Notfunk: IT-Sicherheit

Thomas Grunenberg DL9TG (DN3TG)

DARC-L04
VFDB-Z63

Stand: 20. Januar 2025

Inhalt

IT Sicherheit im Notfunk: Warum? Wie?

Inhalt

Begriffe

Sicherheit

- Schutz vor Ausfall
- Schutz vor Sabotage
- Schutz vor Ausspähen
- Schutz vor Manipulation

Pentesting

- Penetrationstest $\Rightarrow$ Eindringen ins System
- Einnehmen der Angreiferrolle

System

- Beinhaltet **alle** technischen Komponenten
- UND die Anwender

Situation

Damals

- Viele kleine Inselnetze / Wenig globale Vernetzung
- Eindringen/Manipulation/Viren als "Schabernack"
- Angreifer meistens Einzelgänger

Heute

- Viele Verbindungen über das Internet
- Angreife als Geschäftsmodell (z.B. Erpressung)
  - Angreifer arbeiten organisiert
  - Handel mit Exploits (Wissen/Methoden) [a]

[a] https://www.golem.de/news/russland-zero-day-haendler-kauft-exploits-fuer-bis-zu-20-mio-dollar-2309-178047.html

Gefahren

Technische Gefahren

- Defekte
- Konfigurationsfehler
- Rahmenbedingungen (z.B. hohe Last)

Gefahren durch Angreifer

- Ausspähen
- Diebstahl von Daten oder Ressourcen
- Sabotage

Gefahren durch Anwender

- falsche Bedienung
- Fahrlässigkeit z.B. mit Zugangsdaten

Gefahren: Ausspähen

Ausspähen oft als Vorbereitung:

- Späterer Angriff
- Andere IT Ziele (Proxy)
- Sabotage
- Physische Einbrüche

Gefahren: Diebstahl von Daten oder Ressourcen

Ziele beim Diebstahl von Ressourcen

- Rechenleistung (z.B. Bitcoin)
- Erschleichen von Leistungen
- Austausch illegaler Dateien

