Implementace MITTRE ATT&CK pro průmyslové řídící a kontrolní systémy v kontextu objektů SEVESO III

(Analýza vektorů útoku na průmyslové řídící a kontrolní systémy v kontextu objektů SEVESO III)

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Dobeš, P. (pdobes@utb.cz)
Martiníková. B. (VŠB-TUO, FBI), Kotek, L. (VUT, FSI)

APROCHEM 2026, 22.4. (odpoledne), Hustopeče u Brna

Některé ilustrace: Microsoft Copilot

ICS (průmyslové řídící a kontrolní systémy)

https://www.softwareone.com/en/now/cybersecurity-forum#register

Cybersecurity is a critical priority.

Cost and complexity must no longer be a barrier.

Organizations must **defend the unpredictable**. As threats intensify, the demand for effective solutions continues to rise. Our events have seen unprecedented growth year after year, driven by the increasing urgency and relevance of this critical issue. The conversation is at its peak, and the need for action has never been more pressing.

In 2025...

52%
of cyberattacks are driven by extortion and ransomware.

87%
increase in destructive campaigns targeting cloud environments.

200%
increase in effectiveness of phishing due to AI.

VEKTOR ÚTOKU NA ICS

- V matematice a fyzice má **vektor** dva klíčové parametry: **velikost a směr.**
- V kyberbezpečnosti tento koncept přenášíme do analýzy útoků následovně:
  - **Sledování trajektorie:** Útok není izolovaný incident, ale řetězec kroků, který má svůj směr (například z podnikové sítě IT hlouběji do technologické sítě OT).
  - **Identifikace vektorů útoku:** Matice pomáhá definovat konkrétní cesty, kterými se útočník pohybuje. Každá technika v matici představuje jeden segment tohoto vektoru.
  - **Kvantifikace a analýza:** Rozdělením útoku na technické kroky můžeme „měřit“ efektivitu obrany v každém bodě této trajektorie.

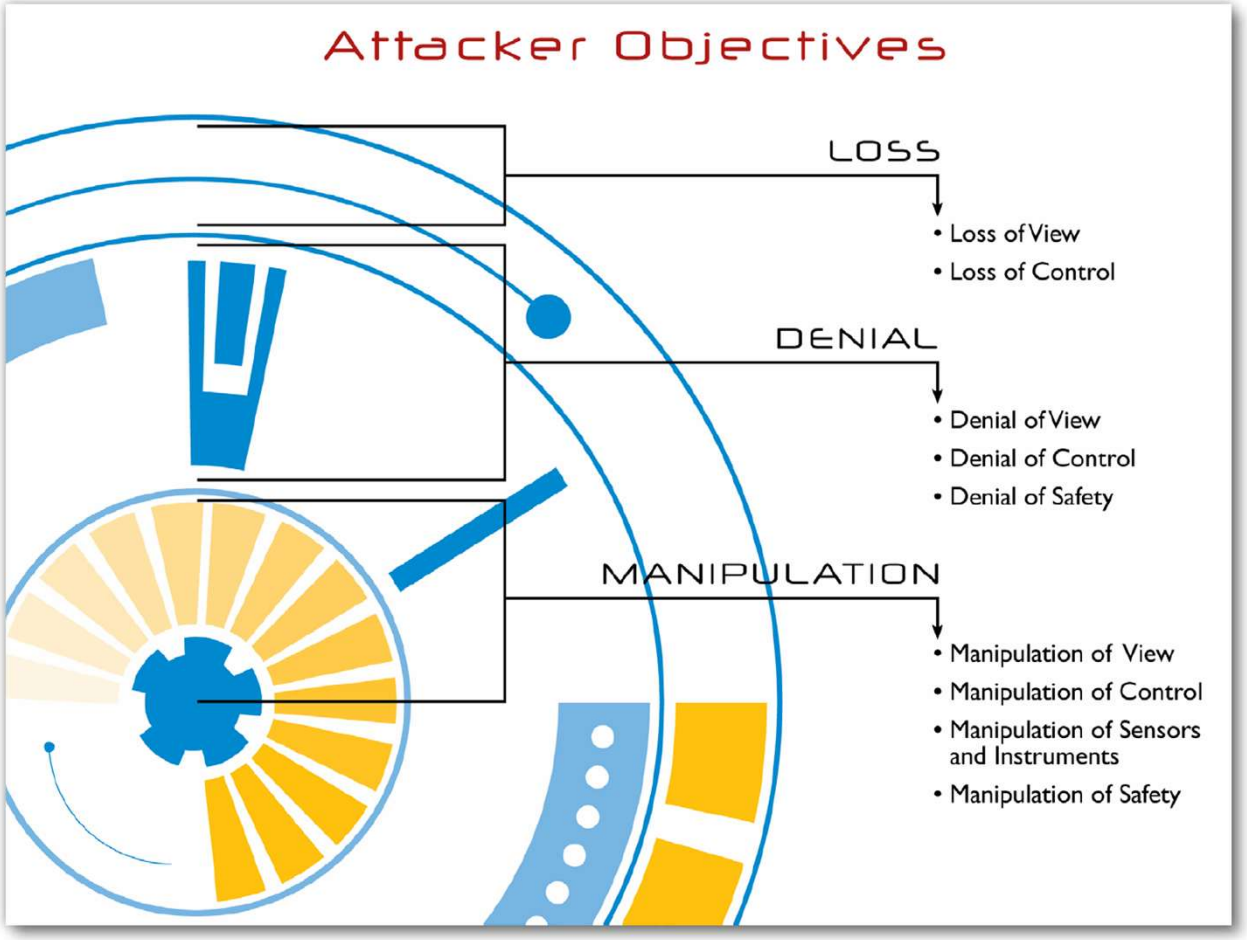
Vektorové metody pro analýzu možných kyberútoků v oblastech IT a OT:

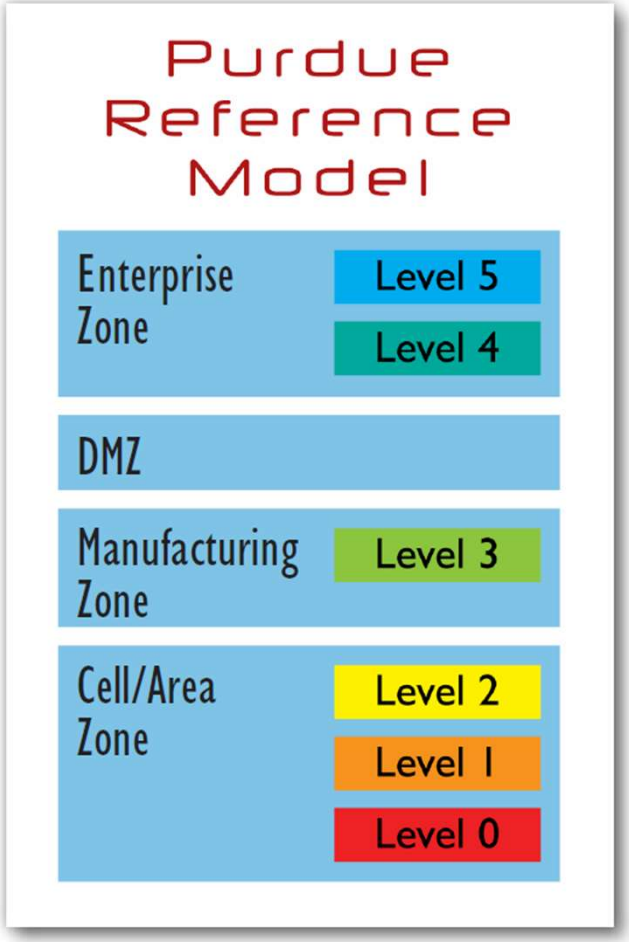
- Cyber Kill Chain (Lockheed Martin),
- Diamond model,
- matice MITRE ATT&CK (vybrána pro potřeby dalších analýz útoků)
- stromy útoků (Attack Trees),
- STRIDE (Microsoft)
- PASTA

při analýze a ošetřování kybernetických rizik pomáhají uvažované či zjištěné scénáře kybernetických útoků rozdělit na konkrétní technické kroky útočníka a navrhovat účinná opatření pro minimalizaci rizik.

