



# Reálný kybernetický incident aneb co se (ne)mělo stát?

Prezentuje: Marek Kocan





**Naší vizí je bezpečný  
kybernetický prostor**



# ComSource

JUNIPER  
NETWORKS

SentinelOne

Flowmon  
Networks

CITRIX

ARISTA

Infinera

Pulse Secure

radware  
Every second counts

FORCEPOINT

SANDVINE



OPSWAT

- Specializace na několik pečlivě vybraných vendorů.



# ComSource partnerství



Jsme součástí týmu CSIRT (Computer Security Incident Response Team). Ukořídíme národního týmu CSIRT.CZ je ve spolupráci s Národním bezpečnostním úřadem reagovat, koordinovat a řešit bezpečnostní incidenty v oblasti bezpečnosti IT.



ComSource je aktivním členem české pobočky AFCEA (Armed Forces Communication and Electronics Association). Členství v této mezinárodní organizaci nám umožňuje sdílet a rozvíjet naše know-how v oblasti kybernetické bezpečnosti a ICT technologií.




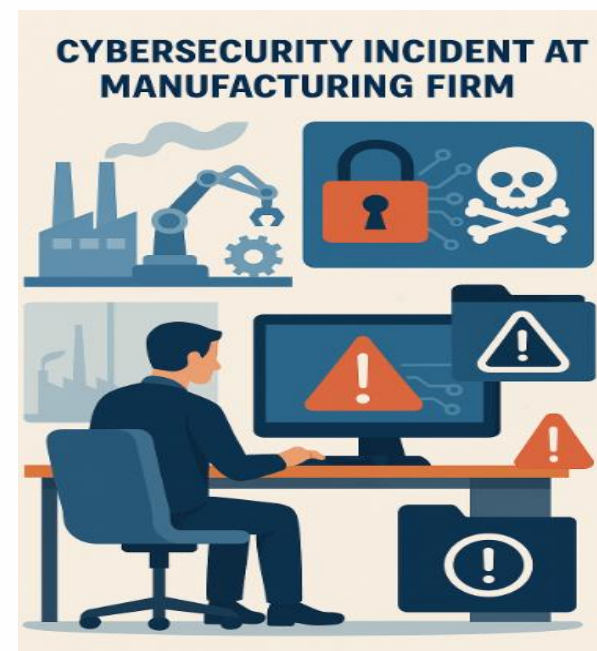
ComSource je členem projektu FENIX, který vznikl v roce 2013 na půdě českého peeringového uzlu, sdružení NIX.CZ, jako reakce na intenzivní DDoS útoky, kterým toho roku čelila významná česká média, banky nebo operátoři.





# Úvod do situace

- Středně velká výrobní, strojírenská firma
  - Vlastní výzkum, mnohaletý speciální vývoj
  - Přesah do strategických oblastí
  - Mezinárodní působení i mimo státy Evropské unie
  - Bezpečnostní incident v podobě ransomware a zcizení dat (řády TB)
  - Reálné dopady na chod firmy, omezení vybraných aktivit
  - Chaotické reakce až k volání o pomoc ve formě *tonoucí se stébla chytá*
  - Zálohy? Hm ... No ne, no ... Tedy alespoň ne v potřebné podobě ...
  - Nešlo o našeho klienta, přesto se obrátili na nás (+1T\_ODI)
  - A začala se otevírat místy až neuvěřitelná džungle ...
- 



# Naše pomoc

- Úvodní konzultace o best practice postupech
- Rychlá nabídka a postupná jednání v řádu hodin
- Nakonec si vybrali pouze část nabízených služeb, a to v rozsahu NDR včetně behaviorálních analýz nad síťovým provozem
- Plus další ad hoc konzultace
- Začátek nicméně s časovým skluzem +10D\_ODI
- Podrobné reporty, výstupy pro další šetření  
(hm, pro další šetření 😊)
- Průběžná doporučení, co dělat a jak postupovat



