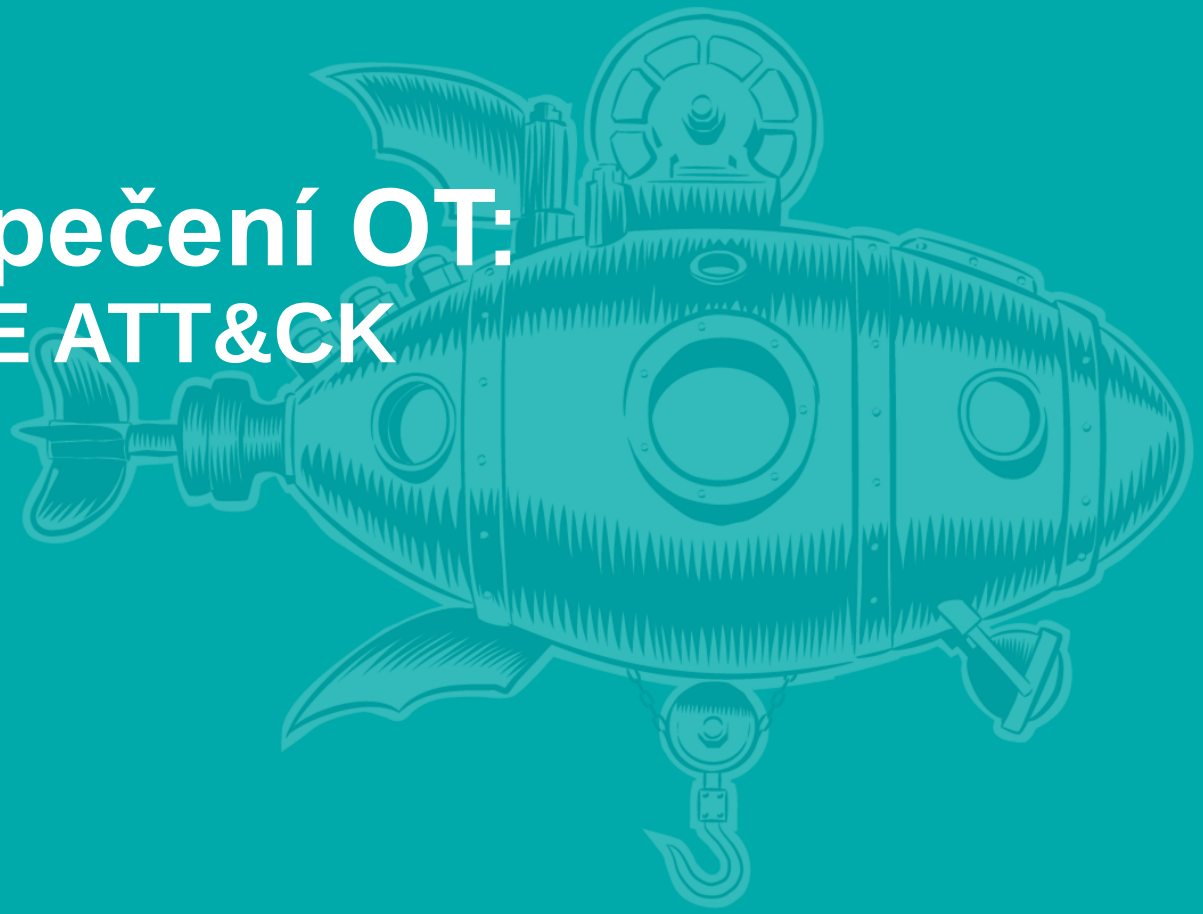
ALEF

Posuzování zabezpečení OT:
Od IEC 62443 po MITRE ATT&CK



Jan Kopřiva

Senior Security Consultant

jan.kopriva@alef.com

TLP:CLEAR

OT prostředí jsou z principu zranitelná…

- Historické OT systémy
  - Velmi dlouhý životní cyklus
  - Často proprietární, uzavřená řešení
  - Nemožnost záplatovat
    - Absence záplat od výrobce a/nebo provozní důvody