ZJEDNODUŠENÝ KILL CHAIN NA ICS (VEKTOR ÚTOKU)

CÍLE útoku NA ICS, TYPICKÁ STRUKTURA SÍTĚ PRO ICS (PURDUE MODEL)

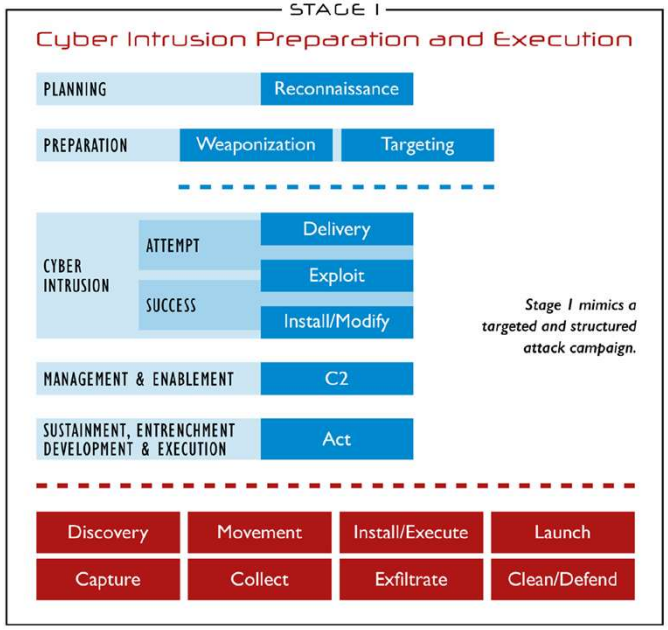


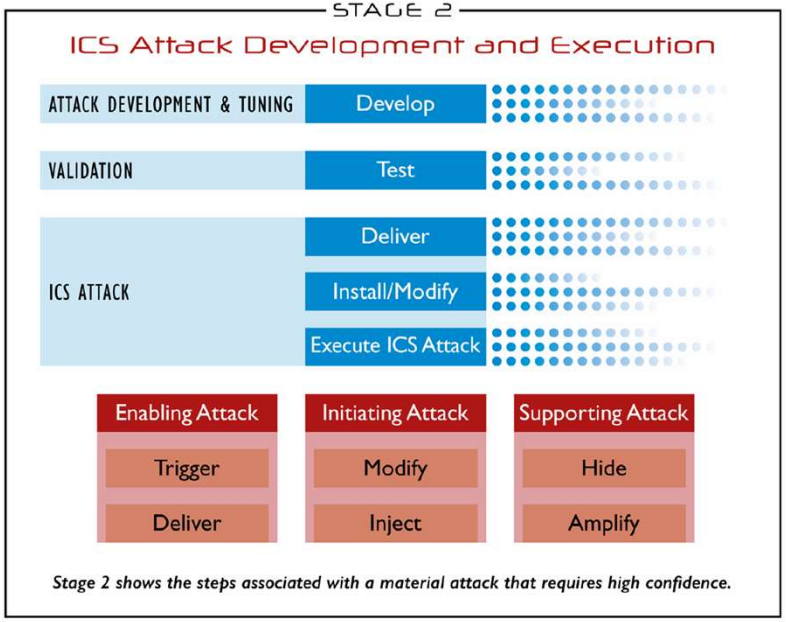


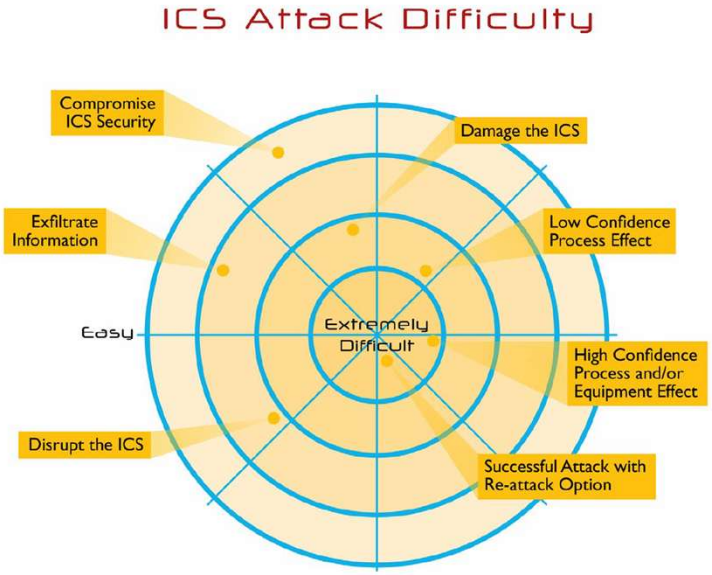
standard pro hierarchické rozdělení průmyslových sítí

ZDROJ: https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf

PODROBNĚJŠÍ fáze útoku NA ICS (dle přístupuCyber Kill Chain)







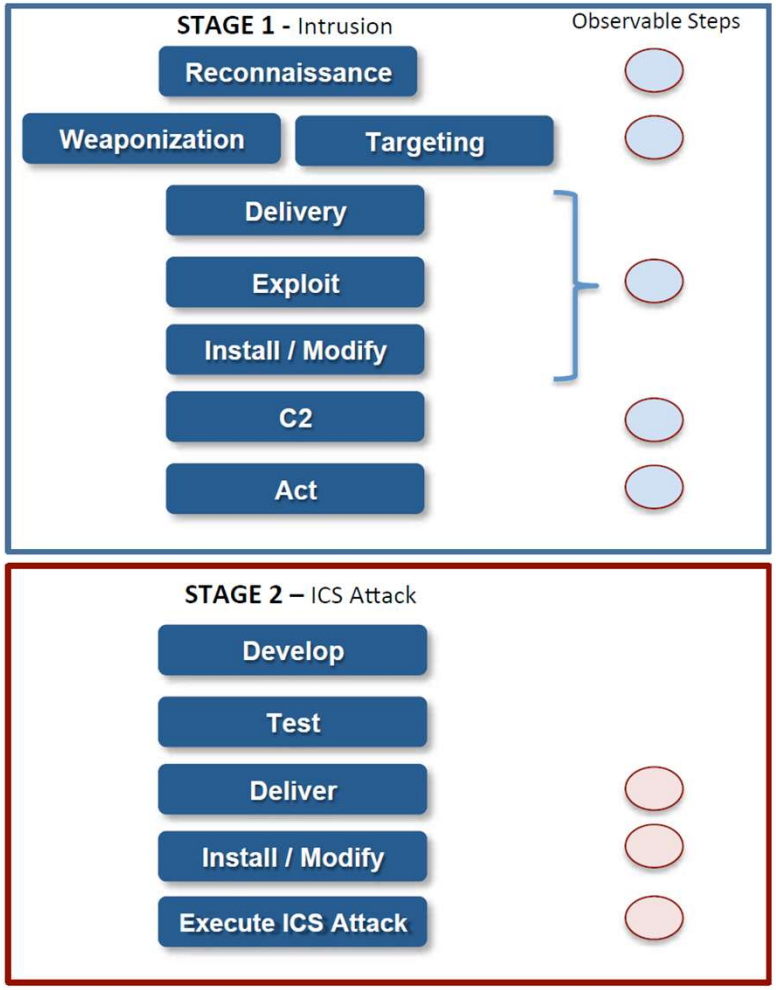
ZDROJ: https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf

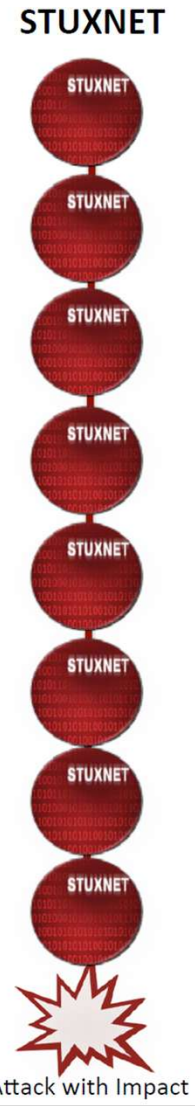
Příklady kybernetických útoků na ICS

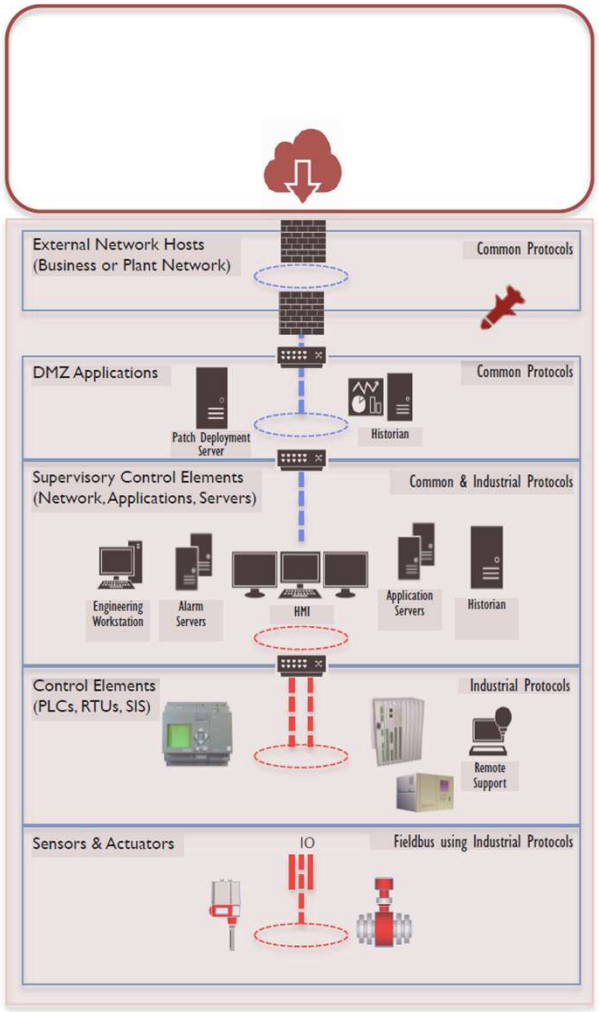
Stuxnet (2010)

- Příklad kybernetického útoku, navrženého k poškození průmyslového zařízení.
- Cílem bylo íránské zařízení na obohacování uranu v Natanzu.
- Malware manipuloval s programovatelnými automaty Siemens S7-315 a S7-417, řídícími centrifugy.
- Útok využíval čtyři dosud neznámé zranitelnosti (zero-day) a šířil se prostřednictvím infikovaných USB disků, čímž překonával bariéru vzdálenosti (air gap), oddělující technologickou síť (OT) od internetu (IT).
- Manipulací frekvence otáčení centrifug mezi 1410 Hz (přetáčení) a 2 Hz (praktické zastavení) způsobil mechanické namáhání vedoucí ke zničení přibližně 1 000 centrifug.
- Pro SEVESO objekty tento útok demonstroval, že i fyzicky izolované systémy mohou být kompromitovány a že manipulace s procesními parametry může způsobit destrukci zařízení.