# Co chybělo?

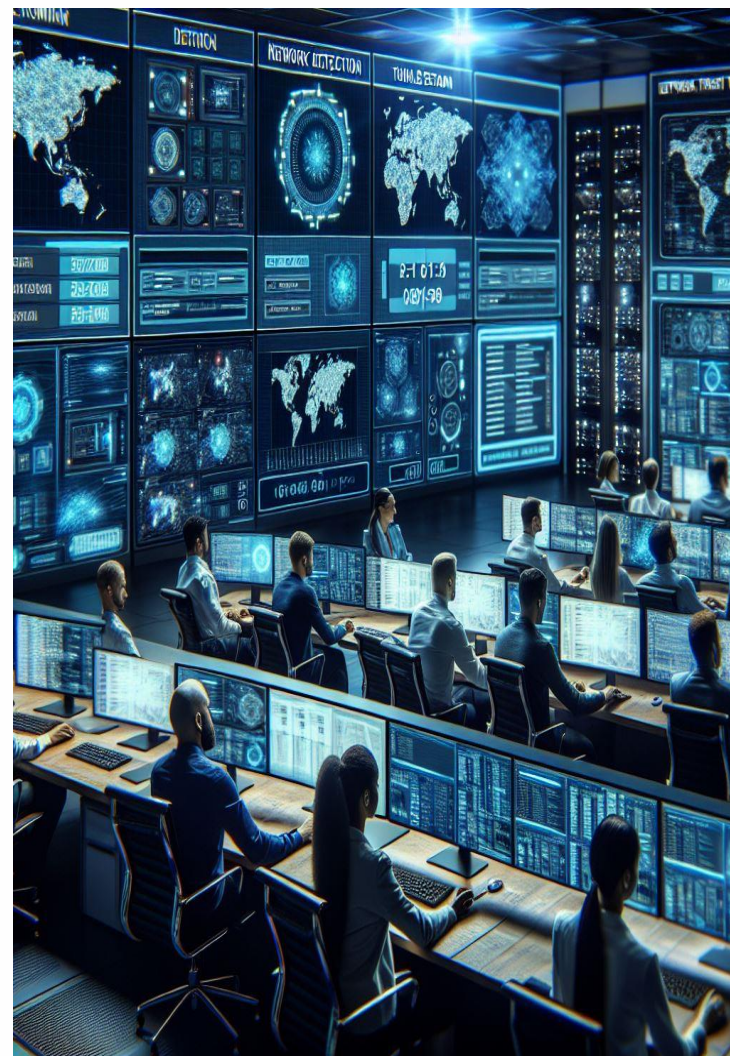
- Vlastně skoro vše ... až neuvěřitelně ...
- Podrobné informace o prostředí
- Plán reakce na incidenty (a pokud existoval, dle všeho se jím neřídili)
- Odborné znalosti (+ tradiční problém odpovědnosti a naplnění rolí)
- Jasně rozdělení působnosti
- Cokoli nad rámec základů fyzické bezpečnosti (přístupy, napojení ...)
- A hlavně ochota zjištění dál SKUTEČNĚ šetřit a jít po podstatě věci





# Jak by pomohlo řešení typu NDR

- Podrobná visibility
- Včasná detekce podezřelých aktivit
- Podezřelých na základě chování a anomálií!!!
- Možnost využití informací z dalších zdrojů (MISP)
- Dřívější ladění reálného stavu infrastruktury
- Eliminace neautorizovaných zařízení
- Snadnější a mocnější vyšetřování
- **Ale hlavně mohli zabránit úniku cenných dat**





# Pohled bezpečnostních složek

- Ozvat se co nejdříve
- Nevypínat systémy, neuklízet
- Poskytnout digitální „důkazy“, mj.:
  - obrazy jednotlivých systémů (forenzní kopie)
  - data o přístupech do systémů
  - logy
  - záznamy síťového provozu
  - data z OT prostředí
  - komunikace s útočníky
- Nevyjednávat (mj. podpora organizovaného zločinu)
- Obecně poskytnout všechny relevantní informace/dokumentace
- Rolí není soudit někoho ve firmě -> nezamlčovat
- **Obecně neřeší mitigaci/dopady, ale vyšetřuje a snaží se vypátrat zločince**



# Vybrané body ideálního postupu



- Stanovit rozsah kompromitace / odcizených dat
- Přesné záznamy o **všech** provedených krocích, nejde ale o doložení postupu dle IRP (patří sem třeba i informace restartovali jsme, zablokovali jsme port na FW, vypnuli jsme podezřelou stanici ...), dle uvážení používat UTC
- Bez domluvy **nevyjednávat, neplatit, nesdílet informace dál**
- Pokud organizace něco předává PČR, tak vytvořit hashe **k okamžiku předávání** (obrazů, logů, v podstatě jakýchkoli dat ...)
- **Nehledat** interního viníka, ničemu to v rámci vyšetřování nepomáhá, nicméně při podezření na interní článek informace poskytnout
- **Maximální** otevřenost



# Pár poznámek závěrem

- Sebelepší legislativa sama o sobě nikdy nestačí
- Důležité je vyhnout se pro forma bezduchým opatřením a postupům
- Důsledné prověřování IRP/DRP
- Pochopit, že k incidentu pravděpodobně dojde, případně že došlo, jen to zatím nevíme
- Důraz na dlouhodobé plánování a prevenci
- Opustit nárazové aktivity
- Když už se něco stane, tak se řešení opravdu věnovat
- **PLUS mít v týmech lidi, kteří tomu fakt rozumí**



# Otázky?





# Děkuji za pozornost

Email: [marek.kocan@comsource.cz](mailto:marek.kocan@comsource.cz)

Tel: 604 766 243