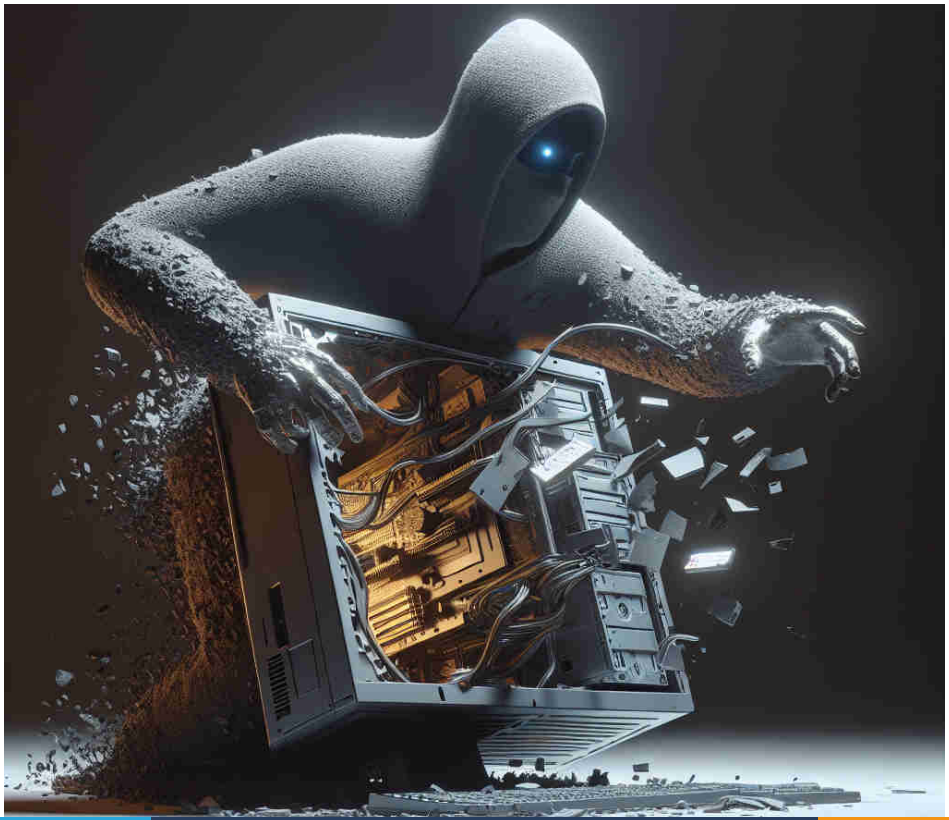
Ziele beim Diebstahl von Daten

- Erpressung
- Daten für gezieltes Phishing
- Erbeuten von Zugangsdaten

Gefahren: Sabotage

Unterschiedliche Motivation

- Erpressung (DDOS)
- Anerkennung / Fähigkeiten beweisen
- Rache



Gefahren: Angreifertypen

Typen

- Bot / Computersystem
  - Skript: dummes abklopfen nach Schwachstelle
  - Künstliche Intelligenz
- Mensch
  - Laie
  - erfahrene Person
  - Profi

Position

- Extern / weit weg
- Interne / Ehemalige
- Physischer Zugriff

Beispiele

Es folgen ein bekannte Beispiele und Methoden

Beispiele: Loveletter

Schadprogramm

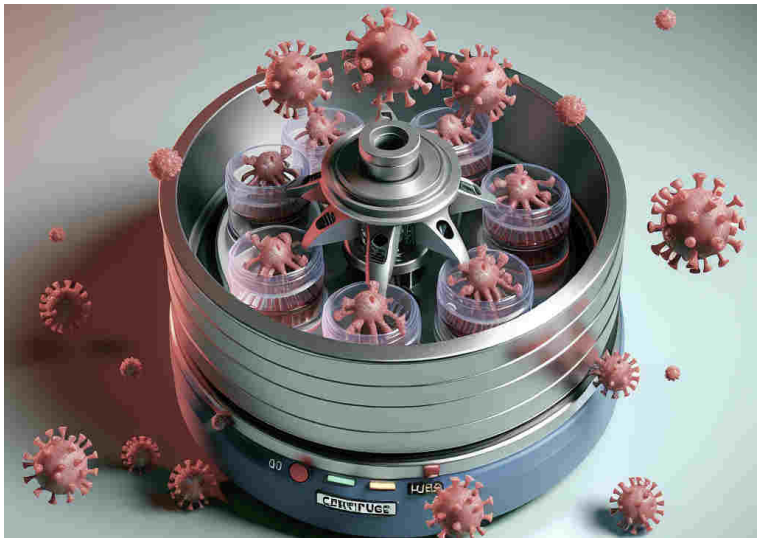
- 2000
- Wurm: Verbreitung per E-Mail ((ILOVEYOU)
- Millionen Rechner waren befallen

[0] https://www.golem.de/news/loveletter-autor-des-i-love-you-virus-wollte-kostenlos-surfen-2005-148249.html

Beispiele: Stuxnet

Schadprogramm zur Sabotage

- 2010
- Angriff zielte eigentlich auf Siemens vom Typ Simatic S7
- Sollte Zenftrifugen für Atomanlagen im Iran sabotieren (Cyberwaffe)
- ca. 45.000 Geräte waren betroffen

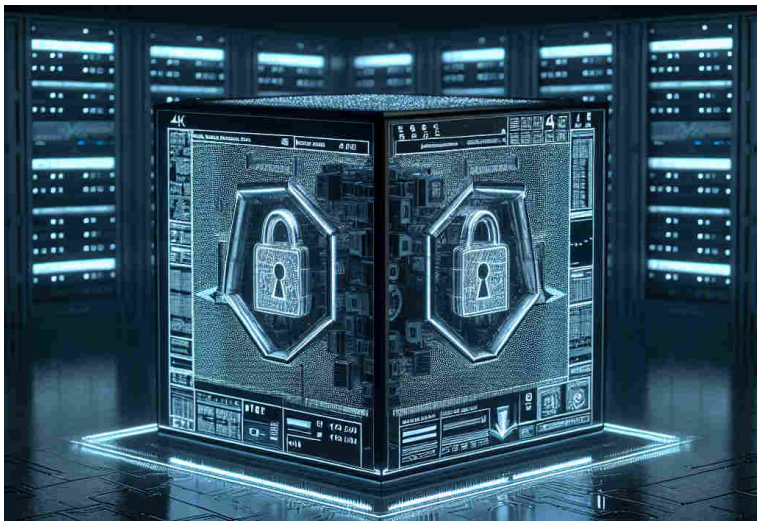


[0] https://www.zeit.de/2010/48/Computerwurm-Stuxnet

Beispiele: WannaCry

Ransomware / Schadprogramm

- 2017
- Erpressung durch Verschlüsselung von Daten
- 230.000 Computer in 150 Ländern