Příklady kybernetických útoků na ICS







Příklady kybernetických útoků na ICS

BlackEnergy (2015) a **Industroyer /CrashOverride (2016)**

- Útok (spearphishing) cílil na ukrajinskou energetickou infrastrukturu.
- BlackEnergy zasáhl 3 distribuční společnosti pomocí spear-phishingu, následného pohybu laterálně sítí a přímé manipulace s HMI rozhraními metodou „phantom mouse" – vzdáleného ovládání kurzoru operátora.
- Útok způsobil výpadek elektřiny pro 230 000 odběratelů a využil metodu Kill Disk pro ztížení obnovy.
- Při útoku Industroyer o rok později prokázali hackeři hluboké znalosti průmyslových protokolů IEC 60870-5-101/104, IEC 61850 a OPC DA, které využili k přímé komunikaci s rozvodnou infrastrukturou, bez nutnosti využít jiné zranitelnosti.
- Základní legitimní příkazy protokolů postačovaly k manipulaci s vypínači (chybějící HW či SW bariéry).

Příklady kybernetických útoků na ICS

TRITON/TRISIS (2017)

- **Případ představuje asi dosud nejzávažnější útok z hlediska bezpečnosti procesů.**
- Cílil na ICS Schneider Electric Triconex v saudskoarabském petrochemickém závodě.
- Na rozdíl od předchozích útoků měl TRITON za cíl vyřadit poslední vrstvu ochrany bránící fyzické havárii.
- Malware využíval proprietární protokol TriStation, který útočníci museli reverzně analyzovat, a zero-day zranitelnost ve firmware řadičů Tricon pro získání privilegovaného přístupu.
- Útok byl odhalen pouze díky chybě v kódu, která způsobila aktivaci bezpečnostního mechanismu TMR (Triple Modular Redundancy) a nouzové odstavení závodu.

Pro SEVESO objekty TRITON prokázal, že bezpečnostní systémy navržené dle IEC 61511 mohou být cílem sofistikovaných útoků se záměrem způsobit ztráty na životech. (Abraham, 2025).

Příklady kybernetických útoků na ICS

Oldsmar – úpravna vody, Florida, USA (2021)

- útočník prostřednictvím vzdáleného přístupu (přes SW TeamViewer) zvýšil dávkování hydroxidu sodného (NaOH) ze 100 ppm na 11 100 ppm

Colonial Pipeline (2021)

- ransomware útok,
- vedl k odstavení klíčové palivové infrastruktury zásobující 45 % východního pobřeží USA po dobu 6 dnů.

Příklady kybernetických útoků na ICS

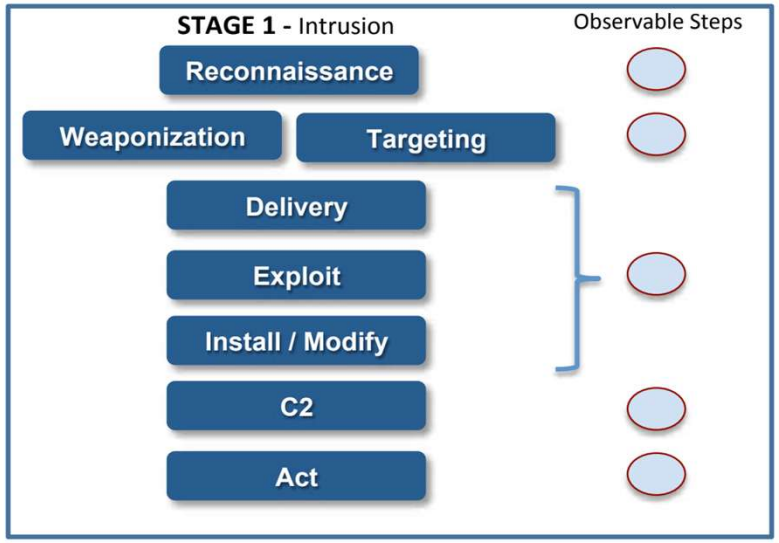
Malware Havex – ÚTOK POMOCÍ TROJSKÉHO KONĚ

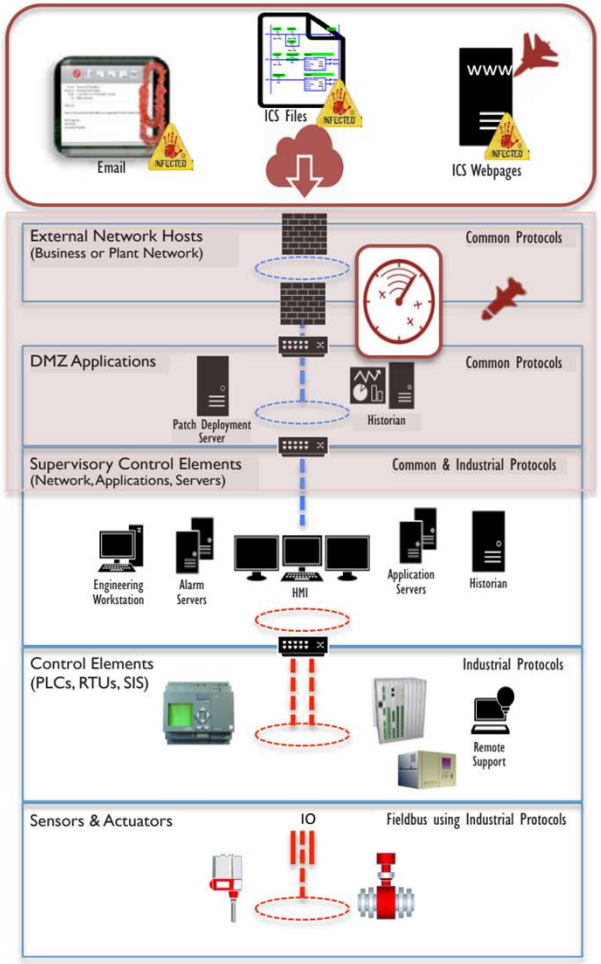
Účel: shromažďování citlivých dat a informací o síťové architektuře z tisíců lokalit po celém světě.

- Šlo o trojský kůň umožňující vzdálený přístup, který byl původně využíván k všeobecné špionáži a postupně se vyvinul v sadu nástrojů pro kriminální účely.
- Byl také upraven tak, aby cílil na ICS, a to přidáním nového kódu a modulů specifických pro prostředí ICS.
- Z veřejně dostupných informací bylo zjištěno, že kampaň probíhala po dobu nejméně tří let.
- Útočníci stojící za Havexem využili několik metod k proniknutí malwaru Havex do sítí:
  - Zasílání spearphishingových e-mailů s přiloženým škodlivým souborem
  - Infikování webových stránek dodavatelů ICS malwarem a ohrožení obránců ICS při návštěvě těchto webových stránek (známé jako technika „watering hole“)
  - Poskytování trojanizované verze instalačních programů (aktualizační balíčky SW, firmware pro ICS), které infikovaly hostitelský systém poté, co zaměstnanci spustili proces aktualizace.

ZDROJ: https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf

KILL CHAIN NA ICS (VEKTOR ÚTOKU),HAVEX TROJAN MALWARE





ZDROJ: https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf

Směrnice NIS2 (2022/2555) - přímý legislativní základ pro kyberbezpečnost KI.

- Chemický průmysl spadá pod Přílohu II jako důležitý subjekt (výroba, produkce a distribuce chemických látek), přičemž velké podniky v sektoru mohou být klasifikovány jako základní subjekty.
- Článek 21 směrnice vyžaduje implementaci technických, provozních a organizačních opatření pro řízení kybernetických rizik včetně politik analýzy rizik, zvládání incidentů, kontinuity činností a bezpečnosti dodavatelského řetězce.
- Směrnice stanovuje povinné hlášení incidentů ve třech fázích:
  - včasné varování do 24 hodin,
  - oznámení do 72 hodin a
  - závěrečná zpráva do jednoho měsíce.
- Maximální sankce dosahují 10 milionů EUR nebo 2 % celosvětového obratu pro základní subjekty.

