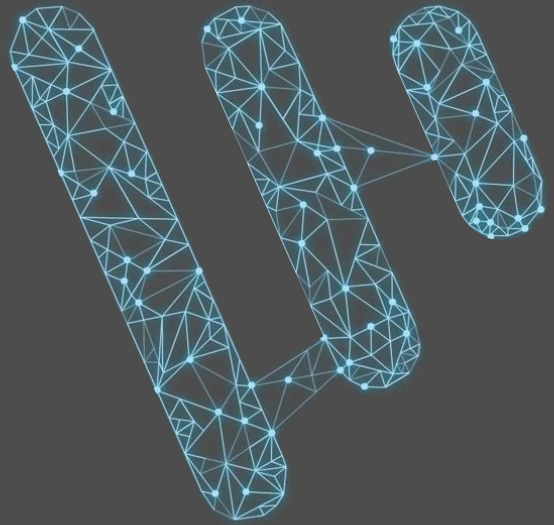



CRA
ČESKÉ RADIOKOMUNIKACE

RANSOMWARE ÚTOKY

CO JSOU TO RANSOMWARE ÚTOKY A JAK SE JIM BRÁNIT

LUKÁŠ BARTAKOVIČ

12. LEDNA 2021

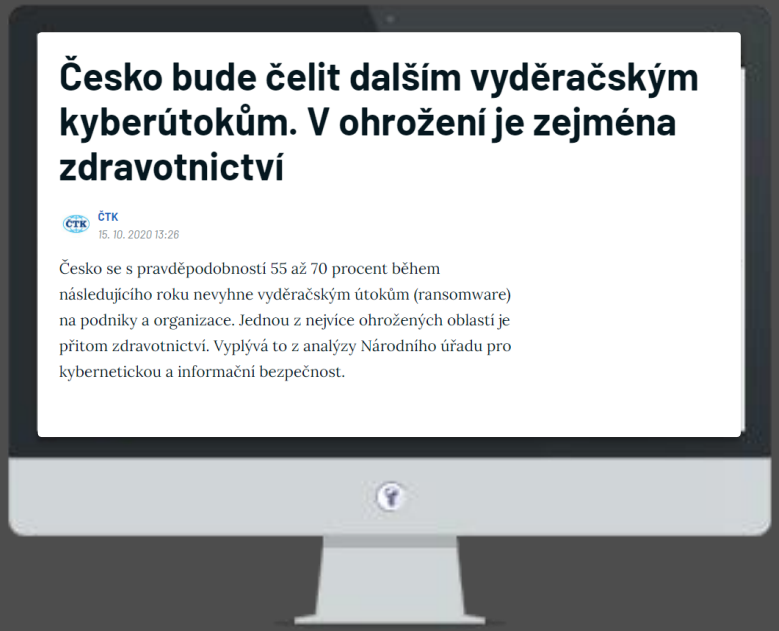
AGENDA:

- O čem bude dnešní webinář?
  - Co je to Ransomware
  - Známé případy v roce 2020
  - Metody obrany
  - Doporučení

RANSOMWARE ÚTOKY

RANSOMWARE ÚTOKY

Aktuální situace



Analýza NÚKIB 14.10.2020

- Změna cílení
  - Dříve: náhodné instituce a uživatelé
  - Nyní: Větší firmy instituce
    - Zdravotnictví, obchod, technologické firmy, poskytovatelé služeb a obsahu
- Důvody:
  - Tlak na rychlé obnovení
    - Vyhnutí se paralýze společnosti
    - Ztráta tržeb, zákazníků, renomé
    - Prostředky na zaplacení

RANSOMWARE ÚTOKY

Známé případy roku 2020

Červenec 2020 – nefungují:

- webové stránky
- technická podpora
- ukládání aktivit
- Garmin Connect

Ransomware: WastedLocker
EvilCorp - Rusko

Výkupné $10 000 000

- Z českého rybníčku....
- Březen 2020
  - První případy Covid v ČR
  - Útok na Fakultní nemocnici Brno
    - Vyřazování IT systémů z provozu
    - Odložení operací
  - Návrat do provozu:
    - NUKIB, NCOZ, tým z VFN a komerční subjekty

Ransomware: Defray

RANSOMWARE ÚTOKY

Analýza Ransomware

- Co je Ransomware
  - *Ransom = výkupné*
  - Zašifrování dat a požadavek na výkupné
  - Kdo?
    - Nestátní skupiny
    - Vládní agentury (Rusko, KLDR, Čína)
  - Jak?
    - Využití zranitelností
    - Phishing
    - Sociální inženýrství

Jak se Ransomware dostal do sítě	Procent
Kliknutí na odkaz/stažení souboru	29%
Vzdálený útok na server	21%
Nakažená příloha emailu	16%
Misconfigurace	9%
Přes Remote Desktop	9%
Přes dodavatele	9%
USB disk	7%
Total	

Zdroj: Průzkum Sophos (2019)

RANSOMWARE ÚTOKY

Analýza Ransomware

- Co je Ransomware
  - *Ransom = výkupné*
  - Zašifrování dat a požadavek na výkupné

  - Kdo?
    - Nestátní skupiny
    - Vládní agentury (Rusko, KLDR, Čína)

  - Jak?
    - Využití zranitelností
    - Phishing
    - Sociální inženýrství

Jak se Ransomware dostal do sítě	Procent
Kliknutí na odkaz/stažení souboru	29%
Vzdálený útok na server	21%
Nakažená příloha emailu	16%
Misconfigurace	9%
Přes Remote Desktop	9%
Přes dodavatele	9%
USB disk	7%
Total	

>80% síťové útoky

RANSOMWARE ÚTOKY

Příklady Ransomware programů

- Cílení na nejslabší článek
  - Uživatel
- Nejvíce Ransomware pro OS Windows

- Ransomware WannaCry
  - DataLocker

Sextortion mail

po 05.10.2020 0:18
miroslav.pestax@agropol.cz
Obchodní nabídka.
Komu ⊞ Region STR

Ahoj!

Bohužel mám pro tebe špatné zprávy.
Před několika měsíci jsem totiž získal přístup k zařízení, které používáš k procházení internetu.
Od té doby pravidelně sleduji tvoji aktivitu na webu.

Jako pravidelný návštěvník erotických stránek mohu potvrdit, že jsi to ty, kdo je za tuhle situaci plně zodpovědný.
Zjednodušeně řečeno, přístup k tvým datům mi poskytly právě webové stránky, které jsi navštívil.

Do tvého systému jsem nahrál ve formě ovladače virus Trojského koně, který aktualizuje několikrát denně svůj podpis, takže je nemožné, aby ho tvůj antivir detekoval.
Virus mi navíc poskytuje přístup k tvé kameře i mikrofonu.
Kromě toho jsem veškerá data, včetně fotek, souborů sociálních sítí, chatů a kontaktů, zálohoval.

Zrovna nedávno jsem dostal úžasný nápad vytvořit video, ve kterém v jedné části obrazovky masturbuješ, zatímco v té druhé se přehrává klip, u kterého si děláš dobře. Panečku, to byla zábava!

