cesnet

IT bezpečnost s virem za zády

Aleš Padrta

Virus přichází

- Problémy s viry (malwarem)
  - Cíl: koncová zařízení, infrastruktura
  - Běžná rutina, standardní postupy
- 2020 $\Rightarrow$ Nové problémy s virem
  - Cíl: člověk (zaměstnanec, uživatel)
  - Pohled bezpečnostního analytika

Signatura	GAC CCC AAA ATC AGC GAA AT
IoC	horečky, ztráta čichu, ..., bez IoC (!)
Vektor útoku	kapénky + sliznice
Patch	modul imunita (živelně, systematicky)
Hotfix	omezení sociálního kontaktu

Co se změnilo

- Hotfixová opatření

  $\Rightarrow$ neshlukovat se $\Rightarrow$ práce z domova
- Uživatel (zaměstnanec organizace)
  - Kancelář $\rightarrow$ Internet
- Potřeba nadále pracovat
  - Stejně jako vždy (práce s e-maily)
  - Nyní nelze (služební kávovar)
  - Jiný postup

    $\Rightarrow$ využití (dosud) nepoužívaných služeb

    $\Rightarrow$ nové služby
- Klíčové slovo *Internet* $\Rightarrow$ IT oddělení

Forenzní laboratoř

Činnosti IT oddělení

Činnost IT oddělení

- Předpoklad
  - Revír IT oddělení = Internet
  - Home office = žádný problém
- Potřeba (fyzické) interakce
  - Uživatel
  - Zařízení uživatele
- Realita
  - Interní postupy $\rightarrow$ potřeba změnit
  - Změna

    $\Rightarrow$ chaos

    $\Rightarrow$ problémy + příležitosti

Uživatelská podpora

- Rady a pomoc uživatelům
  - Příchod na HelpDesk / ServiceDesk
  - On-site
- Péče o zařízení
  - Aktualizace
  - Programové vybavení (i obslužné)
  - SW a HW problémy
- Kvalitní podpora = nezbytná pro bezpečnost
  - Home office $\Rightarrow$ nové nástroje
  - Nové nástroje $\Rightarrow$ nové postupy
  - Bezradný uživatel $\Rightarrow$ kreativní (!) uživatel

Uživatelská podpora

- Standardní situace (stanice v kanceláři)
  - Fyzicky na dosah / vzdálená správa
  - Standardizované vybavení
- Přesun vybavení (stanice u uživatele doma)
  - Mimo fyzický dosah
  - Prověřit vzdálenou správu

    (NAT, IP adresa, bezpečné pro Internet?)
- Vlastní vybavení uživatele
  - Různý HW, různý OS
  - Co vše smí podpora?
  - Definice HW, OS?
  - Druhy problémů k řešení?