[0] https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html

Beispiele: WLAN: WEP

Schwachstelle im Protokoll IEEE 802.11b

- 2013
- RC4 Algorithmus wurde geknackt
- WEP war schlagartig unsicher
- Nachfolger: WPA, WPA2, heute: WPA3

[0] https://www.it-security-wissen.de/wep.html

Beispiele: WLAN: Deauth

Schwachstelle im Protokoll IEEE 802.11

- Protokoll von: 1997
- WPA / WPA2 sichern nur Nutzdaten
- Gefälschte Pakete können Verbindungen trennen
- Basis für DDOS
- Basis für Angriffe auf Verschlüsselung (Handshake)

[0] https://www.golem.de/news/wlan-kameras-ausgeknipst-wer-hat-die-winkekatze-geklaut-1910-144199-2.html

Beispiele: Bahn

Bahn: Durchtrennte Glasfaserkabel

- 2022
- Sabotageakt am GSM-R-Netz
- 3 Stunden Totalausfall in Norddeutschland
- Vertrauliche Pläne standen online

[0] https://www.heise.de/news/Sabotage-bei-der-Bahn-Viele-vertrauliche-Infos-sind-offen-zugaenglich-7307277.html

Beispiele: Log4Shell

Sicherheitslücke in Java-Bibliothek Log4j

- 2021
- CVE-2021-44228
- Sehr viele betroffene Geräte
- War leicht auszunutzen

[0] https://www.security-insider.de/was-ist-log4shell-log4j-schwachstelle-a-6e6873adc74e25e845e027ac024303c8/

Beispiele: Sicherheitsproblem Liontron Batterie

Bluetooth Sicherheitsproblem durch offenes Bluetooth

- 2021
- Bericht durch Wemo Geräte AG
- War leicht auszunutzen: Angriffswerkzeug Smartphone
- Funktionen waren nicht in Standart-App sichtbar
- Hersteller-App ermöglichte Deaktivierung des Akkus

[0] https://www.youtube.com/watch?v=6DD5jcI1ZJU

Beispiele: Hardwareschäden durch Software

Rhythm Nation von Janet Jackson

- 2022
- Festplattenschäden durch akustische Schwingung (Eigenresonanz)
- CVE-2022-38392 nennt z.B. Seagate STDT4000100 763649053447

[0] https://www.sueddeutsche.de/wirtschaft/janet-jackson-festplatte-crash-rhythm-nation-1.5641132
https://nvd.nist.gov/vuln/detail/CVE-2022-38392

Beispiele: Photovoltaik Heimspeicher defekt durch Update

Sungrow: Defektes Update

- 2023
- Hersteller aus China verteilt veesehentlich defektes Update
- 800 Heimspeicher unbrauchbar
- Hardwaretausch war nötig

[0] https://www.pv-magazine.de/2023/04/18/sungrow-speicherproblem-wird-zeitnah-behoben/

Beispiele: xz Attacke

Vorsätzliche Sicherheitslücke in Programbibliothek xz

- 2023/2024
- Supplychain-Angriff
- Hintertüre in Software zu Dekompression von Daten
- Ermöglicht Code auszuführen
- Wurde seit 2021 geplant

[0] https://www.heise.de/news/xz-Attacke-Hintertuer-entraetselt-weitere-Details-zu-betroffenen-Distros-9671588.html

Beispiele: Honeypod

Honigtopf (soll anlocken)

- Ist eine Falle für Angreifer
- Gängiges Verfahren um Angriffe zu analysieren
- Wird zur Gewinnung von Wissen eingesetzt
- Kann auch zur Ablenkung verwendet werden