MECHANIKA MALWARE

Killchain

Email

Kliknutí na odkaz

Škodlivý kód hledá zajímavá data, vypíná antivirus, zálohování

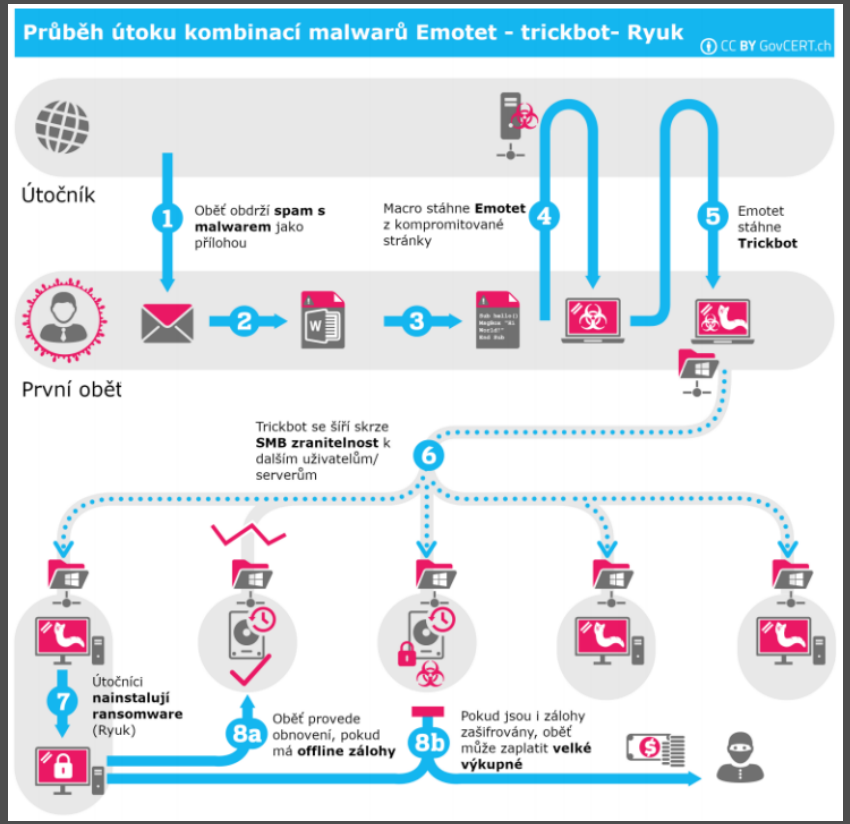
Comannd & Control komunikace

Pohyb v síti

REÁLNÝ PŘÍPAD ÚSPĚŠNÉHO RANSOMWARE ÚTOKU

Z čeho se skládal?

- Součásti útoku:
  - Emotet
    - Malware
    - Makro-virus
    - Získání přístupu do systému
    - Instalace dalšího škodlivého SW
  - Trickbot
    - Bankovní trojan
    - Sběr citlivých dat
    - Vypnutí Windows Defender
    - Rozšiřování v síti (EthernalBlue)
  - Ryuk
    - Ransomware
    - Šifrování dat
    - Offline zálohy



Zdroj: govcert.ch

NEJČASTĚJŠÍ CÍL ÚTOKU

Na koho útočníci nejčastěji cílí

RANSOMWARE ÚTOKY

Cíle útoku

Nejslabší článek = cíl útok

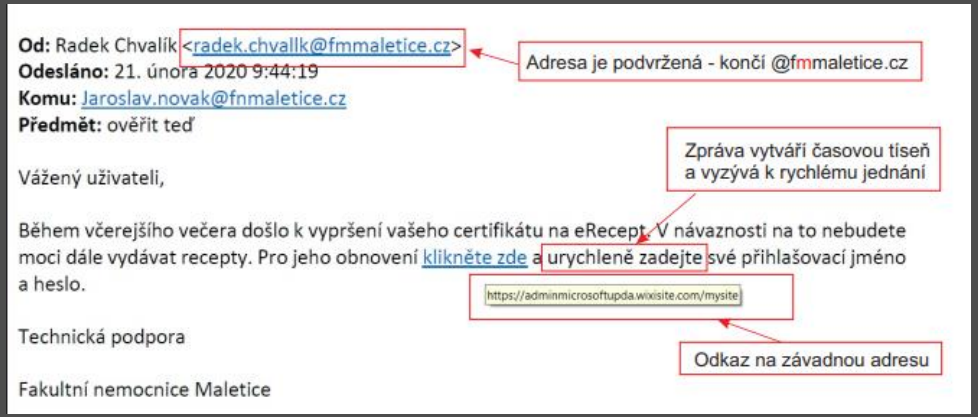
Uživatel

Zdroj: knowyourmeme.com

SOCIÁLNÍ INŽENÝRSTVÍ

Infikované emaily

- Dnešní podvodné emaily jsou rafinovanější
  - Imitují věrohodné uživatele
  - Imitují příslušnost ke známé značce
  - Imitace přihlašovacího prostředí
  - Cílem je získání přístupu



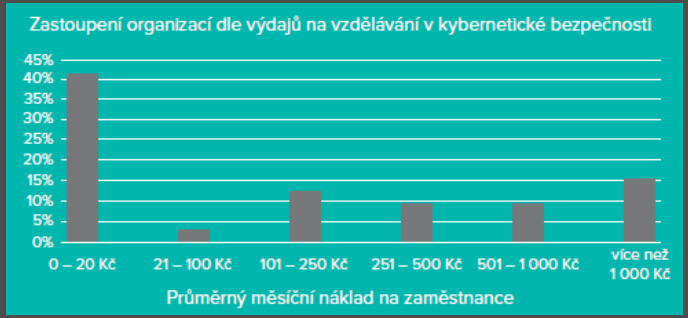
Zdroj: NÚKIB

Edukace uživatelů – jak poznat škodlivý mail

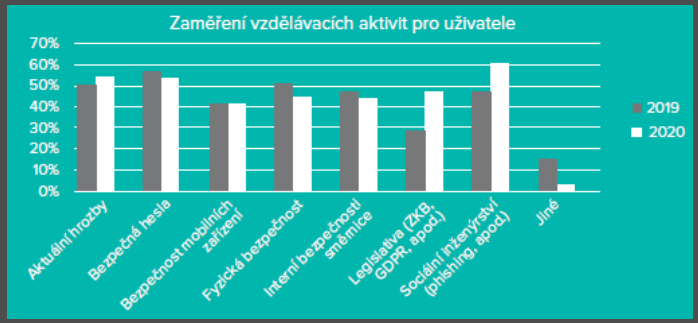
EDUKACE UŽIVATELŮ

Situace ve firmách

- Vzdělávání uživatelů
  - Zvyšování povědomí o KB
    - Jak poznat, že se jedná o podvod
    - Bezpečný pohyb v „kyberprostoru“
    - Jak reagovat, když mám podezření
      - Na koho se obrátit, kam hlásit
    - Jak reagovat, když „omylem“ kliknu
  - Formy, ověřování
    - E-learning
    - Prezentace
    - Testy
    - Simulovaný phishingový útok



Zdroj: Alef.0 – Security Report 2019



Zdroj: Alef.0 – Security Report 2019

Doporučení – školení alespoň 1x ročně

OBRANA PROTI RANSOMWARE

Možnosti ochrany před úspěšným kybernetickým útokem

ZÁKLADNÍ MOŽNOSTI OCHRANY

Doporučení

- Jak se bránit?
- Základní doporučení NÚKIB:
  - Pro IT administrátory:
  - https://www.govcert.cz/cs/informacni-servis/doporuceni/2736-doporuceni-nukib-pro-administratory-verze-4-0/

KONTROLUJTE PŘENOSNÁ MÉDIA
jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU
na pracovních stanicích a serverech, kdekoliv je to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC
může se např. jednat o Protected View nebo Protected mode.

