Sikkerhedsreviews

SÅDAN SIKKERHEDSTESTER I JERES DIGITALE PRODUKT

29/1-2026

Michael Stausholm, Principal Security Architect

Lidt om mig

- Uddannet datalog (kryptologi) i 2011.
- Har arbejdet med cybersikkerhed siden.
- Stort fokus på standarder og compliance de seneste år.

- Deltaget i mange forskellige typer af sikkerhedsreviews.

KOMBIT

DIGITALISERINGSSTYRELSEN

kamstrup

fdo Danske Olieberedskabslagre

PROLØN

nets

GRUNDFOS

Vi bringer den nyeste it-forskning og teknologi i spil i dansk erhvervsliv

- I kan bruge os som uvildigt konsulenthus eller underleverandør.
- I kan indgå i et af vores forsknings- og udviklingsprojekter.
- I kan deltage i vores netværk, workshops og arrangementer.

Hvad er en sikkerhedstest?

- Vi vil gerne cybersikre vores XYZ, men der er mange tilgange:
  - Sikkerhedsreviews – Er arkitekturen i orden?
  - Kodereviews – Er der (tekniske) fejl i koden?
  - Pentest – Er der fejl i det kørende “system”?
  - Audits – Er der processer som håndterer sikkerheden?

  - Certificering – Kan vi få et stempel på om sikkerheden er i orden?

“Certificering”

- Kan vi få et “stempel” på at sikkerheden er i orden?
  - Ja – Hvis der findes en passende standard f.eks:
    - ISO/IEC 27001 – Ledelsessystem IT sikkerhed
    - EN 18031-X, ETSI EN 303 645, (kommende EN 40000-X) – Cybersikkerhed i produkter
    - IEC 62443-X – Cybersikkerhed i OT systemer
  - Kig efter DANAK logoet
    - -> Internationalt anerkendt kvalitetskontrol (ILAC)

- Ikke alle ”frameworks” har en conformance metodik (f.eks OWASP Top 10)

Forskellige tilgange

Whitebox tilgangen:

- Vi leder efter fejl
- Analytikeren har (unaturligt) mange ressourcer til rådighed

Fordelene:

- Grundigere og mere målrettet
- Finder potentielle fremtidige svagheder

Blackbox tilgangen:

- Simulerer et “ægte” angreb

Fordelene:

- Let for kunden at igangsætte
  - Måske eneste mulighed?
- Finder “reelle” problemer

Whitebox tilgangen:

Ulemperne:

- Kræver mere involvering af kunden
- Kan være overvældende – Finder mange mindre problemer

Blackbox tilgangen:

Ulemperne:

- Kan blive standset tidligt i processen
- Begrænset af angriberens tid/evner
- Giver et “øjebliksbillede” – særligt når et angreb er baseret på brugerne

Hvad er formålet – Hvornår vælger man hvilken type test?

- Hvad vil vi opnå med testen?
  - Finde faktiske fejl og mangler?
  - Skabe opmærksomhed på sikkerhed?
  - Se om vores tiltag virker?

- Dokumentere sikkerheden overfor nogen?

Krav til Cybersikkerhed - NIS-2

- NIS 2 stiller krav til cybersikkerheden i “vigtige” og “væsentlige” organisationer
- Kravene er rettet mod generel IT-sikkerhed og ledelsessystemer
  - Audits og ISO 27001 er den “sikre” tilgang
  - CIS-18 og D-mærket kan måske også anvendes

- Også krav mod forsyningskædesikkerhed
  - Vores underleverandører skal også være sikre
  - Og det skal de produkter vi bruger også
    - Her må div. reviews og pentest metoder gerne bruges – Det er op til kunden hvad de vil acceptere

Krav til Cybersikkerhed - CRA (og RED DA)