OT prostředí jsou z principu zranitelná…

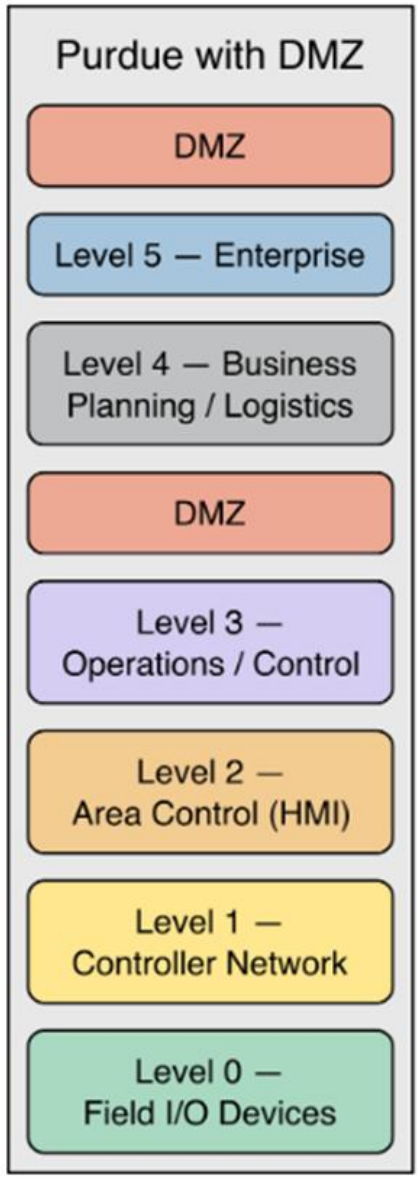
- Nutnost využívání zastaralých operačních systémů a SW i v rámci IT infrastruktury v zájmu zajištění kompatibility s OT systémy
- Bezpečnostní opatření často nevychází z odborných standardů, vznikají dynamicky dle aktuálních potřeb organizací a jejich efektivita nemusí být vždy zřejmá

Jak pak smysluplně posuzovat OT bezpečnost?

- Vybrané přístupy z oblasti kybernetické bezpečnosti zcela validní i v OT
- Jiné vyžadují drobnou modifikaci
- Vybrané postupy (např. tradičně pojatý vulnerability management s „patch all“ mentalitou) zcela nevyužitelné

Klíčová otázka

- Je OT oddělené od IT?
  - Je-li odpověď na tuto otázku „ne“, úroveň bezpečnosti daného OT prostředí z principu nemůže být vysoká…
    - Oddělení IT a OT je nejefektivnějším bezpečnostním opatřením pro zajištění bezpečnosti OT
    - Při posuzování bezpečnosti však chceme jít ideálně o krok dál…



Zdroj: NIST

Národní legislativa

- Jednoduchá gap analýza oproti požadavkům § 28 VoKB může poskytnout základní představu o případných slabých místech

§ 28

Průmyslové, řídicí a obdobné specifické systémy

Povinná osoba pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických systémů používá nástroje a opatření, které zajistí

a) použití technických a programových prostředků, které jsou určeny do specifického prostředí,

b) omezení fyzického přístupu k zařízením těchto systémů a ke komunikační síti,

c) vyčlenění komunikační sítě určené pro tyto systémy od ostatní infrastruktury,

d) omezení a řízení vzdáleného přístupu k těmto systémům,

e) ochranu jednotlivých technických aktiv těchto systémů před využitím známých zranitelností a

f) obnovení chodu těchto systémů po kybernetickém bezpečnostním incidentu.

ALEF

Zdroj: VoKB

IEC 62443

- Sada IEC 62443 obsahuje mj. standardy pro budování CSMS (2-1) i katalogy bezpečnostních opatření (3-3)
- Vedle formálních (i certifikačních) auditů tyto standardy vhodné i pro méně formální posuzování bezpečnosti OT
- Zejména části normy 3-3 dobře využitelné pro hodnocení bezpečnosti
  - Definuje 4 bezpečnostní úrovně (Security Level/SL), přičemž pro každou je uveden výčet požadovaných bezpečnostních opatření

IEC 62443-3-3 – bezpečnostní úrovně

4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

ALEF

Zdroj: IEC

Jednoduchý, osvědčený postup

- Rozdílová analýza proti požadavkům VoKB na OT (6 oblastí) a proti první bezpečnostní úrovni normy IEC 62443-3-3 (37 opatření) může být vhodným výchozím bodem pro komplexnější identifikaci nedostatků v zabezpečení
- Ve vyspělejších OT prostředích pak možno využít rovněž SL 2-4.