VYNUŤTE VYTÁČENÍ VPN,
pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

SPRÁVA ÚČTŮ

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ

STAVÍME OCHRANU PŘED RANSOMWARE ÚTOKY

5 základních elementů

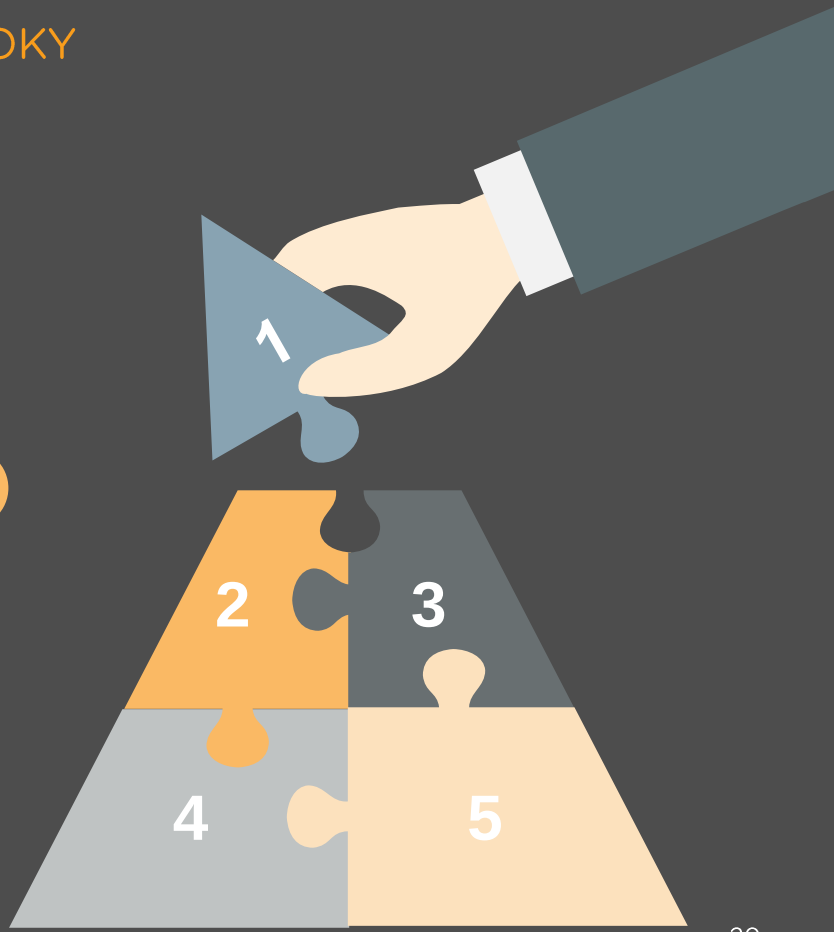
Kvalitní obrana 1
Firewall s UTM funkcemi
Ochranu emailu (proti phishingu)
Ochranu koncových zařízení
Sandbox
Ochranu serverové infrastruktury

Zmenšení útočné plochy infrastruktury 2
„Co nejméně věcí přístupných z venku/internetu“
Zablokovat nepotřebné porty na FW
Zabezpečení používané komunikace Firewallem

Zabezpečený vzdálený přístup 3
Použití šifrovaného VPN tunelu
Least Privilege princip – jen potřebná práva
Logování přístupů a činností

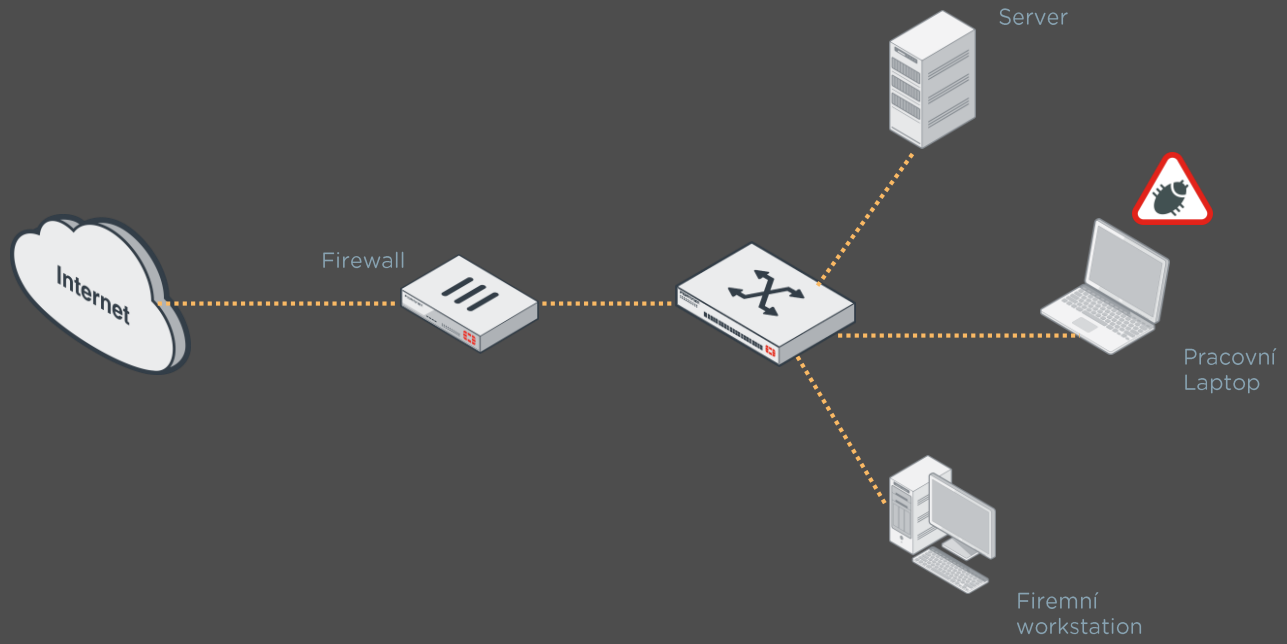
Ověřování uživatelů 4
Použití šifrovaného VPN tunelu
Least Privilege princip – jen potřebná práva
Logování přístupů a činností