Novela českého zákona o kybernetické bezpečnosti (č. 264/2025 Sb.) transponující NIS2, platný od nabyl účinnosti 1. listopadu 2025.

- Zavádí 2úrovňový režim:
  - režim vyšších povinností pro subjekty strategického významu
  - režim nižších povinností pro důležité subjekty.
- Česká implementace jde nad rámec minimálních požadavků NIS2 tím, že vyžaduje hlášení všech kybernetických incidentů, nikoli pouze významných.
- Národní kompetentní orgán s pravomocí ukládat pokuty až do výše 250 milionů Kč, včetně realizace opatření vůči statutárním orgánům firem a organizací při opakovaných nebo závažných porušeních – NÚKIB.
- ? Pro objekty SEVESO III (zejména zařazené do skupiny B), které současně spadají (nebo budou spadat) pod NIS2, (pravděpodobně / možná?) vznikne povinnost integrace požadavků, zahrnutí kybernetických hrozeb do bezpečnostních zpráv (BZ PZH), jako potenciálních iniciačních událostí, rozšíření systému řízení bezpečnosti o kybernetická opatření, koordinaci hlášení incidentů na MŽP a NÚKIB, a rovněž začlenění kybernetických scénářů rizik do vnitřních a vnějších havarijních plánů.

LEGISLATIVA – patří váš podnik mezi tzv. regulované služby?

- https://www.zakonyprolidi.cz/cs/2025-264 (novela zákona o kybernetické bezpečnosti)
- https://www.umimenis2.cz/jak-probiha-registrace-na-portal-nukib/

- https://www.zakonyprolidi.cz/cs/2025-266 *Zákon o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře).*

POZN: Podle návrhů prováděcích vyhlášek k loni novelizovanému zákonu, to zatím nevypadá na to, že by SEVESO podniky ve skupině B všechny automaticky spadaly do působnosti z. č. 266).

(Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.)

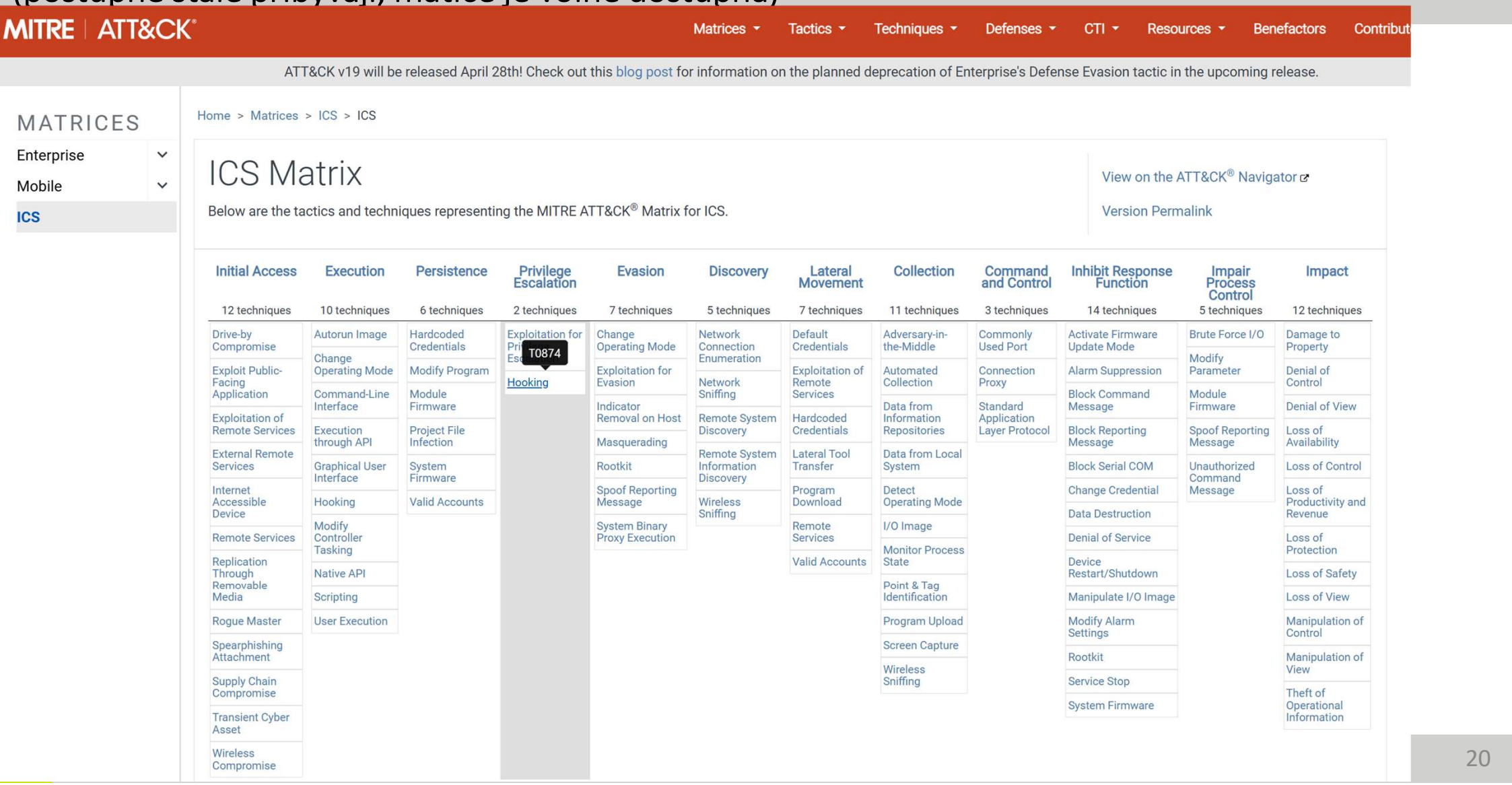
Výběr metody pro analýzu vektorů kybernetických útoků na ICS

MATICE MITRE ATT&CK = metoda klasifikace a popisu chování útočníků.

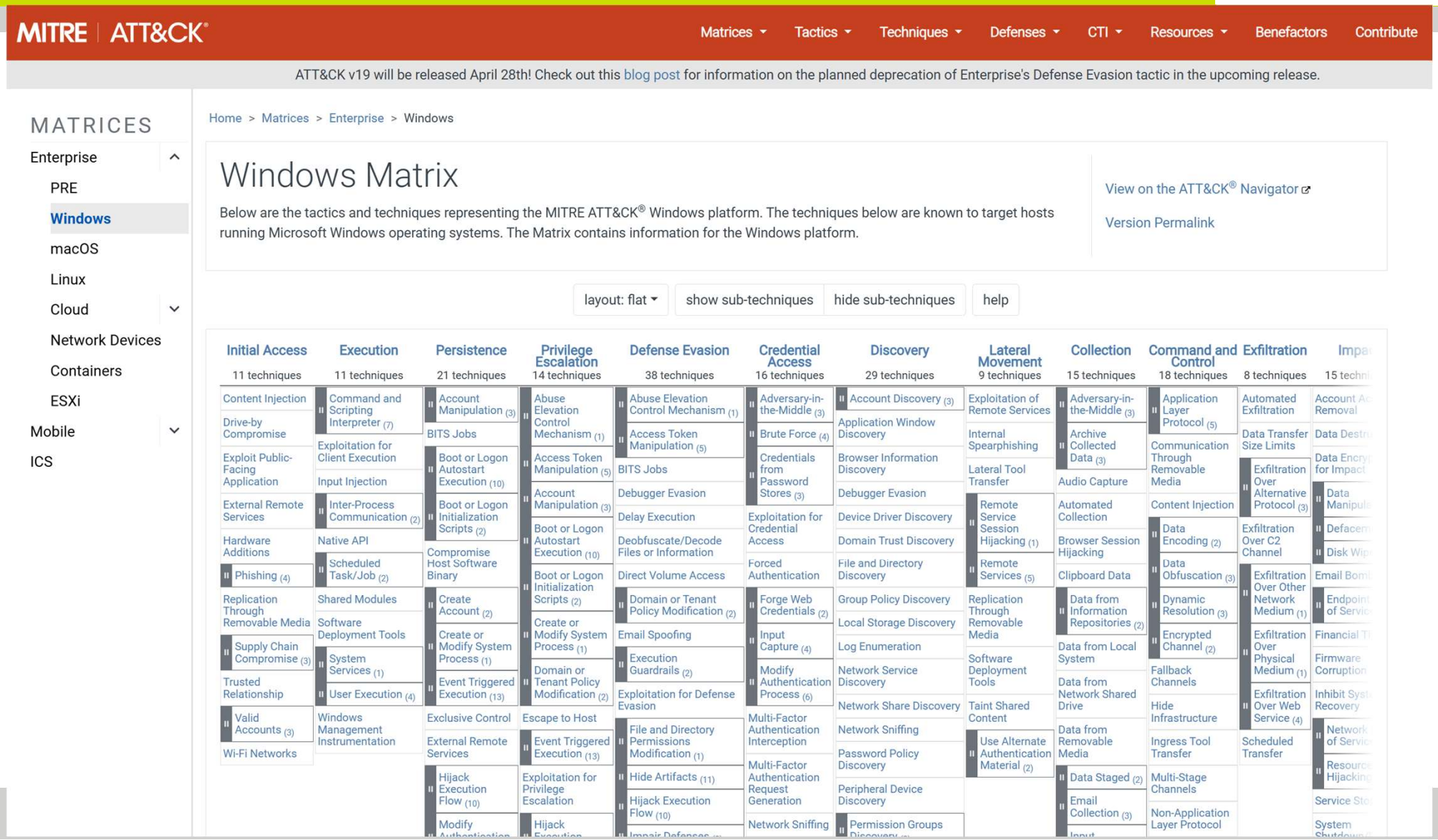
Zaměřuje se na:

- Taktiky, techniky a postupy útočníků. Poskytuje v podstatě taxonomický slovník taktik. **Místo vágního „hackli nás“ díky matici lze říci a popsat: „Útočník použil taktiku získání počátečního přístupu (initial access) skrze techniku vnějších vzdálených služeb (external remote services, s kódovým označením T0822).“**
- Modelování hrozeb (threat modeling). Metoda pomáhá simulovat, jak by reálný útok na vybranou infrastrukturu mohl vypadat.
- Analýza mezer (gap analysis). Zároveň je to metoda vhodná pro zjištění, které technické kroky útočníka dokáže obránce (provozovatel a jeho správci informačních systémů) spíše detekovat, a které jsou pro něj pravděpodobně spíše „neviditelné“.
- Poskytuje i seznamy možných způsobů obrany (mitigační a detekční opatření).
- Je průběžně doplňována a upravována dle vývoje v oblasti KB.

Aktuální popsané taktiky a techniky vektorů útoku na ICS systémy (postupně stále přibývají, matice je volně dostupná)



Aktuální popsané taktiky a techniky vektorů útoku na Enterprise systémy



Aktuální popsané taktiky a techniky vektorů útoku na mobilní přístroje (iOS)

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

ATT&CK v19 will be released April 28th! Check out this blog post for information on the planned deprecation of Enterprise's Defense Evasion tactic in the upcoming release.

MATRICES

Enterprise

Mobile

Android

iOS

ICS

Home > Matrices > Mobile > iOS

iOS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® iOS platform. The techniques below are known to target mobile devices running iOS operating systems. The Matrix contains information for the iOS platform.

View on the ATT&CK® Navigator

Version Permalink

layout: flat | show sub-techniques | hide sub-techniques | help

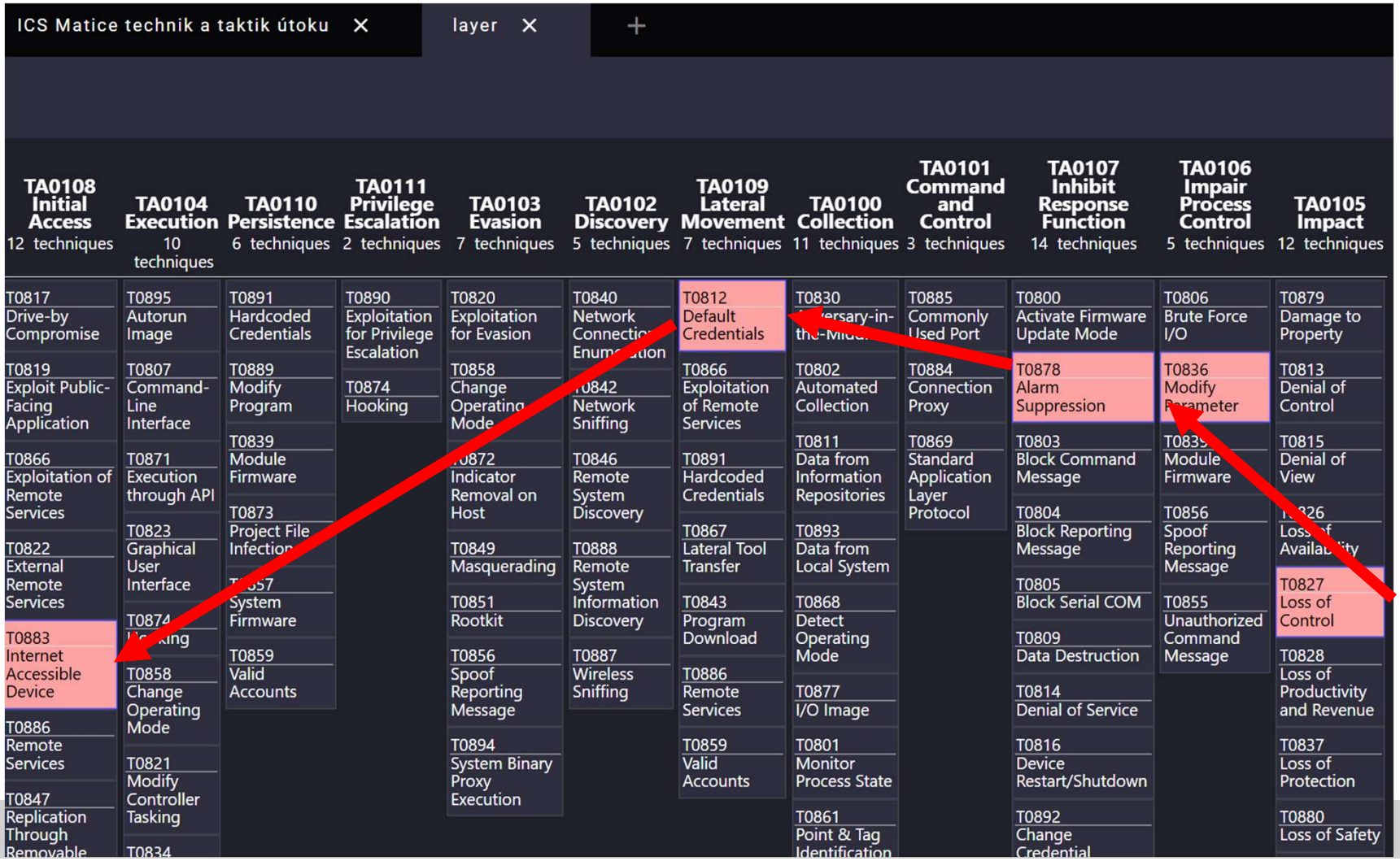
Initial Access (8 techniques)	Execution (3 techniques)	Persistence (4 techniques)	Privilege Escalation (2 techniques)	Defense Evasion (9 techniques)	Credential Access (4 techniques)	Discovery (7 techniques)	Lateral Movement (2 techniques)	Collection (11 techniques)	Command and Control (8 techniques)	Exfiltration (2 techniques)	Impact (3 techniques)
Application Versioning	Command and Scripting Interpreter (1)	Boot or Logon Initialization Scripts	Exploitation for Privilege Escalation	Application Versioning	Clipboard Data	File and Directory Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol (1)	Exfiltration Over Alternative Protocol (1)	Endpoint Denial of Service
Drive-By Compromise	Exploitation for Client Execution	Compromise Client Software Binary	Process Injection (1)	Download New Code at Runtime	Credentials from Password Store (1)	Location Tracking (2)	Replication Through Removable Media	Archive Collected Data	Dynamic Resolution (1)	Exfiltration Over C2 Channel	Generate Traffic from Victim
Exploitation for Initial Access	Scheduled Task/Job	Linked Devices		Execution Guardrails (1)	Input Capture (2)	Network Service Scanning		Audio Capture	Encrypted Channel (3)		Network Denial of Service
Lockscreen Bypass		Scheduled Task/Job		Indicator Removal on Host (1)	Steal Application Access Token (1)	Process Discovery		Clipboard Data	Ingress Tool Transfer		
Phishing				Masquerading (1)		Software Discovery (1)		Data from Local System	Non-Standard Port		
Replication Through Removable Media				Obfuscated Files or Information (1)		System Information Discovery		Input Capture (2)	Out of Band Data		
SIM Card Swap				Process Injection (1)		System Network Configuration Discovery (2)		Linked Devices	Remote Access Software		
Supply Chain Compromise (3)				Subvert Trust Controls (1)				Location Tracking (2)	Web Service (3)		
				Virtualization/Sandbox Evasion (1)				Protected User Data (5)			
								Stored Application Data			
								Video Capture			

Scénář I.: Nekontrolovaná (exotermická) reakce, samovolně se zrychlující (runaway reaction)

- Tento scénář simuluje útok na reaktor, kde je kritické chlazení a míchání.
- Cíl: Vyvolat neřízený nárůst teploty a tlaku v reaktoru.
- Využité techniky MITRE (uvedeny anglicky, dle originálu matice MITRE on-line):
  - **Impair process control (T0827):** Útočník manipuluje s logikou PLC, aby uzavřel ventily chladicího média.
  - **Modify parameter (T0836):** Změna žádané hodnoty (setpoint) pro dávkování katalyzátoru na maximum.
  - **Alarm suppresion (T0878):** Zablokování alarmů, aby operátor včas nezasáhl.
- Vrcholová událost: nekontrolovaná reakce, následovaná explozí nádoby (zdroje rizika, reaktoru, destilační kolony, …) v důsledku překročení konstrukčního tlaku.