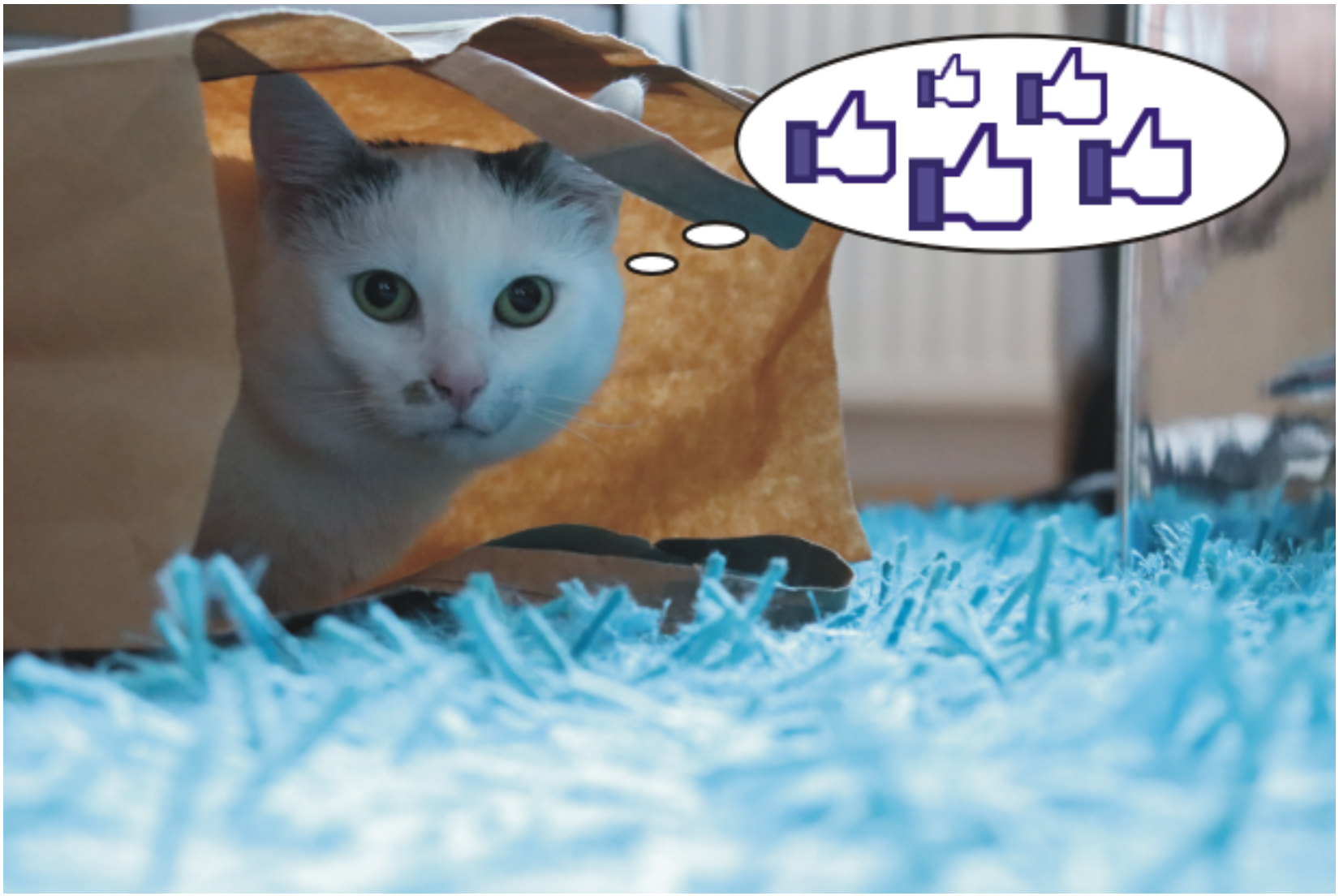
Uživatelská podpora

- Vzdálený přístup ke stanici
  - Stanice zůstává v kanceláři
  - Přístup ze zařízení uživatele
  - Výhoda: navíc „jen“ vzdálený přístup
  - Nevýhoda: „jen“ = zabezpečení zařízení uživatele
- Kombinace uvedených možností
- Nutnost fyzického zásahu
  - Reinstalace, ...
  - Domácí servis (pan ředitel + sekretářka)
  - Uživatel přinese (hmotnost? MHD?)
  - Svoz k servisu (vlastní, kurýr)

Ochrana zařízení

- Fyzická ochrana
  - Krádež, poškození
  - Pracoviště = kancelář, vrátnice, ostraha
  - Doma = bezpečnostní dveře? zamykání?
  - Počítat s rizikem odcizení (šifrovat, zálohovat)
- Přístup k zařízení
  - Pracoviště = firemní kultura
  - Doma = odolnost vůči manželce? dětem? kočce?
  - Oddělená zařízení, oddělené (user) účty
- Vzdálená správa – sdíleno s uživatelem
  - Lokálně lze pozorovat činnost

Ochrana zařízení



Zařízení a síťové prostředí

- Síť organizace
  - Standardy, kapacita
  - Provozní a bezpečnostní monitoring
    (Detekce síťových IoC)
  - Ochrana perimetru (FW, DDoS)
- Domácí síť
  - Wi-fi router $\Rightarrow$ další zařízení v lokální sítí
  - Různí poskytovatelé, kapacita „až *x* Mbit“
- VPN (virtual private network)
  - VPN split tunelling
  - V lokální síti – L2