Zamezení nekontrolovaného šíření 5
Segmentace sítě
Logování provozu



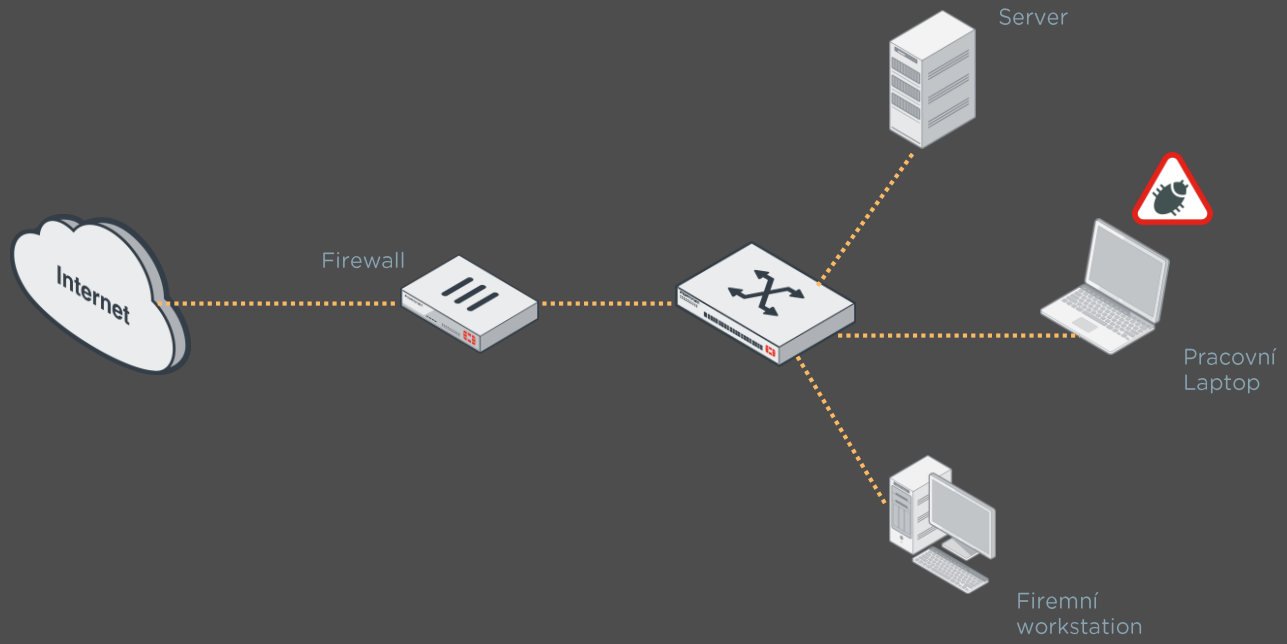
SEGMENTACE SÍTĚ

Šíření útoku v nesegmentované (ploché) síti



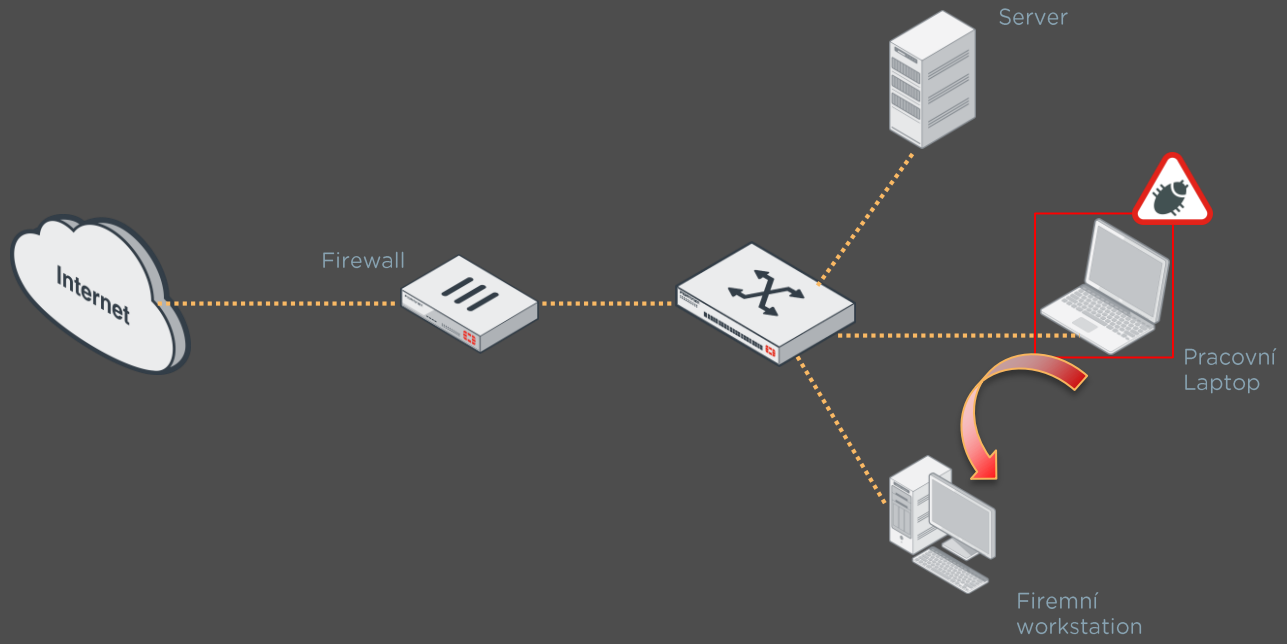
SEGMENTACE SÍTĚ

Šíření útoku v nesegmentované (ploché) síti



