Digitale Vernetzung und Verletzbarkeit von Industrie und kritischen Infrastrukturen

Bedrohungen - Schwachstellen - Abwehrstrategien

Invent & Verify

Intro

- Gregor Kopf
  - Seit 2008 Security Consultant bei der Recurity Labs GmbH
  - Reviews komplexer IT-Systeme und Umgebungen
    - Source Code / Binary
    - Kryptographische Protokolle
    - Design

Bekannte Hacks

- TLS
  - Heartbleed
  - Diginotar
- BMW hack
- Diverse SCADA hacks
- ICANN
- New York Times (Syrian Electronic Army)

Einen Schritt Zurück

- Gemeinsamkeiten
  - Vernetzung
    - Erreichbarkeit
    - Verteilung von Verantwortlichkeiten
  - Abstraktion
    - Automatisierung
    - Treffen von Annahmen

Vernetzung

Vernetzung

- Vormals isolierte Systeme werden zu einem großen Netzwerk
- Alle sprechen IP
  - Autos
  - Telefone
  - Medizinische Produkte
- Nicht alle erreichbaren Parteien sind auch vertrauenswürdig
- Man kann andere erreichen, ist aber auch selbst erreichbar

Vernetzung

- Internet of Things
  - Und keiner weiß, welche Dinge
- M2M
- Dynamic DNS
- Autoregistration
- Mesh-Netzwerke
- Forderung nach dynamischen Systemen, die immer schwieriger zu verstehen werden

Abstraktion

Abstraktion

- Abstraktion
  - Wiederverwenden bestehender Komponenten
    - Welche Eigenschaften dürfen angenommen werden?
    - Welche (Software-)Komponente leistet was?
- Delegieren von Verantwortung
- Leaky Abstractions
  - Ungerechtfertigte Annahmen
  - Bei Produktlebenszyklen von > 20 Jahren

Infrastruktur

- Worauf wir aufbauen
  - BGP
  - DNS
  - Email
  - X.509
  - Authentifizierung über Google / Facebook
  - „Cloud“
    - a.k.a. Copy Lots Of User Data

Kritische Infrastruktur

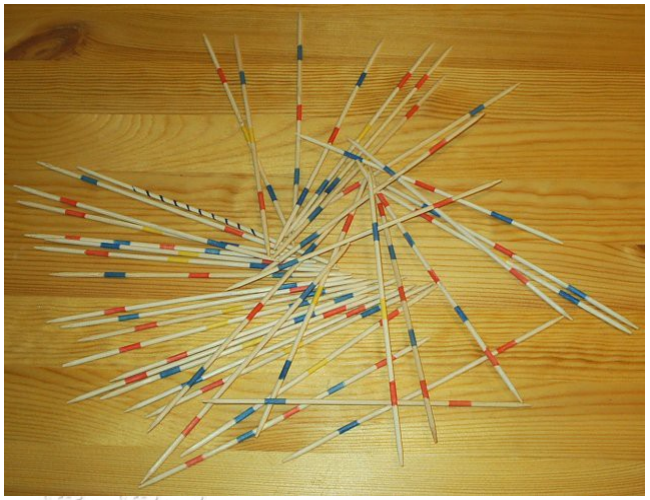
- Kritische Infrastruktur
  - Was ist das?
    - Kritische Infrastruktur vs. kritische Anwendungen
  - Wer bestimmt, was kritisch ist?
    - Die Regierung (IT-Sicherheitsgesetz)?
- Frage nach Verantwortlichkeiten
  - Infrastruktur kann kritisch werden
    - Wenn kritische Komponenten darauf aufbauen
    - Vor allem, wenn sie sich weit unten im Stack befindet

Kritische Infrastruktur

- Passwort-Reset über Email
  - MX-Records im DNS
  - Seit wann gilt Email als vertrauenswürdig?
- X.509
  - StartSSL stellt X.509-Zertifikate aus
  - Prüfung des Domaininhabers per Email
    - Mail an postmaster@, hostmaster@ oder webmaster@
    - Was könnte da wohl schiefgehen...

gTLD

- Grundlegende Änderung in bestehender Komponente
  - Meine Wunschliste: .onion, .daimler, .scada, .bmw
- GccTLD
  - Google interpretiert einige ccTLD mit anderer Semantik



gTLD

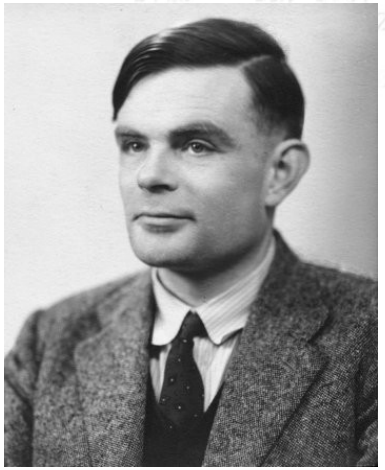
- Ungerechtfertigte Annahme: .onion ist keine gültige TLD
  - Welches RFC schreibt die Abwesenheit von .onion vor?
  - Analogie: RFC1918-Adressen
    - 2.2.2.2 als interne Adresse verwenden?
      - Hallo, DTAG
- Besserer Ansatz
  - ISO 3166-1: User-assigned code elements
- Das Problem resultiert aus ungültigen Annahmen

Probleme

- Fehlerhafte Annahmen
  - Der Angreifer kontrolliert das DNS nicht
    - Im Internet mag das (manchmal) stimmen
    - Am Flughafen / im Hotel auch?
  - .gibt-es-nicht ist keine gültige TLD
    - Und 2.2.2.2 kann man problemlos intern verwenden...
- Auf der positiven Seite:
  - OpenSSH kann Host-Keys per DNS prüfen
  - Fragt standardmäßig dennoch nach (außer bei DNSSEC)

Und die Sicherheit?

- Wie funktioniert Security?
  - Die bauen wir oben drauf!
    - AV
    - IDS
    - IPS
  - Grundlegende Probleme ignorieren wir dabei
  - Und unseren schiefen Turm stützen wir seitlich ab
    - ASLR
    - DEP



Sicherheit

- Sicherheit ist charakterisiert durch nicht-funktionale Eigenschaften
- Beispiel:
  - Anwesenheit von Zugriffkontrolle
  - Abwesenheit von
    - Speicherkorruption
    - Injection-Problemen
    - Kryptographischen Seitenkanälen
    - …
- Kein „one size fits it all“

Zusammenfassung

- Sicherheitseigenschaften werden behauptet oder angenommen
  - Wo ist die Produkthaftung?
- Alte Weisheit: man muss auch das Auto vor und hinter sich fahren
  - Aufbau sicherer Systeme ist nicht anders
  - Akteure sollten sowohl den Stack unterhalb als auch oberhalb des eigenen Systems kennen
- In Mitarbeiter investieren!

Vielen Dank.

Gregor Kopf
Security Consultant

greg@recurity-labs.com

Recurity Labs GmbH, Berlin, Germany
http://www.recurity-labs.com

Invent & Verify