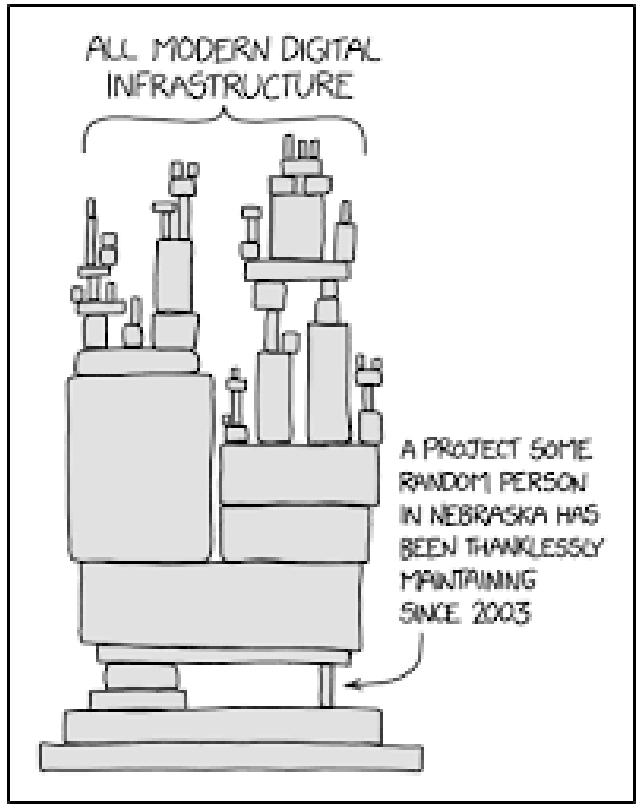
- Cyber Resilience Act stiller krav til cybersikkerheden i “Produkter med digitale elementer” (fra December 2027)
  - Pt. gælder noget tilsvarende kun for radioudstyr

- En række tekniske krav til produkterne
- En række organisatoriske krav
- Primært en udfordring mht. dokumentation
  - Forudsætter en whitebox tilgang
  - I nogle tilfælde også en **uvildig** tredjepart

Hvad finder vi så?
- De største trusler

Usikre/gamle dependencies

- I stort set alle kodereviews
  - Ofte falske positiver, men ...
- Lette at finde med automatiske værktøjer



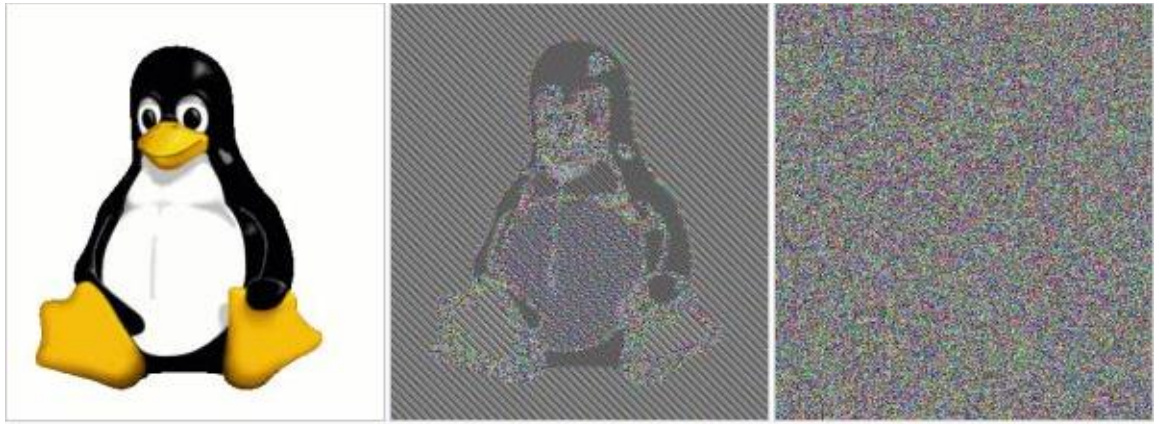
Authorization / Authentication

- Ofte problematisk:
  - “Forkert” brug af JWT
  - Sessionshåndtering
  - Svage login mekanismer
  - Inkonsistente roller
  - Manglende kontrol af adgangsrettighed

Uhensigtsmæssig brug af kryptografi

- TLS konfigurationer
- Valg af hash algoritmer
  - Sikkerheds relevant eller ej?

- Generelle problemer med kryptografien:



Original image | Encrypted using ECB mode | Modes other than ECB result in pseudo-randomness

Hvad kommer vi videre?

- Find ud af hvad der skal undersøges:
  - Hele organisationen, et produkt eller (dele af) en teknisk løsning?
- Overvej hvorfor du vil have en sikkerhedstest?
  - Intern læring? Ekstern kommunikation? Compliance?
- Bestem derefter metoden:
  - Whitebox eller blackbox?
  - Baseres på en standard eller er frie tøjler?
- Vi kan hjælpe med det meste, men vi ved også hvor vi er stærkest

Kontakt

Michael Stausholm
Principal Security Architect

Michael.stausholm@alexandra.dk
20296322

ALEXANDRA INSTITUTTET