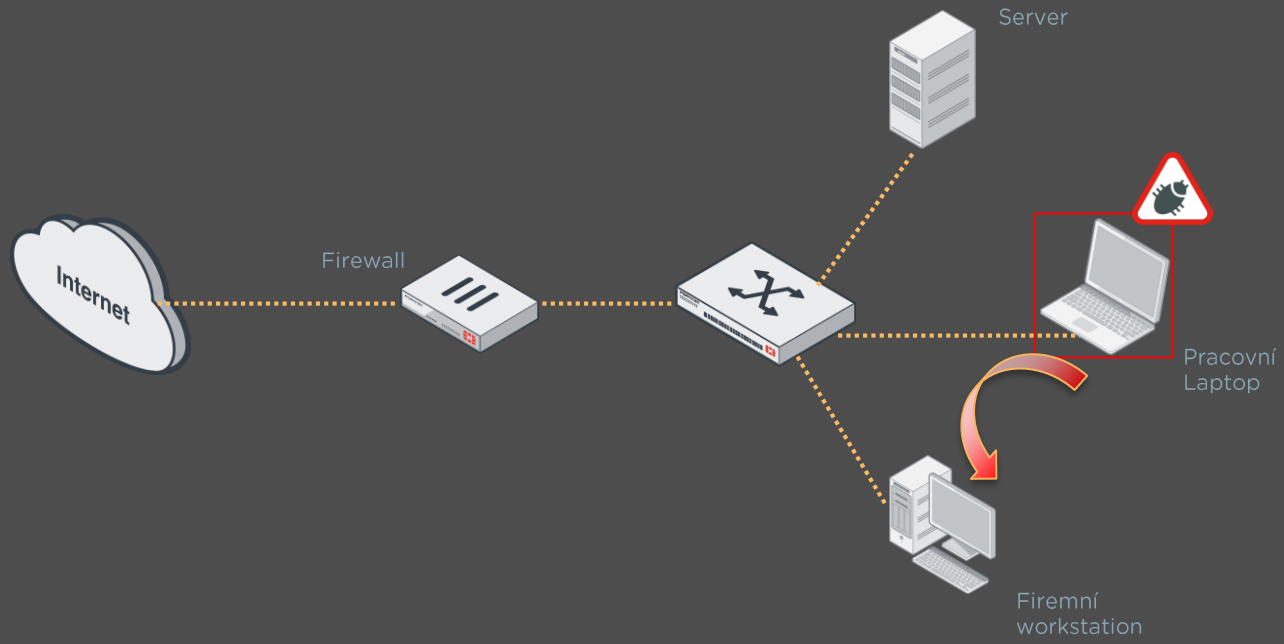
SEGMENTACE SÍTĚ

Šíření útoku v nesegmentované (ploché) síti



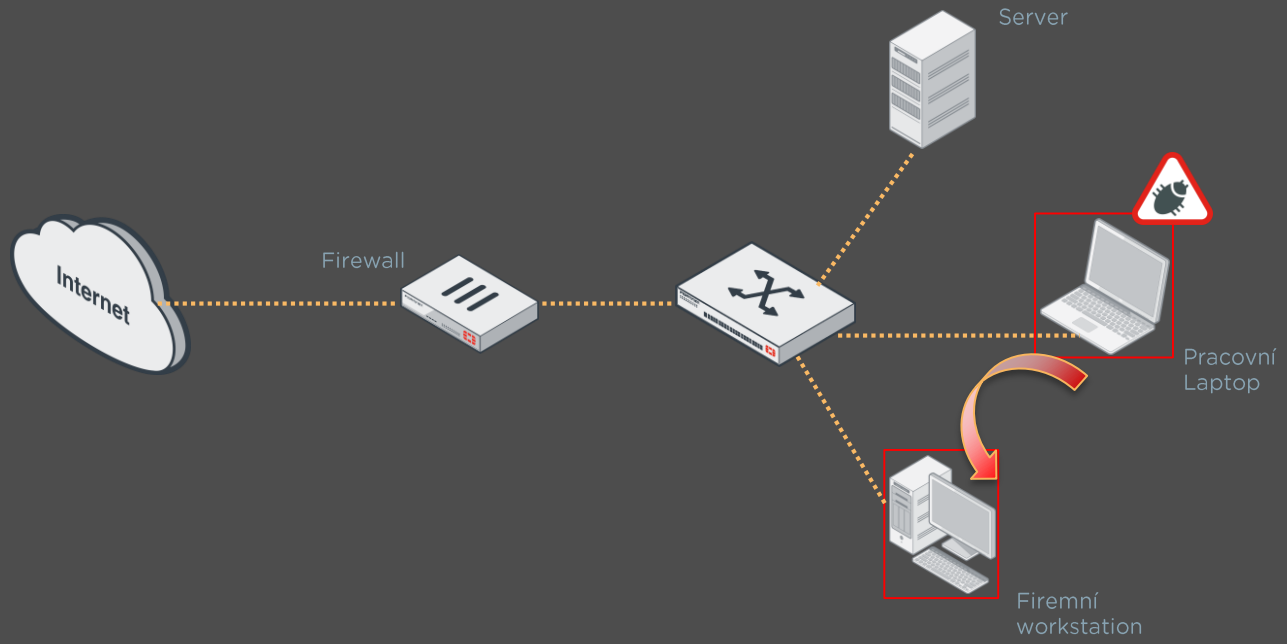
SEGMENTACE SÍTĚ

Šíření útoku v nesegmentované (ploché) síti



SEGMENTACE SÍTĚ

Šíření útoku v nesegmentované (ploché) síti

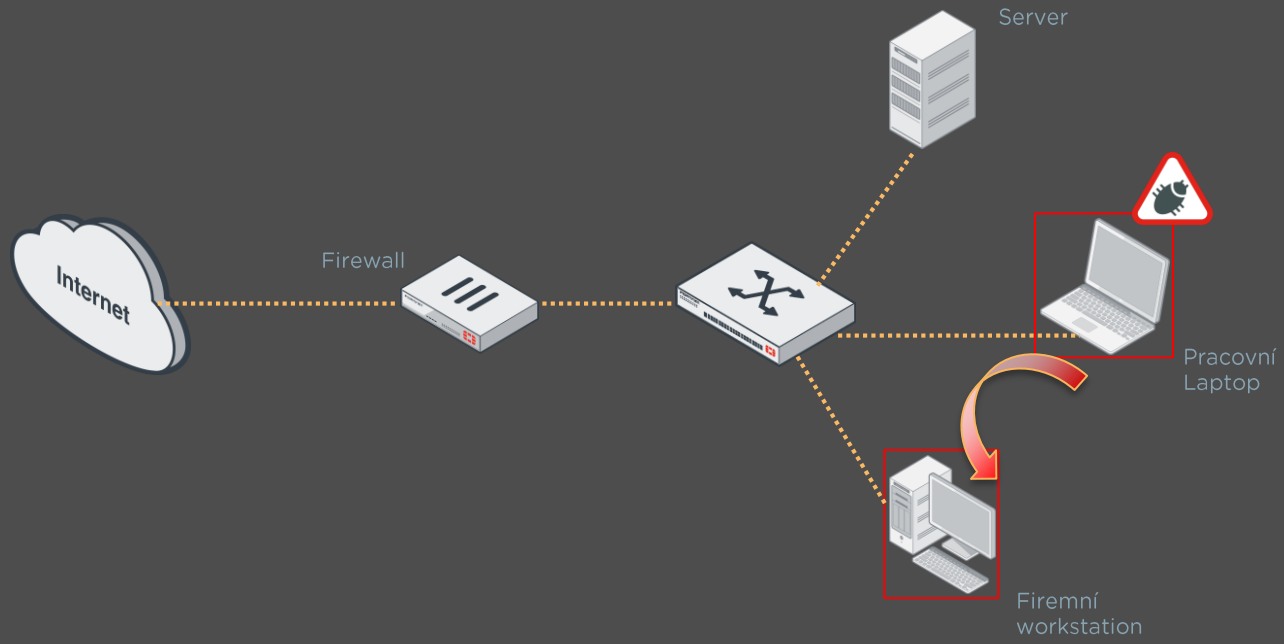


