ARICOMA

Aj Lesy potrebujú kybernetickú ochranu

Martin Gavurník

Obsah

- Krátko o zákazníkovi
- Priebeh kybernetického útoku
- Obnova prostredia po útoku
- Odporúčania platné pre všetkých

O Zákazníkovi

- Slovenská akciová spoločnosť
- CCA 3 300 zamestnancov
- CCA 25 regionálnych stredísk
- Odbor informatiky a komunikačných technológií
  - 10 zamestnancov IT
  - 2 dátové centrá
  - 200 fyzických a virtuálnych servrov
  - 55 TB dát
  - Významne zastúpení výrobcovia: HPE, Cisco, Sophos

Postavenie AUTOCONTu/ARICOMA u zákazníka

- AUTOCONT/ARICOMA je dlhodobý partner zákazníka
  - Technická podpora prostredia Microsoft, vrátane Sharepoint
  - Dodávka a implementácia Veeam riešenia
  - Dodávky infraštruktúry
  - Dodávky kancelárskej techniky

- V čase útoku bola platná iba Zmluva na technickú podporu Microsoft

- Autocont/Aricoma dlhodobo navrhoval projekty na zvýšenie bezpečnosti
  - Nasadenie riešenia na zabezpečenie prístupov (MFA, Conditional Access, Tiering privilegovaných účtov, …)
  - Zvýšenie ochrany koncových zariadení (LAPS, EDR, …)
  - Ochrana DNS pred phishing útokmi