Beispiele: Aktuell

Krieg Ukraine

- Gezielte Angriffe auf Infrastruktur
- Zu Beginn: Sat-Kom war gestört ⇒ Windkraftanlagen in Deutschland betroffen [a]
- Verfassungsschutz warnt offiziell vor Cyberangriffen russischer GRU-Einheit 29155 [b]

---

[a] https://www.faz.net/aktuell/wirtschaft/fernsteuerung-von-tausenden-windkraftanlagen-gestoert-17845889.html

[b] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2024/2024-09-05-cybersecurity-advisory-3.html

Beispiele: Aktuell

Interview mit Generalleutnant

- Infrastruktur ist ein Ziel (Hybride Bedrohung)
- Sabortage und Sabortagevorbereitung: "hatten wir schon"
- Versteckter Sprengstoff wurde gefunden (nicht älter als $1\frac{1}{2}$ Jahre)
- "Krieg zu führen ohne einen Schuss abzugeben"
- Dieses Interview von BR24 ist sehr zu empfehlen bitte in voller Länge ansehen.

a

[a] https://www.br.de/nachrichten/deutschland-welt/generalleutnant-deutschland-schon-lange-nicht-mehr-im-frieden,Ua8q55u

Schutzmaßnahmen

Schutzmaßnahmen umfassen

- Prävention
- Schadensbegrenzung
- Planung Schadenbehebung

Schutzmaßnahmen umfassen ALLES

- Hardware
- Software
- Anwender UND technisches Personal

Betriebssicherheit

Betriebssicherheit

- Systeme sollen nicht ausfallen
- Systeme sollen nicht zum Ausfall anderer Systeme führen

Maßnahmen

- Überwachung
- Redundanz (auch beim technischen Personal)
- Diversität

Schutz gegen Angriffe

Physisch

- abgeschlossene Räume / verteilte Systeme
- Wachschutz
- Energieversorgung: Überspannungsschutz, USV
- Abschirmung / EMV
- Klimasysteme / Luftfilter

Virtuell

- Zugriffskontrolle
- IDS (Einbruchserkennung im Netzwerk)
- Backup der Daten und Einstellungen
- Härtung der Software (z.B. SecureBoot)
- Sicherheitsupdates

Schutz gegen Angriffe

Menschlich

- Schulung (z.B. wegen Phishing)
- Veraltete Zugangsdaten löschen
- Vorbeugung Bestechung
- Vorbeugung Erpressung

Weiteres

- Räumlich verteile Systeme
- Datenverschlüsselung
- Signierung von Nachrichten

Pentesting zum prüfen des Schutzes

Pentesting

- Versuch in System einzudringen
- Informationen über System einholen
- Suche nach Schwachstellen

⇒**Pentesting machen am besten Außenstehende**

Aktualität

- Software verändert sich (Updates)
- Auch Lücken in Hardware können bekannt werden
- Weiterentwicklung von Angriffen bei menschlichen Sicherheitslücken

⇒**Pentesting muss regelmäßig wiederholt werden**

Übertragung auf Notfunk

Wissen aus der IT Sicherheit lässt sich größtenteils auf das Thema Notfunk übertragen

Situation im Notfunk

Basis ist AFU

- offen für jeden (unverschlüsselt, ungesicherter Zugang)
- offene Dokumentation
- Mitgliedermangel ⇒ Leichter Zugang in Orga. / wenig Reserve
- Sehr hohe Individualität ⇒ hohe Diversität

Möglichkeiten/Empfehlungen für Notfunk

- Aufmerksamkeit im Bezug auf Sicherheit
- Planung der Sicherheit von Anfang an
- Überwachung der Geräte
- Pentesting

Situation im Notfunk

Vor der Notfunksituation

- Viele vernünftige Menschen, aber auch Egoisten und Kriminelle dabei
- Es liegt die Vermutung nahe, das Lebensumstände welche die Situation verschlechtern das Verhalten beeinflussen. Z.B Zunahme der Ladendiebstähle in 2024 um 24% nach hoher Inflation. [a] [b]
- Viele Menschen sind nicht auf stärkere Krisen vorbereitet, Ende 2022 hatten nur 38% Notvorräte. [c]

---

[a] https://csl.mpg.de/690906/ansteigender-ladendiebstahl

[b] https://www.finanz-tools.de/inflation/inflationsraten-deutschland

[c] https://www.rnd.de/bauen-und-wohnen/krisenvorsorge-38-prozent-haben-notvorraete-viele-halten-das-aber-geheim-EGSNSAQVRC74SO3MIQRQAWYCPA.html