SEGMENTACE SÍTĚ

Základní koncepce

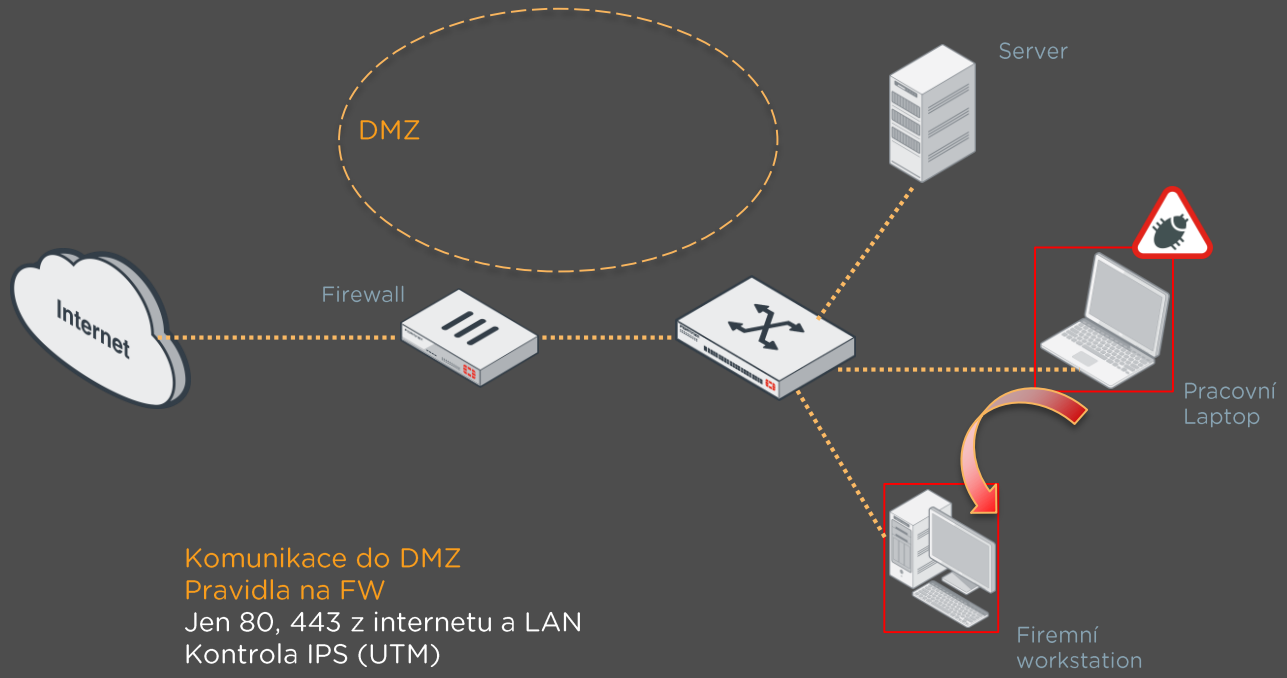
SEGMENTACE SÍTĚ

Rozdělení na menší podsítě



SEGMENTACE SÍTĚ

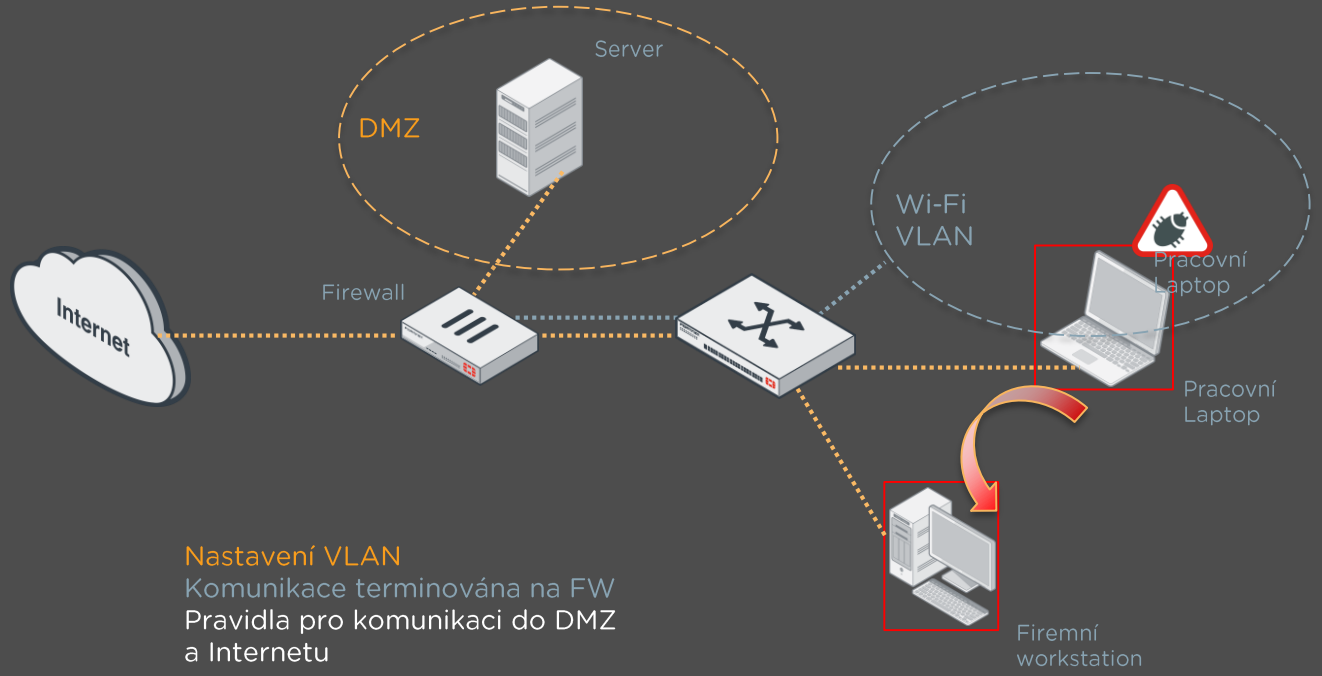
Rozdělení na menší podsítě



Komunikace do DMZ
Pravidla na FW
Jen 80, 443 z internetu a LAN
Kontrola IPS (UTM)