Priebeh kybernetického útoku

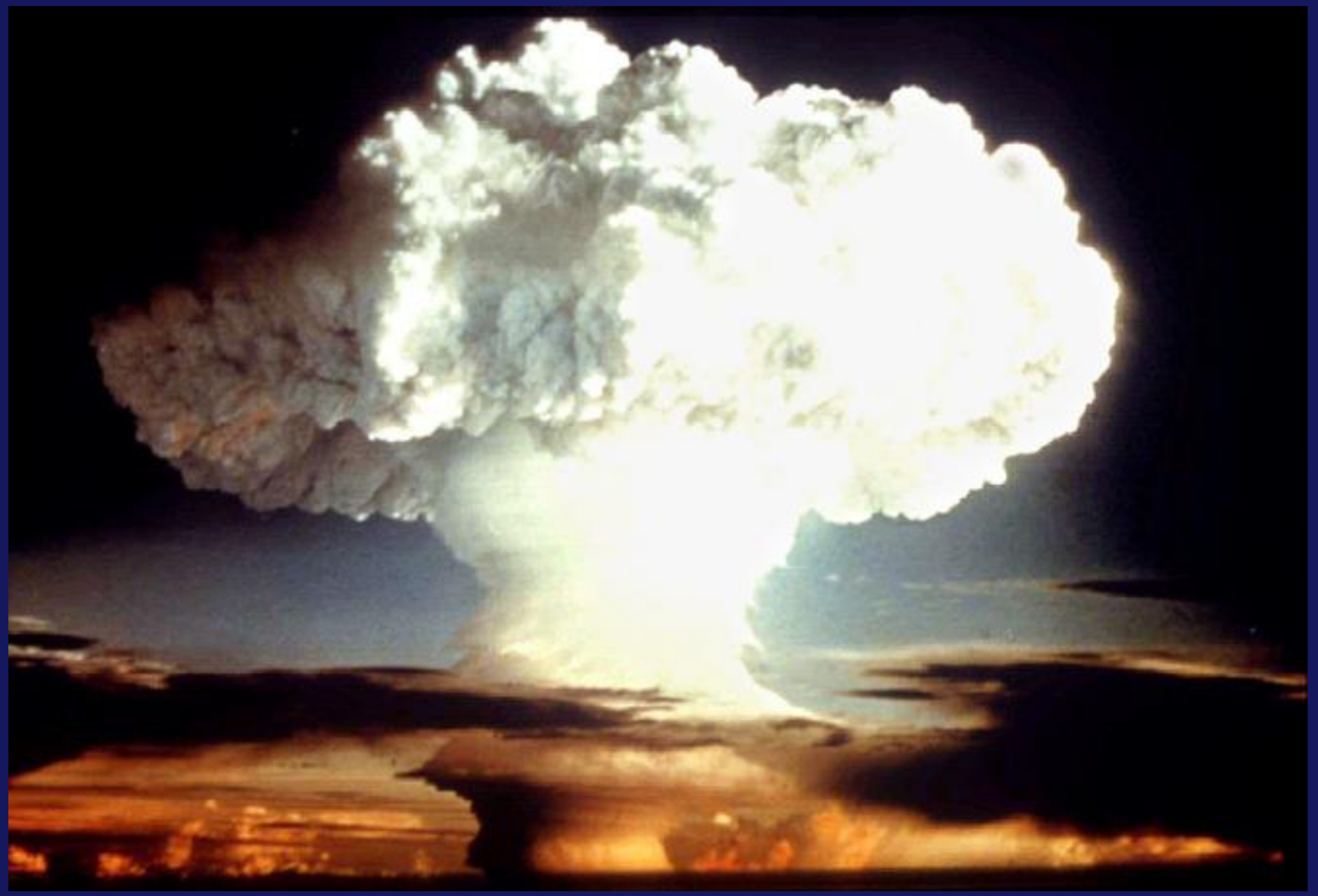
Koniec prázdnin

August / August
September / September

35. týždeň / week

SK Nikola, Nikolaj, Výročie SNP	29	Pondelok / Monday
Ružena	30	Utorok / Tuesday
Nora	31	Streda / Wednesday
SK Drahoslava, Deň Ústavy SR	1	Štvrtok / Thursday
Linda, Rebeka	2	Piatok / Friday
Belo	3	Sobota / Saturday
Rozália	4	Nedeľa / Sunday

Útok – 31.8.2022



Obnova prostredia

Deň NULA – Zákazník

- 31.8.2022 okolo 6:30 lokálny administrátor zaregistroval šifrovanie súborov a začal okamžite vypínať všetky centrálne zariadenia
- ”zburcovanie” ostatných IT administrátorov
- Následné vypnutie serverov a zariadení vo všetkých lokalitách
- Vydaný celofiremný zákaz spúšťania IT zariadení – notebook, PC, server, …
- Vznikol informačný chaos, nakoľko na takýto scenár nebola firma pripravená

Obnova prostredia

Deň NULA – AUTOCONT/ARICOMA

- 31.8.22 okolo 8:00 kontaktovaná podpora AUTOCONT
- Okamžité vytvorenie
  - Krízový tím AC: 7 systémových inžinierov + krízový manažment
  - Definovanie zdieľaných bezpečných kanálov
  - Pravidelné status meetingy 2 x denne aj počas víkendov
  - Nahlásenie incidentu na NBU a CSIRT

- Paralelne sa riešil právny rámec Autocont/Aricoma

- 1. týždeň analýzy a obnovy – 557 človeko-hodín

Obnova prostredia

Deň NULA – Prvotná analýza

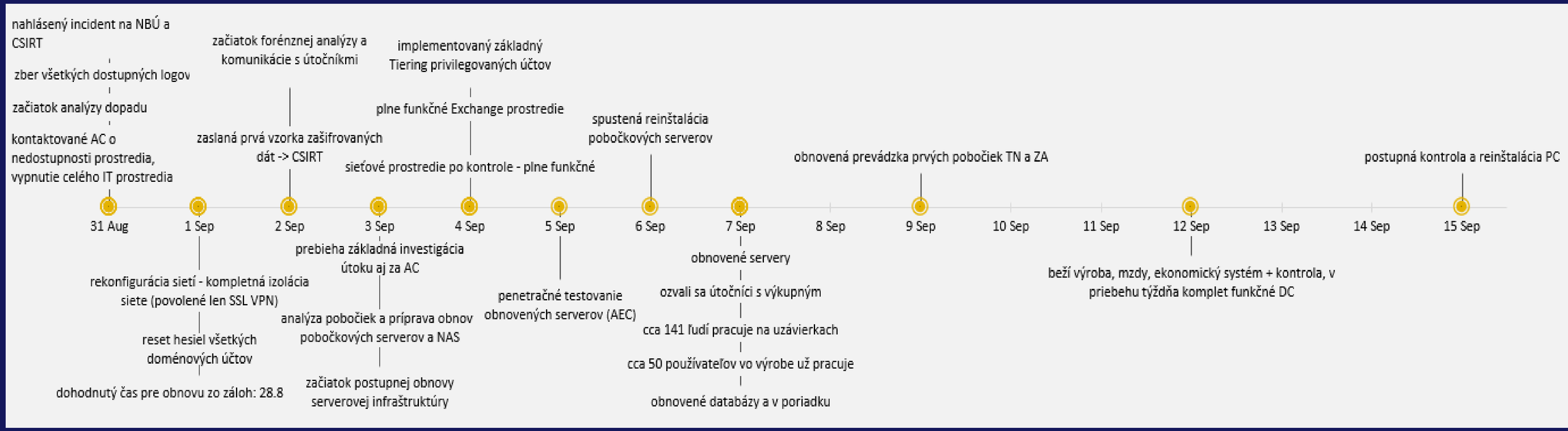
- Čo všetko bolo kompromitované? Nevedel NIKTO
  - Zber všetkých dostupných logov
  - Analýza dopadu
  - Prvé kontroly naznačovali nepoužiteľnosť záloh
  - Záchrana – offline AD kópia z inej lokality + nezašifrované zálohy produkcie