ALEF

Existence opatření negarantuje jejich efektivitu

- Samotná implementace bezpečnostních opatření nemusí znamenat, že daná opatření jsou vhodně nakonfigurována, nebo že efektivně brání před pravděpodobnými vektory útoků
- Bezpečnost OT prostředí je tak vhodné ověřovat i s pomocí praktických testů, a to jak v oblasti preventivních tak reaktivních bezpečnostních opatření

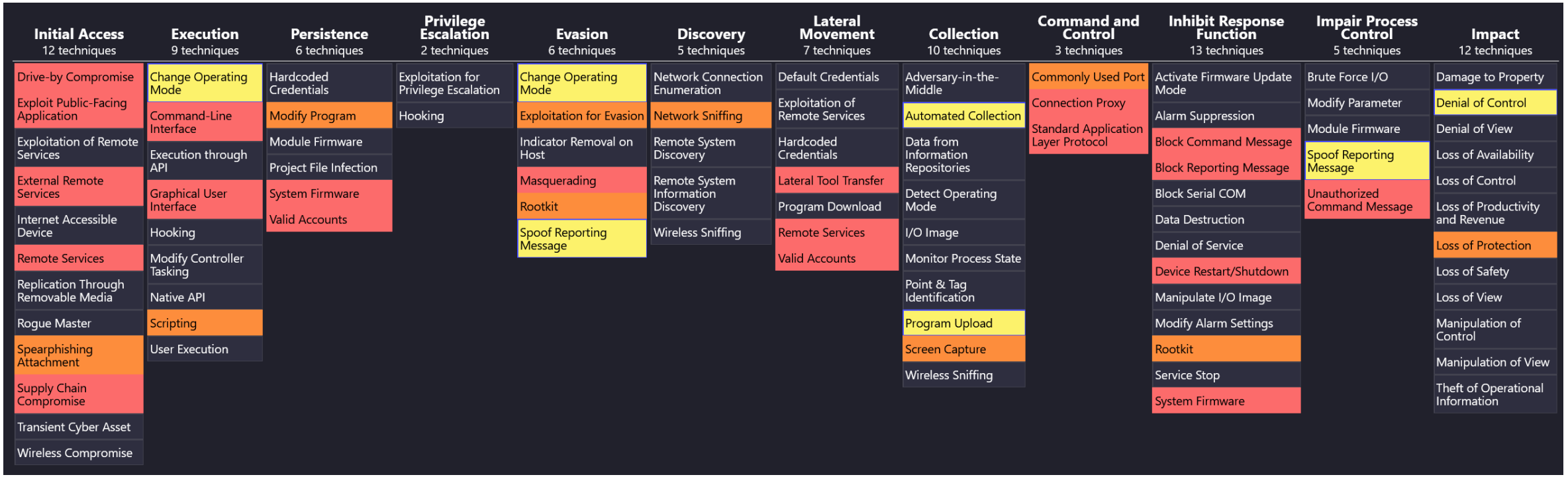
Penetrační testy a red teaming v OT

- Tradiční „infrastrukturní“ penetrační testy jsou pro OT prostředí omezeně využitelné
  - U IT infrastruktury v OT často možné vybrané obvyklé postupy a nástroje použít
  - U OT zpravidla vhodnější pasivní identifikace zranitelností a hloubkové technické posouzení jejich dopadů
- Vzhledem ke známé „vnitřní zranitelnosti“ OT prostředí může být vysoce přínosný i red teaming zaměřený na získání přístupu do OT z vnějšku

Testy rozsahu bezpečnostního dohledu

- Ověřovat efektivní fungování detekčních mechanismů lze relativně snadno (nástroje pro emulaci hrozeb, purple teaming, …)
- Významnější je, zda detekční schopnosti odpovídají hrozbám, které jsou pro organizaci a její OT relevantní
  - Nezbytné vytvořit model hrozeb pro cílové prostředí
    - Velmi dobře využitelný rámec MITRE ATT&CK
      - Matice Enterprise a ICS, případně hybridní matice dostupná v projektu Defending OT With ATT&CK

Žádoucí rozsah monitoringu lze snadno definovat



ALEF

Zdroj: MITRE

Co neměříme, nemůžeme řídit…

- Výše uvedené platí i o kybernetické bezpečnosti (nejen) v OT
- Identifikace jakýchkoli chybějících základních bezpečnostních opatření (VoKB, SL 1, …) je dobrý a nenáročný první „měřící“ krok
- Validace schopnosti reálně zabránit průniku do OT prostředí a/nebo jej detekovat je pak přinejmenším vhodným návazným krokem

ALEF

Děkuji Vám za pozornost