Autentizace – změny

- Nutnost změny autentizačních prvků
  - Zapomenuté heslo, pin, ...
  - Ztráta tokenu, tel. čísla, ...
- Vydání nových
  - Příchod, ověření, změna, odchod
  - Nutnost ověření identity – osobně (OP, pas, RL)
- Změna hesla na dálku
  - Telefonní číslo + znalost ID
  - Nutno připravit předem
- Multifaktorová autentizace
  - Selektivní / celkové vypnutí 1 až $(m-1)$ faktorů
  - $m > 2 \Rightarrow$ použít $(m-1)$ pro změnu m-tého

Vyjádření souhlasu

- Legislativně-administrativní důvody
  - Odsouhlasení podmínek
  - Potvrzení o seznámení, proškolení
  - Potvrzení absolvování pohovoru
  - Žádost o placenou službu
- Kdo to vyžaduje?
  - Zákon, auditor, vlastní právník, vlastní úředník
- Možnosti
  - Osobní návštěva
  - Pošta, kurýr
  - Elektronický podpis, autentizace MFA

Komunikace s uživateli

- E-mail a systémy pro správu požadavků
  - Beze změny
- Telefonát
  - Zavolám jako vždy – zvoní v prázdné kanceláři
  - Přesměrování telefonů / mobilní čísla
  - Soukromé / služební čísla
- Videokonference místo osobního setkání
  - Nutno dohodnout (nelze „jít kolem“)
- Instant messaging (rychlé zprávy)
  - Skupinové konverzace
  - Slack, Mattermost, ...

Komunikace s uživateli

- S kým se vlastně bavíme?
  - E-mail – elektronický podpis
  - Instant messaging – přihlášený uživatel
  - Telefonní hovor – podle tel. čísla, rozpoznání hlasu (aktuální věrohodný seznam, import)
- Typy informací vs. komunikační kanál
  - Výběr správného (rychlost, obsah, čas)
  - IM, telefon – domluva (rychlé, pohodlné)
  - E-mail – el. podpis, E2E šifrování
- Služby zadarmo (např. instant messaging)
  - Bez smlouvy, záruk – důvěrnost? dostupnost?

Komerční přestávka

Umístění mimo vlastní síť?

Dostupnost při problému?

Spolehlivý partner?

Virtualizační platforma!

Obsluha vstřícná
Ceny přívětivé
Služba kvalitní

https://virtualizace.cesnet.cz

Provozní monitoring

- Zjistit problém + zjednat nápravu
  - Funkčnost jednotlivých částí
  - Možnost realizovat činnost
- Umístění sond
  - Síť organizace
- Home office = uživatel není v síti organizace
  - Přímá dostupnost
  - Dostupnost přes VPN
- Řešení
  - Vlastní sonda v Internetu
  - Sondy na pracovních stanicích

Forenzní laboratoř

Činnosti uživatelů

Používání zařízení

- Umístěná doma
  - Pracovní stanice, laptop, smartphone
  - Základní péče – svépomocí + uživatelská podpora
- Umístěná mimo
  - Laboratoře, kancelář
  - Sdílení, velikost, příkon, ...
  - Zřízení přístupu
- Vzdálený přístup (RDP, SSH)
  - Systémově pro celou organizaci
  - VPN
  - Klíče místo hesel

Přístup ke službám

- Využívání služeb organizace
  - Informační systémy
  - Elektronické informační zdroje
  - Licence
  - ...
- Dostupnost
  - NAT, filtrování IP rozsahu $\Rightarrow$ VPN
- Možnosti přístupu k IS
  - Webové rozhraní
  - Tlustý/tenký klient

    (zkontrolovat protokol, počet licencí)

Využívání licencí

- Počet licencí
- Vlastník zařízení
  - Licenční smlouva – pouze vlastněná organizací
  - Uživatelé používají svá
- Akademické licence
  - Vadí použití manželkou, dítětem, kočkou?
- Včas domluvit s dodavatelem
  - Dokoupit, revidovat a doplnit smlouvu
- Dostupnost licenčních serverů
  - Nutné pro funkci SW (online zápůjčka licence)
  - Filtrování IP $\Rightarrow$ VPN (více rozsahů)

Schůzování

- Schůzování
  - Meeting, call
  - Setkání skupinky lidí + prezentace
- Adekvátní náhrada
  - Videokonference
- Bezpečné používání
  - Samostatná prezentace

