schutz für Journalisten
  - Und deren Quellen

# Darknet – Gut/Böse?

- Prinzipell neutral
  - → anonyme/versteckte Dienste
- Alles kann missbraucht werden
  - Messer, Auto, Pistole, ...
- Illegale Webseiten
  - Waffen-/Drogen-Verkauf, Kinderpornos, ...
- Doku ARD - Das Darknet

# Botnetz & DDoS

# Botnetz

- Kontrolle über SEHR VIELE Geräte
  - PC, Laptop, Smartphone, Router, IoT, ...
  - 10.000 – 30.000.000
- Verwendung
  - Spam-Mails (Phishing-Mails)
  - DDoS-Angriffe
  - Klickbetrug
  - Bitcoin Mining

# DDoS?

- Distributed Denial of Service
  - Überlastungsangriff
- Warum: Protest, Erpressung, Schädigung
- Angriffe:
  - DDoS-Attacke auf Heizungssteuerung
  - französischer Web-Hosters
  - Größter Angriff - Dyn

# DDoS mittels Botnetz

# Sichere Kommunikation

# Was bedeutet sicher?

- Verschlüsselung
  - Algorithmus
  - End-to-End
  - Perfect Forward Secrecy
  - Abstreitbarkeit
- Korrekter Kommunikationspartner
- Korrekte Nachrichten
- Metadaten
- Verfügbarkeit (Blockade, Ausfallsrate)

# Kommunikationsmittel

- Telefon
- SMS / MMS
- E-Mail
- Diverse Messenger (WhatsApp, Signal)
- VoIP
- Videochat

# Messenger

- WhatsApp
- Signal
- Telegram
- Threema
- Skype

- Liste von mobilen Instant-Messengern

# E-Mail

- „Normale E-Mail“ = Postkarte
  - → nicht sicher
- Verschlüsselte E-Mail
  - PGP, S/MIME
- Möglichkeiten
  - Verschlüsseln = „Briefkuvert“
  - Signieren = unterschreiben
- Probleme
  - Metadaten, Key-Management, hat nicht jeder

# E-Mail Programme

- Webclient
  - Gmail, GMX, Hotmail, Posteo, Mailbox, ...
- Desktop
  - Microsoft Outlook, Mozilla Thunderbird, ...
- Mobile
  - K9-Mail, ...
- Verschlüsselung
  - GnuPG, OpenKeychain

# Sicheres Surfen

# Diverse Browser

- Closed Source
  - Internet Explorer / Microsoft Edge
  - Google Chrome
  - Apple Safari
- Open Source
  - Mozilla Firefox
  - Chromium
  - ...

# Wahl des Browsers

- Open Source
- Häufige und schnelle Updates
- Allgemein als sicher anerkannt
- Passende Add-ons zur Verbesserung der Sicherheit
- Sandbox
- Webstandards
- Schnelligkeit

# Browser Einstellungen

- „Tracking Flag“ (Do Not Track)
- Cookies
- Masterpasswort
- Domain in URL hervorheben
- Privacy Suchmaschine (Startpage, DuckDuckGo)
- JavaScript deaktiveren

# Add-ons (Firefox)

- Ad-Blocker: uBlock Origin
- Script-Blocker: NoScript, uMatrix
- Tracking-Blocker: Privacy Badger
- TLS: HTTPS Everywhere

# Kinderschutz

# Kinderschutz

- Möglichkeiten
  - Webseitenfilter (Porno, Glück-/Gewalt-Spiele)
  - Zeitmanagement (z.B. Internet von 8-21 Uhr)
  - Programmsperre (z.B. nur Office & Browser)
- Einstufungen nach Alter
  - PEGI, FSK
- Software
  - Anti-Viren-Programme
  - Spezielle Kinderschutz Software

# Zusammenfassung

- Jeder hat etwas zu verbergen!
- Machen wir es Ihnen so schwer es geht
- Tor bzw Darknet nicht per se böse
- Botnetze werden immer bedrohlicher
- Nutzt Signal und verschlüsselte E-Mails
- Sichert euren Browser ab

# Links

- https://www.onlinesicherheit.gv.at/
- https://www.bsi-fuer-buerger.de/
- https://www.saferinternet.at/
- https://www.klicksafe.de/
- https://www.internet-abc.de/
- https://www.ispa.at/wissenspool/broschueren.html
- https://cryptoparty.at/
- https://epicenter.works/crypto

# Fühlst du dich jetzt sicherer?

Spenden gehen an:
- epicenter.works (AKVorrat)
- NOYB
- Netzpolitik.org
- Electronic Frontier Foundation
- Weitere Vorschläge?

KONTAKT:
rupprecht.thomas@gmail.com