Vizualizace scénáře I. pro potřeby analýz, akcí red týmů, pen. testování:

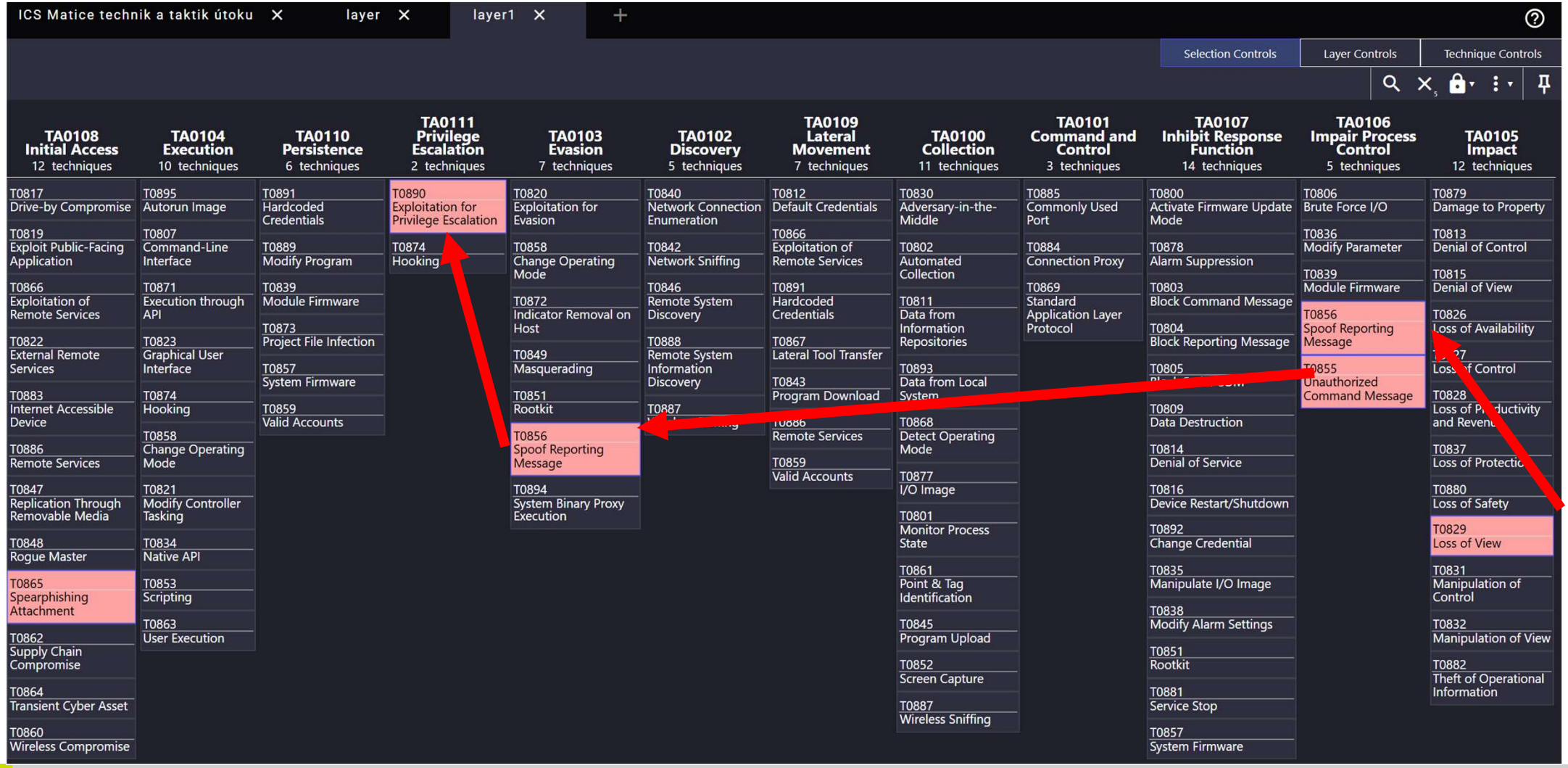
- https://mitre-attack.github.io/attack-navigator/



Scénář II.: Ztráta obsahu (loss of containment, únik nebezpečných látek)

- Zaměřen na skladovací terminály (např. zkapalněné plyny pod tlakem).
- Cíl: Přetečení nádrže nebo mechanické porušení potrubí.
- Využité techniky MITRE:
  - **Spoof reporting message (T0856):** Falešné hlášení hladinoměru (stále ukazuje "bezpečno"), zatímco čerpadla běží.
  - **Unauthorized command message (T0855):** Vzdálené otevření vypouštěcích ventilů do nechráněných, nezajištěných prostor.
  - **Loss of view (T0829):** Odpojení obrazovek na dispečinku (HMI), aby operátor zčásti nebo úplně ztratil přehled o stavu provozu.
- Vrcholová událost: Ztráta obsahu – toxický mrak nebo únik hořlavé kapaliny do okolí zdroje rizika.

Vizualizace scénáře II. pro potřeby analýz, akcí red týmů, pen. testování:

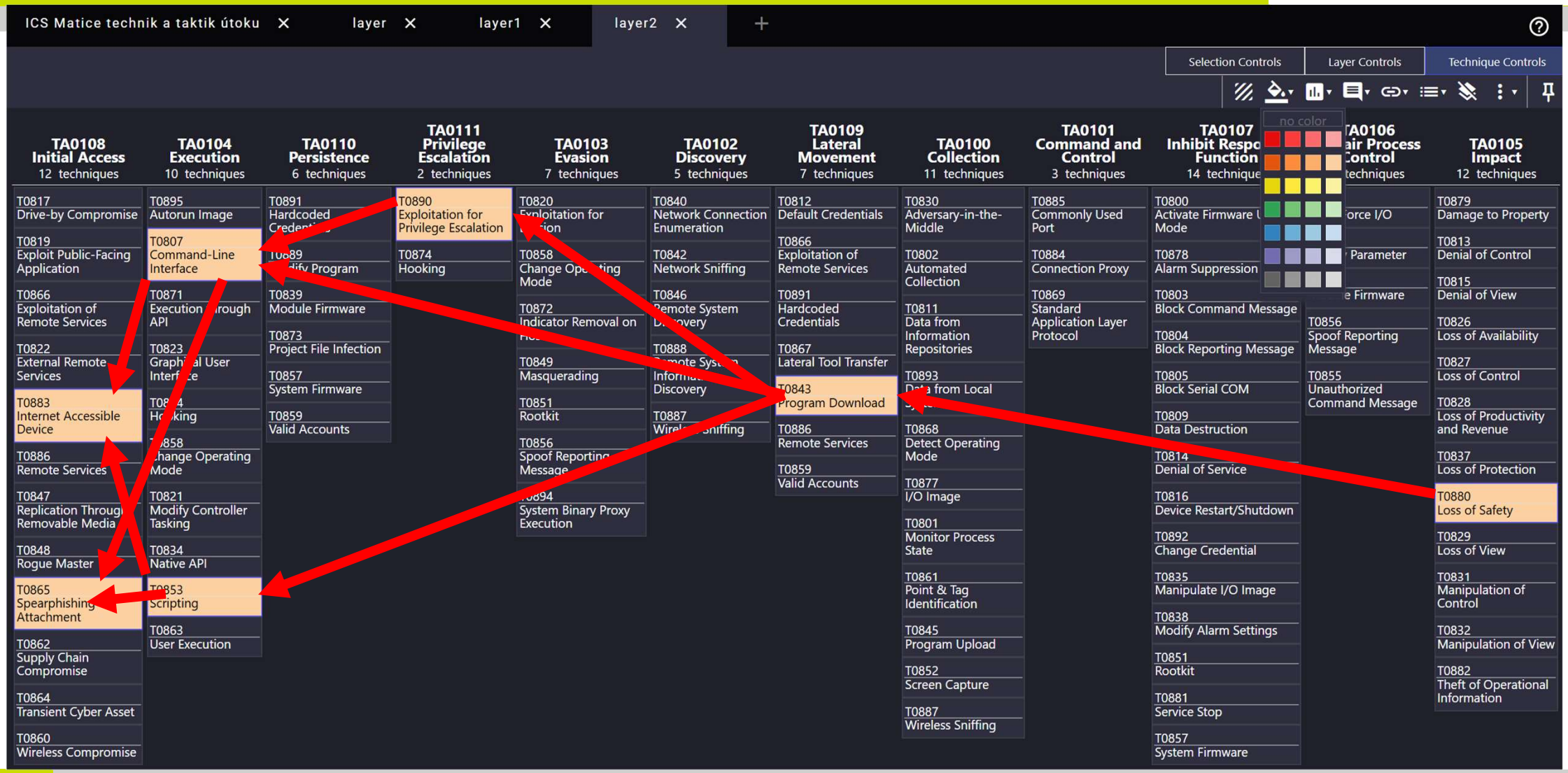


Scénář IV.: Ztráta zabezpečení (Loss of safety function, ochrnutí bezpečnostních systémů)

- Tento scénář cílil na systémy SIS (Safety Instrumented Systems).
- Cíl: Vyřadit poslední linii obrany a bezpečnostní systémy před vznikem, případně rozvojem havárie.
- Využité techniky MITRE:
  - **Loss of safety (T0880):** Přepsání logiky bezpečnostního PLC (např. TRICONEX), aby ignorovalo mezní stavy.
  - **Program download (T0843):** Nahrání modifikovaného projektu do bezpečnostního kontroléru, který deaktivuje nouzové odstavení (ESD).
- Vrcholová událost: Samotná technika nevyvolá havárii okamžitě, ale připraví podmínky pro to, aby běžná provozní porucha (např. výpadek čerpadla) přerostla v katastrofální havárii, protože bezpečnostní systém nezareaguje.