    „Také u videokonferencí je třeba dbát na bezpečnost!“
  - Kolega Miloš Liška

Spolupráce

- Práce v týmech
  - Tvorba dokumentů
  - Diskuse nad schématem
  - Hledání vhodného řezu na CT snímcích
- Náhrada – kolaborativní prostředí
  - Např. Google Workspace (Google Apps)
  - Prakticky použitelné
  - Omezené zážitky (lze kombinovat s VC)
- Problém – řízení přístupu
  - Normálně: vidíme, kdo je přítomen
  - Kolaborativní prostředí: nastavení práv

Spolupráce

- Řízení přístupu
  - Pouze správce (správci) dokumentu
  - Výčet uživatelů
  - Použití skupin
  - Nepoužívat odkaz (security by obscurity)
- Předání výsledku
  - Mimo kolaborativní prostředí
  - Vývoj vs. finální výsledek
- Zálohování
  - Nezávisle na službě (má jiné priority)
- Smluvní podmínky

Sdílení, předávání výsledků

- Výstupy na pracovní stanici
  - Předat ostatním, odevzdat nadřízenému
- Standardní postup pro 21. století
  - Dokumentová a datová úložiště, sdílené disky
- Konzervativní uživatel
  - Příloha e-mailu, USB flash disk
- Práce z domova $\Rightarrow$ kreativní řešení
  - Úložiště, které zná (ulož.to, úschovna.cz, ...)
  - Důvěrnost dat?
- Práce na stanici $\Rightarrow$ zálohovat
  - Instalace, konfigurace, NAT, kapacita sítě, protokol

Sekundární komunikace

- Neformální informační toky
  - Náhodná spolujízda výtahem
  - Společná služební cesta
  - Povídání si při vaření kávy, na obědě
- Obsah
  - Kdo na čem pracuje + zajímavosti
  - Kolize v plánech
  - Nápady na vylepšení
- Náhrada při home office
  - Instant messaging (podpora skupin, kanálů)
  - „Kávové“ videokonference

Forenzní laboratoř

Zvýšená rizika pro uživatele

Úpadek firemní kultury

- Firemní kultura
  - Standardy, zaběhnuté postupy
  - Všichni okolo se chovají stejně
- Home office
  - Okolo není nikdo $\Rightarrow$ oslabení vlivu koletivu
  - Opouštění standardních postupů

    (+ problém osvojit si nové)
  - Od drobností po vážné problémy

Úpadek firemní kultury

Úpadek firemní kultury

- Příčina
  - Pokušení být kreativní
  - Zjednodušování si práce
  - Nevidí další souvislosti
- Řešení – zvýšit skupinové působení
  - Připomínat správné postupy
  - Proškolení
  - Jít příkladem (!)
  - Dostatek sekundární komunikace
- Vylepšení postupů
  - Správný = uživatelsky výhodný

Sociální inženýrství

- Nevýhoda pro uživatele
  - Odtržení od kolektivu
  - Omezená sekundární komunikace
  - Neví co se děje (v organizaci)
  - Mnoho změn $\Rightarrow$ nové kontextové možnosti
- Phishing
  - Nová služba
  - Přihlášení o kompenzace
  - Souhlas s home office
  - Očkování jako firemní benefit

Sociální inženýrství

- Fake news (falešné zprávy)
  - Nepodložené, často zcela vymyšlené
  - Ovlivnění a manipulace
- Zaměření
  - Organizace (změny postupů, propouštění, ...)
  - Obecná témata (UFO, politika, vir, ...)
- Řešení – kritické myšlení
  - Víc hlav víc ví
  - Sekundární komunikace
  - Mnohdy zajímavé diskuse
- Předcházení vzniku
  - Dostatek pravdivých a ověřených zpráv

Forenzní laboratoř

Shrnutí

Shrnutí

- Virus $\Rightarrow$ nové pořádky $\Rightarrow$ přechodová doba
  - Řada problémů
  - Nové příležitosti
- Motor pokroku
  - Krizová situace
  - Války, ...
- Nemáme na výběr
  - Reálná hrozba (virus)
  - Příkazy (státní rozhodnutí)
- Optimalizace postupů
- Příjemná a bezpečná (!) práce uživatelů

Forenzní laboratoř

Diskuse