Überlegungen zum Notfunk

Normaler AFU Betrieb

- EMV Probleme
- Relaisstörer

Notfunk ~~Probleme~~ Herausforderungen

- Keine Verschlüsselung, keine Signierung
- Andere Bedingungen im echten Notfunk als im Testbetrieb
- Stress im echten Notfunkbetrieb

$\Rightarrow$**Vorher gut nachdenken über Sicherheit**

Überlegungen zum Notfunk

Überlegungen mit bekannten Hintergründen beim Internet.

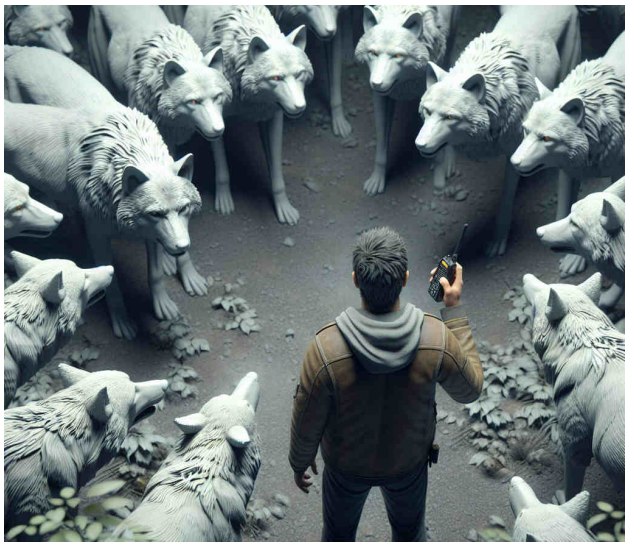
Motivation

- Diebstahl/Erpressung
  - Geld als Ziel: Unwahrscheinlich
  - Sexuelle Motivation: Sehr unwahrscheinlich
  - Persönliche Motivation: Möglich
  - Ressourcen als Ziel (Wasser/Nahrung/Strom/Wärme): Wahrscheinlich
- Sabotage :
  - Ist der Grund für den Notfunkfall Sabotage sind Reservesysteme wahrscheinlich auch ein Ziel.
  - Sabotage kann auch versehentlich passieren, z.B. durch unbedachte Überlast. Fallen andere Systeme aus werden OMs vermehrt zum Funk greifen. Akkus von Relais so z.B. schneller entladen.
  - OMs könnten sauer sein, wenn Notfunk Vorrang hat oder keine Kapazität hat ihnen vorrangig zu helfen.

Überlegungen zum Notfunk

Schwachstellen

- AFU ist nicht für Sicherheit ausgelegt:
  - Keine Verschlüsselung
  - Kein Zugriffsschutz
  - Keine digitalen Signaturen
- Metadaten:
  - Rufzeichen: Liste mit Adressen
  - Position: Peilen / oder im Signal (z.B.APRS)



Beispiel Stimmen kopieren

Enkeltrickbetrüger

- Skrupellose Menschen mit psychologischen Fähigkeiten andere in einen Schockzustand zu versetzen zur Manipulation
- Weiterentwicklung durch Stimmen clonen [a]

[a] https://www.tagesschau.de/investigativ/swr/ki-kuenstliche-intelligenz-voice-cloning-100.html

Übertragung auf Notfunk

- Diese Kriminellen werden in einer Notfunksituation weiterhin da sein!
- Fähigkeiten könnten genutzt werden um im Notfunk Beute zu machen
- Stimmen im Sprechfunk könnten gefälscht werden ⇒ Rufzeichen und Stimme sind keine sichere Identifizierung.