SEGMENTACE SÍTĚ

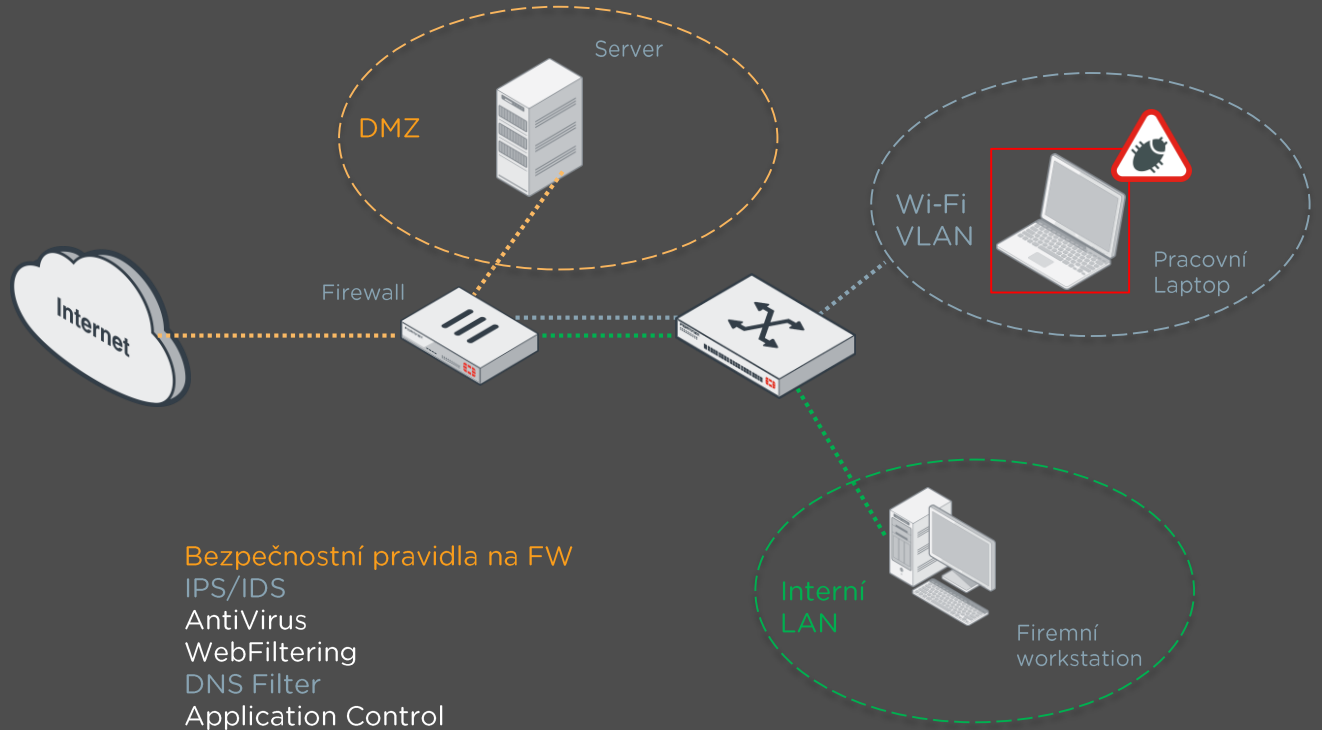
Rozdělení na menší podsítě



Nastavení VLAN
Komunikace terminována na FW
Pravidla pro komunikaci do DMZ
a Internetu

SEGMENTACE SÍTĚ

Rozdělení na menší podsítě



Bezpečnostní pravidla na FW
IPS/IDS
AntiVirus
WebFiltering
DNS Filter
Application Control

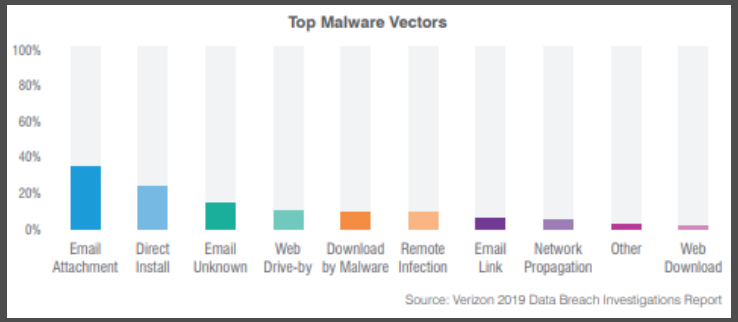
DALŠÍ BEZPEČNOSTNÍ NÁSTROJE

Ochrany před Ransomware

DALŠÍ ELEMENTY OCHRANY PŘED RANSOMWARE

Ochrana mailové komunikace

- E-mail
  - Nejčastější vektor



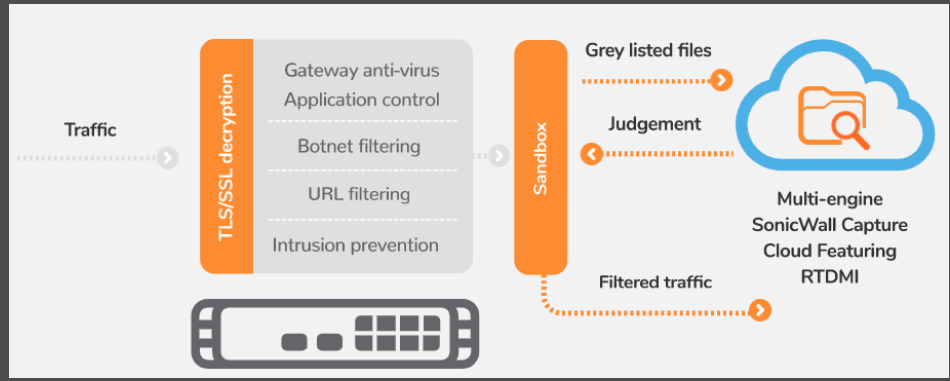
  - Malware (škodlivý kód)
  - Phishing (podvodné e-maily)
  - Emailové podvody (vylákání peněz)

- Zajištění bezpečnosti:
  - Před doručením:
    - Kontrola na výskyt škodlivého kódu
    - Reputace odesílatelů a IP
    - Kontrola obsahu
    - Validace odesílatele (DMARC)
  - Po doručení:
    - Click protection
    - DLP
- Vhodné kombinovat se SandBoxem

DALŠÍ ELEMENTY OCHRANY PŘED RANSOMWARE

Sandboxing

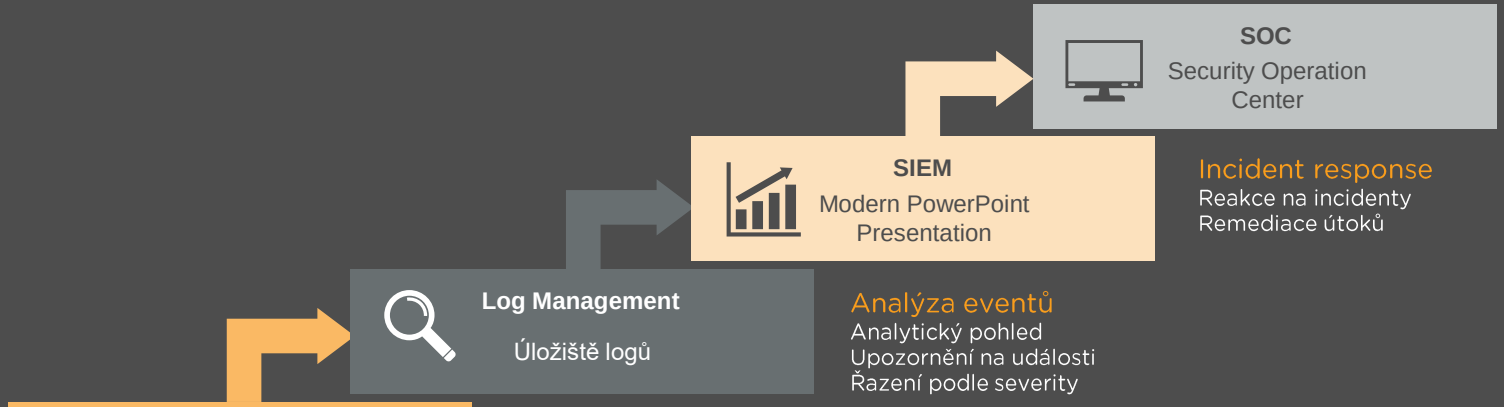
- Sandbox
  - Co přináší?
    - Detekce a ochrana před „Zero-day“ útoky
      - Nejsou signatury
    - Detekce neznámých hrozeb
  - Test podezřelého souboru
    - Ve virtuálním prostředí
    - Čeká se, jak se projeví
    - Doručit/Nedoručit