Vizualizace scénáře IV. pro potřeby analýz, akcí red týmů, pen. testování.

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení



1. Průnik do IT sítě a rekognoskace

- Vše začíná klasikou: phishingem, kompromitací VPN nebo zneužitím neošetřené zranitelnosti na serveru v intranetu. Jakmile je útočník v běžné Windows/Unix síti, nehledá Excel tabulky, ale **mosty**.
- **Hledání spojnic:** Útočník skenuje síť a hledá zařízení, která mají dvě síťové karty (tzv. *dual-homed*). Jedna karta kouká do kanceláří, druhá do výroby.
- **Identifikace cílů:** Hledají se servery s názvy jako „SCADA“, „Historian“, „HMI“ nebo „Engineering Workstation“.

2. Průlom přes DMZ nebo "Jump Server"

- V moderních podnicích jsou IT a OT sítě odděleny firewallem (často v demilitarizované zóně – DMZ). Útočník se musí dostat přes tento kontrolní bod.
- **Zneužití Jump Serveru:** Správci často používají jeden konkrétní počítač, ze kterého se vzdáleně připojují do výroby (přes RDP nebo SSH). Pokud útočník tento stroj ovládne, má „legitimní“ vstupenku do výrobní haly.
- **Zneužití důvěry:** Pokud firewall dovoluje přenos souborů (např. pro aktualizace softwaru PLC), útočník může zkusit propašovat škodlivý kód v rámci těchto balíčků.

3. Ovládnutí inženýrské stanice (EWS - Engineering Workstation)

- Tohle je **Svatý grál**. Inženýrská staniceje počítač, na kterém běží software od firem jako Siemens, Rockwell nebo Schneider Electric. Tento počítač má přímou moc měnit program v PLC.
- **Keylogging:** Útočník sleduje, jaké kódy a hesla inženýr zadává do softwaru (např. TIA Portal).
- **DLL Hijacking:** Útočník podvrhne knihovnu přímo v inženýrském softwaru. Když inženýr klikne na „Nahrát program do PLC“, software nevědomky přibalí i útočníkův škodlivý kód (payload).

3. Ovládnutí inženýrské stanice (EWS - Engineering Workstation)

- Tohle je **Svatý grál**. Inženýrská staniceje počítač, na kterém běží software od firem jako Siemens, Rockwell nebo Schneider Electric. Tento počítač má přímou moc měnit program v PLC.
- **Keylogging:** Útočník sleduje, jaké kódy a hesla inženýr zadává do softwaru (např. TIA Portal).
- **DLL Hijacking:** Útočník podvrhne knihovnu přímo v inženýrském softwaru. Když inženýr klikne na „Nahrát program do PLC“, software nevědomky přibalí i útočníkův škodlivý kód (payload).

4. Komunikace s PLC kartou (OT protokoly)

- Jakmile je útočník na stroji, který vidí na PLC, musí začít mluvit „jejich řečí“. Běžné IT protokoly (HTTP, SMB) jsou mu k ničemu.
- **Průmyslové protokoly:** Útočník použije knihovny pro protokoly jako **Modbus, Profinet, EtherNet/IP nebo S7comm**.
- **Využití chybějící autentizace:** Šokující pravdou je, že mnoho starších PLC (tzv. legacy systems) nemá **žádné heslo**. Pokud na ně „uvidíte“ v síti a pošlete správně zformátovaný paket STOP, PLC se prostě zastaví.
- **Firmware útok:** Útočník se může pokusit nahrát do PLC modifikovaný firmware, který zajistí, že se stroj bude chovat podle jeho pokynů, zatímco operátor na obrazovce (HMI) uvidí, že je vše v pořádku (tzv. *Stuxnet styl*).

Jak se tomu bránit? Cesta do hlubin stroje OT

Aby nedošlo ve finále k úspěšnému kyberútoku na OT, profíci nasazují několik vrstev obrany:

1) **Segmentace sítě:** Důsledné oddělení IT a OT (žádné sdílené tiskárny, přes zastaralý zranitelný protokol, port, službu).
2) **MFA (Vícefaktorové ověřování):** I když útočník ukradne heslo na vstupní server, bez druhého faktoru se do výroby nedostane.
3) **IDS pro OT:** Speciální senzory, které hlídají anomálie v průmyslových protokolech (např. „Proč se někdo snaží přepsat program v PLC ve 3 ráno?“).
4) **Data diody:** Hardware, který fyzicky dovoluje tok dat pouze jedním směrem (z výroby ven na monitoring), ale nikdy ne dovnitř.
5) **V PLC kartách:** šifrované a podepsané protokoly, integrovaný Firewall a Access Control Listy (ACL)
6) **Hardwarové přepínače** (analogová obrana, Moderní PLC mají fyzický klíček nebo přepínač (RUN / STOP / TERM).Moderní PLC mají fyzický klíček nebo přepínač (RUN / STOP / TERM).)

Je to v podstatě neustálá hra na kočku a myš, kde je nejslabším článkem bohužel často zapomenutý servisní notebook připojený k oběma sítím naráz.

Jak se tomu bránit? Strategie „Opevnění“ bez výměny všech strojů a PLC

Výměna všech PLC v továrně je drahá a na dlouho.

Proto se častěji používá tzv. **Defense-in-Depth** (Obrana do hloubky):

- **Průmyslový firewall (Industrial Security Appliance):** Před staré PLC s Modbusem se postaví malá krabička (např. Cisco ISA, Phoenix Contact mGuard). Ta funguje jako „ochranka“. Filtruje provoz a do PLC pustí jen legitimní pakety.
- **Detekce anomálií (IDS):** Systém (např. Nozomi, Claroty), který se „učí“, jak vypadá běžný provoz. Pokud najednou začne váš skript skenovat registry, IDS okamžitě spustí alarm, protože to není „normální chování“.
- **VLAN a Mikrosegmentace:** Rozdělení sítě tak, aby se z jednoho napadeného Unix serveru v intranetu útočník nedostal na celou výrobní linku, ale jen do úzké chodbičky, která nikam nevede.

Pomůže výměna starých PLC za novější s lepším certifikátem SIL1, SIL2?

Výměna za novější PLC rozhodně pomůže, ale samotný certifikát **SIL (Safety Integrity Level)** vás před hackerem nutně neochrání. Pojďme si to rozklíčovat, protože je to kritický rozdíl.

Safety vs. Security: V čem je háček?

Vlastnost	**Functional Safety (SIL)**	**Cybersecurity (IEC 62443)**
Cíl	Ochrana lidí a prostředí před poruchou stroje.	Ochrana stroje před zlým úmyslem člověka.
Hrozba	Náhodné hardwarové chyby, únava materiálu.	Cílený útok, virus, zneužití protokolu.
Příklad	„Když selže procesor, ventil se musí zavřít.“	„Nepusť k ventilu nikoho bez certifikátu.“

Průmyslová „latina” – např. Modbus protokol

- Starý, jednoduchý, mluví jím skoro každý, ale nikdo se v něm neobtěžoval řešit zabezpečení.
- Modbus původně vznikl v roce 1979 pro komunikaci přes sériové linky, a když se později „navlékl“ na TCP/IP (port 502), na bezpečnost se úplně zapomnělo:

Modbus trpí 3 zásadními nedostatky, které útočníkovi hrají do karet:

- **Žádná autentizace:** Kdokoliv, kdo se dokáže připojit na port 502, může posílat příkazy. PLC se neptá „Kdo jsi?“, prostě poslechne.
- **Žádné šifrování:** Veškerá komunikace běží v čistém textu. Pokud útočník „odposlouchává“ síť, vidí přesně, co se v továrně děje.
- **Žádná integrita:** Neexistuje způsob, jak ověřit, že příkaz skutečně poslal řídicí systém a ne útočník.

1. Skenování a mapování (Reconnaissance)

- Útočník nejprve zjistí, co je na síti. Použije nástroje jako nmap se skripty pro Modbus, aby zjistil **Unit ID** (identifikátor zařízení) a typ zařízení.
- **Cíl:** Najít tzv. **Registry**. To jsou v podstatě adresy v paměti PLC, kde jsou uloženy hodnoty (např. teplota, otáčky motoru, stav ventilu).