Beispiel VHF/UHF Relais

Ist Zustand

- Offen für jeden
- Selten: Notstrom, Monitoring vom Akku
- Kennung über CW

Übertragung auf Notfunk

- Notstrom wäre gut mit Monitoring
- Umschaltbare Ansagen / automatische Hinweise wären gut
- Vorbereitung gegen Störer wären gut:
  - Adressliste Rufzeichen offline bereit halten
  - Schnelles anpeilen von Störern sollte möglich sein / evt. geübt werden.
  - künstliche Notches beim Empfang

Beispiele Ausfall Infrastruktur

Sabotage

- Reservesystem wird wahrscheinlich auch Ziel
- Kann vorab vorbereitet worden sein
- Ziel sind Geräte **und** Personen, Rufzeichen werden offen übertragen und Adressen sind in Liste abrufbar

Katastrophenfall

- Leute benötigen dringend Ressourcen: Nahrung/Wasser/Wärme/...
- Notfunkpersonal ist im Einsatz
- Im Notfunk werden offen Rufzeichen übertragen
  1. Adresse kann mit Rufzeichen nachgesehen werden
  2. Dort ist vermutlich was zu holen
  - 3a Haus/Wohnung ist unbewacht
  - 3b Familie vom Notfunkpersonal ist da und hat Ressourcen

WLAN/Bluetooth im Notfunkfall

Situation bezogen auf mögliche Angreifer

- Vermutlich kein oder wenig Strom
- Smartphones (Powerbanks) noch länger aktiv
- Kein Handynetz, kein WLAN von Nachbarn
- Viele Menschen in Not $\Rightarrow$ Viel Motivation für neue Handlungswege

Jedes Smartphone kann WLAN/Blutooth sehen

- Bluetooth und WLAN sollte nicht sichtbar sein
  - Am besten gar nicht nutzen / deaktiveren
  - Sendeleistung wenn möglich reduzieren
  - Nur mit Passwort/PIN geschützt nutzen
  - Sichtbare Netze verraten Notstrom (da ist was zu holen)!

Hamnet

AFU

- OMs nutzen vermutlich normalen PC (Viren/Würmer,...)
- basiert auf WLAN ⇒ anfällig für Deauth Angriffe
- Kann im Vorfeld mit öffentlichen Quellen ausgekundschaftet werden. ⇒ Überlegen welche Infos man wirklich öffentlich machen muss. [a]
- Kann im Vorfeld (und mit falschem Rufzeichen) leicht ausgekundschaftet werden ⇒ Schon im Vorfeld gut überwachen.

[a] `https://hamnetdb.net/`

Übertragung auf Notfunk

- Gerätesoftware sollte immer aktuell gehalten werden
- Kritische Zugänge (z.B. Router Konfiguration) sollten gut geschützt werden
- Methoden zur Priorisierung von Datenverkehr prüfen für Notfunk

APRS / Meshcom

AFU

- Basiert auf AX.25 Protokoll
- Mesh: Automatische Organisation ⇒ Stresssicher in Anwendung [a]

[a] https://icssw.org/meshcom-2-0-protokoll/

Übertragung auf Notfunk

- Keine Verschlüsselung oder digitale Signatur
- Andere Absicherung empfehlenswert z.B. TAN Listen.
- Überlegen ob man Positionsausendungen wirklich braucht und wenn nicht abschalten

Digitale Signatur

Verschlüsselung

- Symmetrisch: ein gemeinsamer Schlüssel
- Asymmetrisch: Schlüsselpaar
  - privater Schlüssel
  - öffentlicher Schlüssel

Übertragung auf AFU/Notfunk

- Symmetrische Verschlüsselung $\Rightarrow$ keine offene Sprache
  - Schlecht zum üben
  - Schlüsseltausch ist ein Problem
- Asymmetrische Verschlüsselung: Möglichkeit Nachrichten nur zu signieren, jeder kann über öffentlichen Schlüssel prüfen ob ein Absender echt ist

Digitale Signatur

Anwendung

- Bei Winlink z.B. möglich via Zwischenablage
- Gute Software OpenPGP [a]
  - Sehr sicher
  - Gemacht für E-Mails
  - Verfügbar für Linux, Windows, Apple, ...
  - Nur Signieren möglich
  - Verschlüsselung wäre zuschaltbar
  - Vertrauenwürdige/Signierte Zertifikate möglich ⇒ Öffentliche Schlüssel können auch noch in Notfunklage getauscht und gerpüft werden.
  - Alle nicht signierten Zertifikate müssen VORHER über sichere Wege (persönlich) getauscht werden.

[a] https://www.openpgp.org/

Ende

Vielen Dank für die Aufmerksamkeit