Zdroj: Sonicwall.com

DALŠÍ ELEMENTY OCHRANY PŘED RANSOMWARE

Logování (událostí, provozu)



Incident response
Reakce na incidenty
Remediace útoků

Analýza eventů
Analytický pohled
Upozornění na události
Řazení podle severity

Ukládání logů
Forenzní analýza
Reporty
Audit
Logování přístupů

Logování
SEC – bezpečnostní zařízení
OS - Operační systémy
APP - Aplikace
(Flow)

Ukládání, analýza logů a událostí výrazní usnadní odhalení případného kybernetického útoku ale může, díky moderním nástrojům, případným útokům předejít.

DALŠÍ BEZPEČNOSTNÍ NÁSTROJE

Ochrana uživatelských zařízení

DOBA HOME-OFICCEOVÁ A POST-HOME-OFICCEOVÁ

Jak to bude dál?

Home office napořád. Avast chce lidem nabídnout trvalou práci z domova

Zdroj: seznamzpravy.cz

Navždy home office. Někteří zaměstnanci Twitteru se už do kanceláře nevrátí, firma je nechá pracovat na dálku

Zdroj: czechcrunch.cz

Home office nemá žádná pozitiva, tvrdí šéf Netflixu. Obdivuje, jak se lidé pro práci obětovali

Zdroj: irozhlas.cz

Pandemie Covid-19 zvýšila poptávku po flexibilních kancelářích

Zdroj: e15.cz

DOBA HOME-OFICCEOVÁ A POST-HOME-OFICEOVÁ

Hlavní scénáře

- Zajištění provozu během nečekaných událostí

- Flexibilita a efektivita zaměstnanců (+bezpečnost)

- Benefit pro zaměstnance

OCHRANA UŽIVATELSKÝCH ZAŘÍZENÍ

Co se řeší

- Nové výzvy/překážky
  - Zařízení na Home-office:
    - Nejsou chráněny firemním perimetrovým FW
    - Uživatelé mohou častěji přistupovat z veřejných sítí (Wi-Fi)
    - Složitější instalace a správa firemních zařízení na dálku
    - Problematické aktualizace systémů a správa povolených aplikací u BYOD

  - Správce IT by měl zajistit:
    - Bezpečné/šifrované VPN připojení ke zdrojům firmy
    - Ochranu koncových zařízení (Laptopy, PC, Mobily)
      - Ochranu proti Malware
      - Ochrana proti ATP (Advance Persistent Threat)
      - Vulnerability a patch management
    - Vzdálenou správu a monitoring

OCHRANA UŽIVATELSKÝCH ZAŘÍZENÍ

Základní dělení

Ochrana koncového zařízení (EPP)

App FW, Anti-malware, Anti-exploit, Web Filtering

- Chrání koncové zařízení před škodlivým kódem, viry

FABRIC AGENT

Telemetry, Quarantine, Vulnerability, App Inventory

- Analýza a správa koncových zařízení

SECURE REMOTE ACCESS

SSL & IPSec VPN, SSO

- Zajišťuje šifrovanou komunikaci a ověřování uživatelů

ADVANCED THREAT PROTECTION

Sandbox Integration

- Ochrana proti pokročilým hrozbám

Systémy Endpoint Protections Platfrom (EPP)

OCHRANA UŽIVATELSKÝCH ZAŘÍZENÍ

Trendy

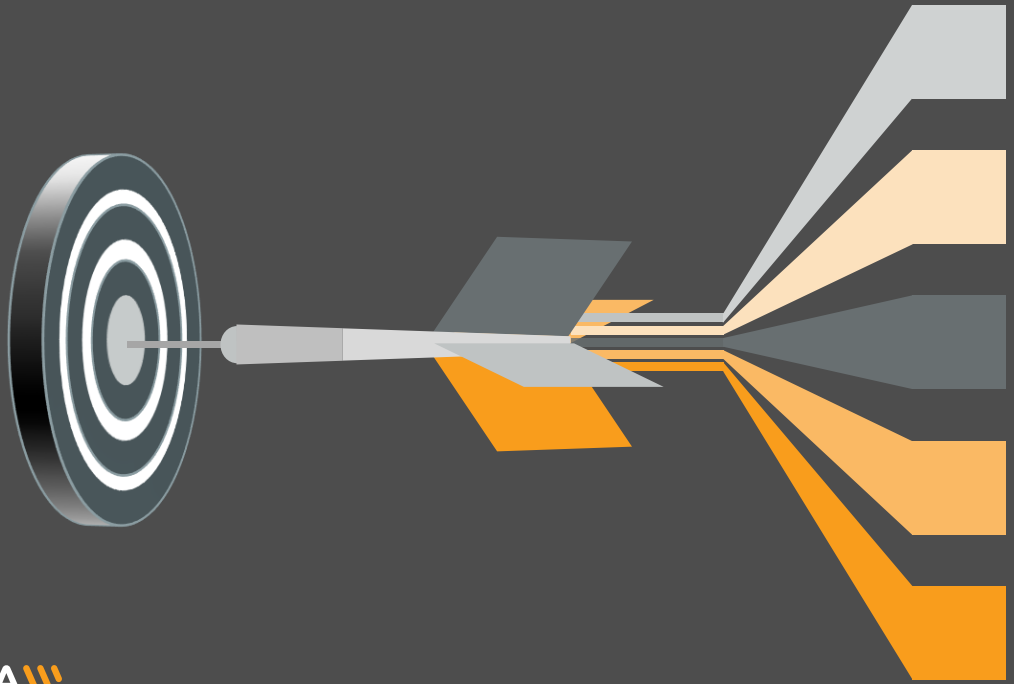
- Nový přístup
  - EDR (Endpoint Detecion & Response)
    - Doplněk k EPP
    - Sběr dat z EP, analýza, AI, ML

    - Snaží se předvídat a zamezit útoku
    - Pomáhá při úspěšném průniku
      - Automatizace
      - Incident Response
      - Remediace útoku
      - Forenzní analýza

Zdroj: Fortinet.com

DOPORUČENÉ NA ZÁVĚR

Best-practice pro ochranu před Ransomware



Školení a edukace zaměstnanců/uživatelů
(jak poznat podezřelý email a kam to nahlásit)

Zálohování (ideálně kopie off-line)

Instalace nejnovějších aktualizací a patchů

Připravený plán v případě útoku a obnovy

Kvalitní nástroje ochrany pře kyber-útoky

DĚKUJEME ZA POZORNOST