2. Čtení dat (Information Theft)

- Pomocí funkcí pro čtení (např. *Function Code 03 - Read Holding Registers*) začne útočník vysávat data z PLC.
- **Příklad:** Útočník zjistí, že na adrese 40001 je uložena cílová teplota kotle. Vidí, že je nastavená na 80 °C.

3. Zápis a manipulace (Command Injection)

- Tohle je ta nebezpečná část. Útočník použije funkci pro zápis (např. *Function Code 06 - Write Single Register* nebo *16 - Write Multiple Registers*).
- **Scénář „Sabotáž“:** Útočník pošle příkaz k přepsání hodnoty na adrese 40001 z 80 °C na 200 °C. Pokud PLC nemá vnitřní logické pojistky, začne kotel nekontrolovaně hřát.
- **Scénář „DoS“ (Denial of Service):** Útočník začne PLC bombardovat nesmyslnými požadavky tak rychle, že procesor PLC zamrzne a celá linka se zastaví.

4. Replay attack (Útok opakováním)

- Útočník nahraje legitimní komunikaci mezi operátorem a strojem (např. „otevřít ventil“). Později, když se mu to hodí, tento záznam prostě „pustí“ do sítě znovu. PLC nepozná rozdíl a ventil otevře, i když je to v tu chvíli nežádoucí.

Příklad částí Python scriptu, cílího na ICS systém

Útočníci k tomu nepotřebují žádný složitý software. Stačí jim:

- **Metasploit Framework:** Obsahuje moduly přímo pro skenování a zápis do Modbus registrů.
- **Python (knihovna pymodbus):** Pár řádků kódu stačí k tomu, aby skript v nekonečné smyčce vypínal motor pokaždé, když ho operátor zapne.

```
# Ukázka jednoduchého (a nebezpečného) Python skriptu
from pymodbus.client import ModbusTcpClient
client = ModbusTcpClient('192.168.1.50') # IP adresa PLC ve výrobě
client.connect()
# Zapíše hodnotu 1 (ON) do registru 10, což může být třeba alarm
client.write_register(10, 1)
client.close()
```

Jak Modbus vyléčit?

Protože protokol samotný opravit nejde (změna by znefunkčnila miliony zařízení), řeší se to **obálkou**:

- **Modbus Secure:** Novější verze protokolu, která přidává TLS šifrování a certifikáty (bohužel se nasazuje pomalu).

- Průmyslové firewally (Deep Packet Inspection): Tyto firewally nekoukají jen na to, odkud data jdou, ale *co* říkají. Pokud firewall vidí, že se někdo snaží zapsat do registru pro „nouzové zastavení“ a není to autorizovaná inženýrská stanice, paket zahodí.

Diskuse – svět IT (enterprise, mobile) vs. OT (ICS)

Vlastnost	IT (informační technologie)	OT (provozní technologie)
Priorita **(triáda)**	Hlavním cílem je důvěrnost (aby data nikdo nepřečetl). **C-I-A** (confidentiality - integrity - availability)	Hlavním cílem je dostupnost a bezpečnost (aby stroj běžel a nikoho nezabil). **A-I-C** (availability - integrity - confidentiality)
Životní cyklus	Krátký (3–5 let, rychlá obměna)	Dlouhý (15–30 let, stroje z 90. let nejsou v průmyslu velkou výjimkou)
Dostupnost	Výpadky jsou nepříjemné (restart je běžný)	Výpadek je kritický (restart může trvat dny nebo zničit stroj)
Patchování (aktualizace)	Časté a automatizované	Vzácné, vyžaduje odstávku a testování bezpečnosti
Prostředí	Klimatizované kanceláře, čisté servery	Prašné haly, vibrace, extrémní teploty
Protokoly	Standardní (HTTP, TCP/IP, SMTP, …)	Specifické (Modbus, Profibus, DNP3, EtherCAT, …)

DISKUSE - svět IT (enterprise, mobile) vs. OT (ICS)

Dříve byly OT sítě od IT sítí více izolované (oddělené).

- Systémy IT byly určeny primárně pro zpracování, ukládání a přenos informací:
  - e-maily, databáze, systémy plánování podnikových zdrojů, webové servery, apod.).
- Systémy provozních technologií (OT) představují zejména hardware a software, detekující či způsobující změnu prostřednictvím přímého monitoringu a řízení fyzických zařízení:
  - programovatelné logické automaty (PLC), robotická ramena, snímače tlaku či ventily.

DISKUSE - svět IT (enterprise, mobile) vs. OT (ICS)

Dnes se tyto světy stále více propojují (Průmysl 4.0, IIoT) a projevuje se fenomén jejich konvergence.

- IT chce data z výroby, aby mohlo optimalizovat byznys.
- OT se začíná podobat IT (používá Windows, Linux, Wi-Fi).

Když do OT světa pronikne malware z IT (třeba přes infikovaný e-mail účetní), tradiční IT ochrana (např. agresivní skenování sítě) může paradoxně OT systémy shodit, protože jsou velmi citlivé na latenci a neobvyklý síťový provoz.

ZÁVĚR

- Příspěvek se snažil zprostředkovat praktický návod s příklady pro analytiky rizik a manažery bezpečnosti, jak pomocí matice MITRE ATT&CK pro ICS (nebo jiné podobné vektorové metody) mapovat zranitelnosti specifických průmyslových komponent (PLC, HMI, SIS).
- Tento přístup umožňuje proaktivní zjišťování možných hrozeb a může pomoci včasné detekci kybernetických hrozeb proti ICS zařízením
- Na teoretickou analýzu vektorů možných útoků nejen na ICS systémy by dále mělo v bezpečnostní praxi navazovat testování odolnosti kritických ICS, s využitím metody fyzických či digitálních dvojčat v izolovaném prostředí. (HLEDÁME PARTNERY PRO TESTOVÁNÍ a OVĚŘENÍ ZABEZPEČENÍ ZÁJMOVÝCH SETUPŮ. *Zájem už projevilo VŠB-TUO, VĚC, dohledové centrum pro fotovoltaické elektrárny. Máme kontakty a dřívější spolupráci s firmou ELVAC.*
- Souběžně by měly být v rámci prevence a mitigace navrhovány opatření pro posílení odolnosti kritické infrastruktury, v souladu s principy "Security by Design".
- To zahrnuje adaptaci nástrojů pro hodnocení rizik a kybernetických bezpečnostních kontrol.

Global NEWS

Watch World Canada Local Politics Money Health Entertainm

TECH

Anthropic says new Claude Mythos AI is too risky for public use

By Adriana Fallico • Global News

Posted April 9, 2026 4:03 pm · Updated April 9, 2026 5:55 pm · **5 min read**

Ing. Pavel Dobeš, Ph.D.

pdobes@utb.cz

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Děkuji za pozornost.

Reference:

- Abraham, D., D'Souza, A., Kappiarukudil, K., Rai, S. "Cyber-Attacks on Energy Infrastructure—A Literature Review." *Appl. Sci.* 2025, *15*, 9233.
- Alexander, O D et al. (2020). MITRE ATT\&CK® for Industrial Control Systems: Design and Philosophy. https://www.semanticscholar.org/paper/51a2b3210d8d24944500c182c7224f8c1c21e729
- Ekisa, C et al. (2024). Leveraging the MITRE ATT\&CK Framework for Threat Identification and Evaluation in Industrial Control System Simulations. 2024 35th Irish Signals and Systems Conference (ISSC), 1-6. https://doi.org/10.1109/ISSC61953.2024.10602968
- Georgiadou, A et al. (2021). Assessing MITRE ATT\&CK Risk Using a Cyber-Security Culture Framework. Sensors (Basel, Switzerland), 21. https://doi.org/10.3390/s21093267
- Choi, W et al. (2024). Detecting Cybersecurity Threats for Industrial Control Systems Using Machine Learning. IEEE Access, 12, 153550-153563. https://doi.org/10.1109/ACCESS.2024.3478830
- Jadidi, Z, Lu, Y (2021). A Threat Hunting Framework for Industrial Control Systems. IEEE Access, 9, 164118-164130. https://doi.org/10.1109/access.2021.3133260

Reference:

- Jeffries, B., Saravia, S., Carter, C., Ankuda, Z. Cyber Risk to Mission Case Study. Mitre Corporation, 2022.
- Joy, A et al. (2024). An Investigative Evaluation of Open Source Intrusion Detection Systems for Operational Technology Networks Using MITRE ICS Attack Simulation on a Thermal Power Plant Test Bed. 2024 IEEE 21st India Council International Conference (INDICON), 1-6. https://doi.org/10.1109/INDICON63790.2024.10958514
- Kushner, D. "The real story of stuxnet." in *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53, March 2013, doi: 10.1109/MSPEC.2013.6471059.
- Progoulakis, I et al. (2021). Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering. https://doi.org/10.3390/jmse9121384
- Štefko, R., Eliáš, K., Glajc, K., Hyseni, Margita, Šimčák, J. "Cybersecurity Challenges in the Power Sector: Analysing Attacks on Electrical Grids and Substations." 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 2025.
- Toker, F., S., et al. (2021). MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System. 2021 9th International Symposium on Digital Forensics and Security (ISDFS), 1-6. https://doi.org/10.1109/ISDFS52919.2021.9486331