- Boli infiltrované:
  - Doménové účty a AD doména
  - Zašifrované dáta – produkčné prostredie, testovacie prostredia aj časť záloh

- Komponenty sieťovej infraštruktúry neboli infiltrované

Obnova prostredia

Časový priebeh obnovy



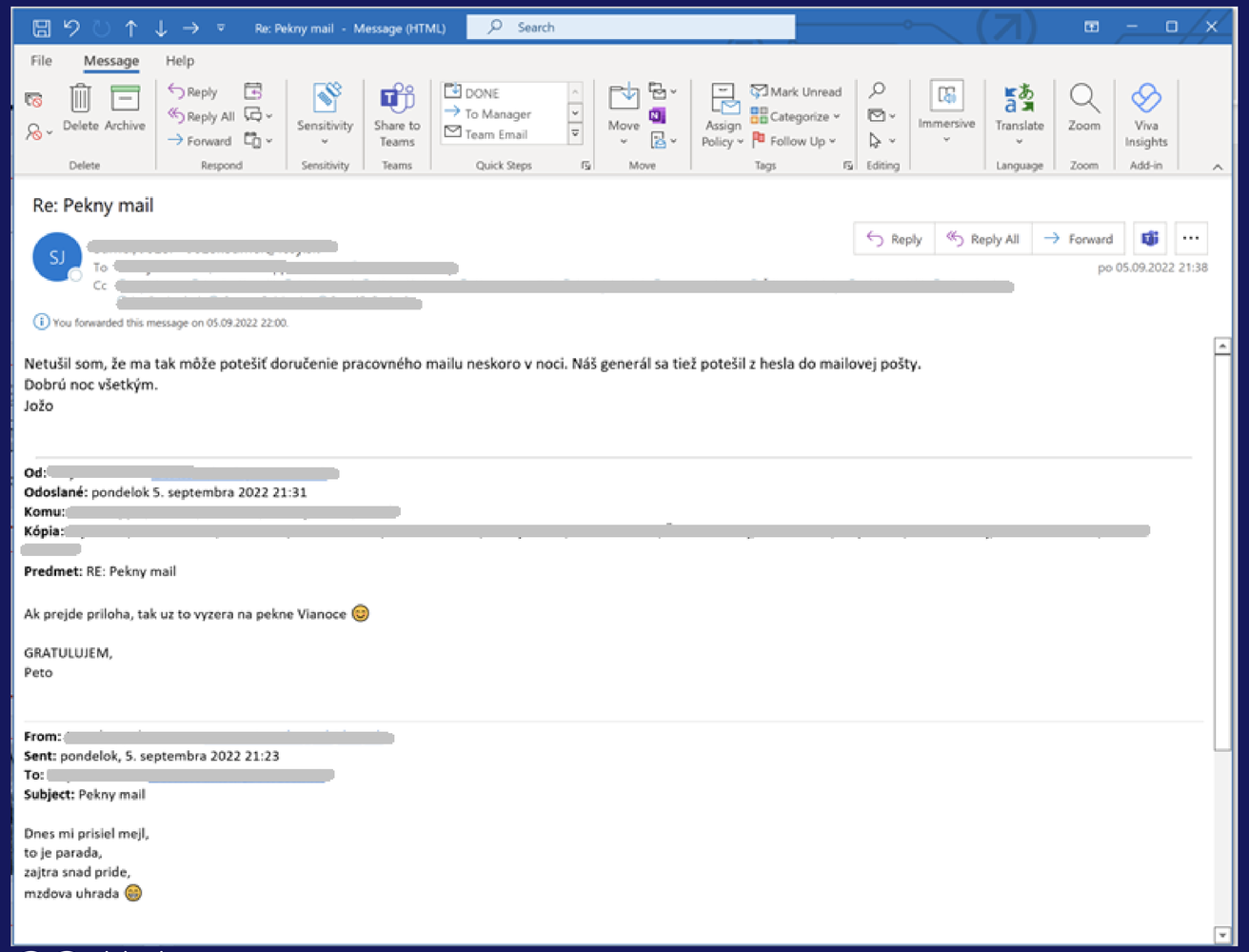
Obnova prostredia

FAKTY

- Všetky kritické produkčné systémy sa podarilo obnoviť zo záloh, niektoré systémy museli byť reinštalované
- Centrálne systémy obnovené zo zálohy z noci 27.-28.8. (celkom 38 TB, súčasne zachovaná zasiahnutá infraštruktúra pre forenznú analýzu)
- Systémy určené pre centrálne zálohovanie vybudované nanovo
- Štart obnovy serverov 2.9. o 21:09, dokončenie obnovy 4.9. o 17:37
- Vzhľadom na víkend/sviatok sa prišlo „len“ o dáta zhruba za 1 pracovný deň (backup z 28.8. (nedeľa), 29.8. sviatok, vypnuté IT 31.8. ráno)
- Prvý systém (Exchange) plne a bezpečne funkčný už 4.9.2022 (pre užívateľov od 5.9.2022)
- Po obnove servery odovzdávané priebežne na penetračné testy a následnú kontrolu a štart aplikácií, následne naspäť zaradené do zálohovania

Obnova prostredia

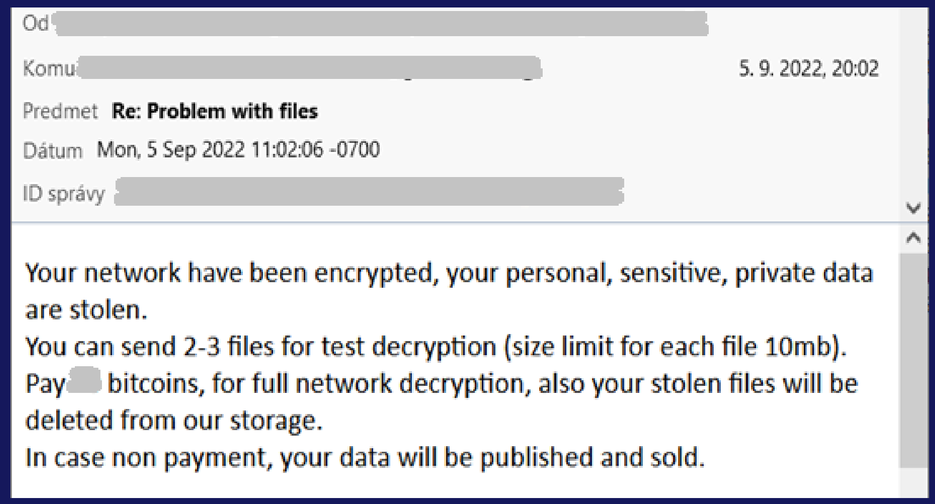
K tomuto nie je čo dodať



Obnova prostredia

Komunikácia s útočníkom

- Komunikácia prebehla medzi 5.9.2022 až 12.9.2022 (6 správ)
- Zistenia z komunikácie:
  - výkupné v hodnote ## Bitcoin
  - útočník:
    - mal vedomosť o tom, aká organizácia bola kompromitovaná
    - preukázal schopnosť dešifrovať súbory
    - preukázal exfiltráciu časti súborov
- Vzorka exfiltrovaných údajov:
  - 26 súborov
  - faktúry, zmluvy



Odporúčania

Oblasti zlepšenia 1/3

- **Akceptovať pravdepodobnosť úspešného útoku a pripraviť**
  - komunikačné scenáre
  - formalizovať podporné tímy / spoločnosti (napr. pre forenznú analýzu)
  - vzdelaných zamestnancov

- **Endpoint protection** – minimalizovať možnosť infiltrácie
  - Local Administrator Password Solution (LAPS) a Privileged Access Workstation (PAW)
  - zlepšenie centrálne riadenej antimalvérovej ochrany vrátane EDR
  - zavedenie phishingovej ochrany
  - zamedzenie / obmedzenie využívania súkromných zariadení na pracovné účely a naopak

Odporúčania

Oblasti zlepšenia 2/3

- **Identity manažment**
  - tiering privilegovaných účtov
  - hĺbková analýza účtov, skupín Active Directory a ich používania
  - hardening AD

- **Access manažment**
  - minimalizovať a prehodnotiť používanie terminálových služieb
  - zavedenie MFA / Conditional Access, aj pre lokálne prístupy
  - všetky vzdialené prístupy musia ísť cez VPN
  - implementácia 802.1x
  - mikrosegmentácia siete

Odporúčania

Oblasti zlepšenia 3/3

- **Ochrana dát**
  - redizajn zálohovania tak, aby nikto (ani správca zálohovania) nevedel prepísať kópie záloh
- **Manažment zraniteľností**
  - patchovať a nepoužívať staré verzie OS a SW
- **SIEM**
  - minimálne implementovať centrálne neprepisovateľné logovanie s dostatočnou kapacitou pre dlhú históriu
  - optimálne SIEM s čo najširšou sadou korelácií
  - ideálne aktívny SOC (Security Defense Center)

Nasadené

ESET EDR

- **Licencie**
  - ESET Endpoint Security + ESET Server Security
  - ESET Full Disk Encryption
  - ESET LiveGuard Advanced for Endpoint Security + Server Security
  - ESET Inspect

Ďakujem za pozornosť

Martin Gavurník

+421 903 262 403
martin.gavurník@aricoma.com