Kybernetická bezpečnost ve firmách v souladu se ZKB

Vyhláška č.82 o bezpečnostních opatřeních – hlava II

Jiří Zvolánek | SE Czechia

CCSE, CCNP Security, CCNP

25.04.2024

YOU DESERVE THE BEST SECURITY

Vyhláška č.82 – Hlava II – Technická opatření

§ 17 Fyzická bezpečnost

§ 18 Bezpečnost komunikačních sítí

§ 19 Správa a ověřování identit

§ 20 Řízení přístupových oprávnění

§ 21 Ochrana před škodlivým kódem

§ 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

§ 23 Detekce kybernetických bezpečnostních událostí

§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí

§ 25 Aplikační bezpečnost

§ 26 Kryptografické prostředky

§ 27 Zajišťování úrovně dostupnosti informací

§ 28 Průmyslové, řídicí a obdobné specifické systémy

§ 18 Bezpečnost komunikačních sítí

Požadavky paragrafu:

- segmentace
- řízení
- důvěrnost a integritu při vzdáleném přístupu
- blokovat nežádoucí komunikaci
- používáte nástroj pro segmentaci a řízení

Technická řešení:

Next Generation Firewall

SASE / ZTNA + SDWAN

§ 19 Správa a ověřování identit

Požadavky paragrafu:

- Centrální nástroj pro správu
- MFA
- Když né MFA, tak dlouhé heslo
- Pravidelná změna hesel
- Edukace k tvorbě hsla

Technická řešení:

Identity Management

Active Directory

§ 20 Řízení přístupových oprávnění

Požadavky paragrafu:

- Centralizovaný nástroj pro řízení přístupových oprvánění

Technická řešení:

Active Directory

Entra ID

Radius

§ 21 Ochrana před škodlivým kódem

Požadavky paragrafu:

- Použije nástroj na nepřetržitou automatickou ochranu
  - Stanic
  - Mobilních zařízení
  - Serverů
  - Datových úložišť
  - Komunikační sítě

Technická řešení:

Běžně dostupné AV

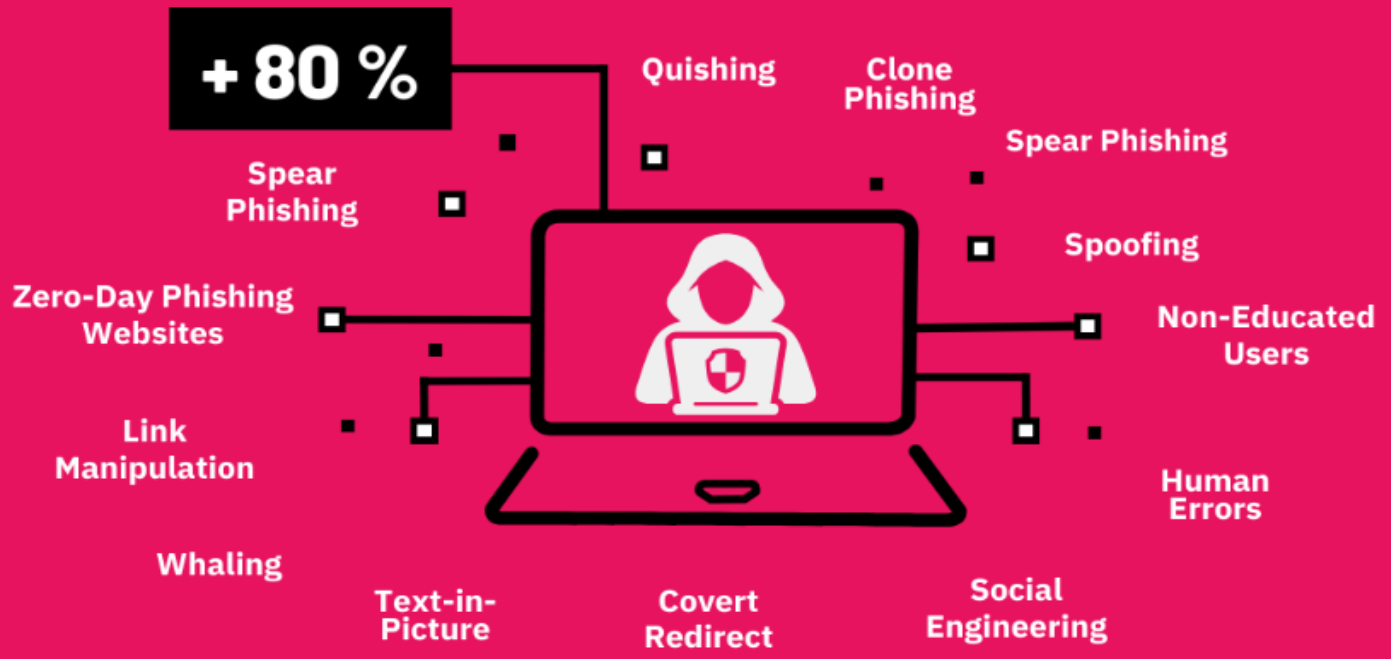
EDR/EPR

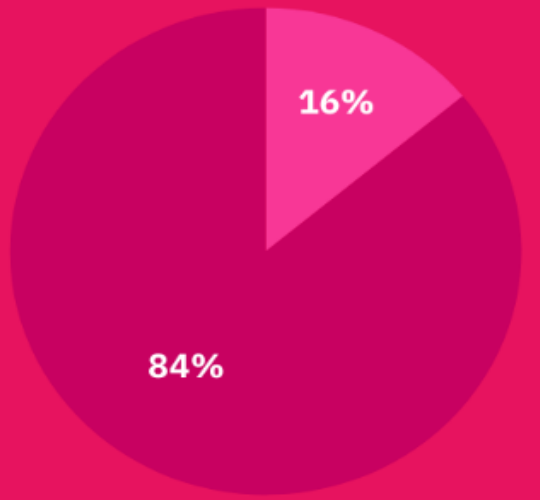
Ochrana mailového vektoru

NGFW

MTD

Kybernetické útoky





cp<r>
CHECK POINT RESEARCH

Delivery Protocols - Email vs. Web Attack Vectors in 2022

Přes 80% kybernetických útoků začíná přes email.
Moderní phishing je složité řešit!

YOU DESERVE THE BEST SECURITY

§ 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

Požadavky paragrafu:

- Zaznamenává bezpečnostní a provozní události
- Určuje v jaké rozsahu logujete
- Synchronizace času
- Uchování 12 až 18 měsíců

Technická řešení:

Syslog

NAS

3rd party syslog řešení

Cloud storage

§ 23 Detekce kybernetických bezpečnostních událostí

Požadavky paragrafu:

- Používá nástroj na detekci kybernetických bezp. událostí
- Blokování nežádoucí komunikace
- Koncové stanice, mobilní zařízení, servery ...

Technická řešení:

NGFW

IPS

EDR

§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí

Požadavky paragrafu:

- Používá nástroj na sběr a **vyhodnocování** k.b.u. §21 a §22
- Vyhledávání a vyhodnocování událostí
- Omezit případy nesprávného vyhodnocování
- Využít informace k optimálnímu nastavení bezpečnostních opatření

Technická řešení:

SIEM

SOC

XDR řešení

20
XDR/XPR Sources

3 Months of XDR/XPR Efficiency

2 TRILLION
EVENTS

Infinity
XDR/XPR

99%
NOISE REDUCTION

600K
HIGH/CRITICAL
INCIDENTS

§ 25 Aplikační bezpečnost

Požadavky paragrafu:

- Provádět penetrační testy
  - Před uvedením do provozu
  - Při významné změně
  - Provádět penetrační testy
- Zajisti trvalou ochranu aplikací
  - Před neoprávněnou činností
  - Popřením provedených činností

Technická řešení:

Penetrační testování

Bezpečný vývoj

§ 26 Kryptografické prostředky

Požadavky paragrafu:

- Používáte aktuálně odolné kryptografické algoritmy a kryptografické klíče
- Používáte systém správy klíčů a certifikátů
- Bezpečně nakládat s kryptografickými prostředky
- Zohledňujete doporučení NÚKIB

Technická řešení:

Key Management system

Password manager

Zdravý rozum a systematický přístup

§ 27 Zajišťování úrovně dostupnosti informací

Požadavky paragrafu:

- Vysoká dostupnost
  - Informačních a komunikačních sytémů
- Odolnost
- Redundance aktiv potřebných k zajištění dostupnosti

Technická řešení:

Zálohované konektivity

Redundance síťových prvků

Redundance serverů/virtualizace

Disaster recovery

§ 28 Průmyslové, řídicí a obdobné specifické systémy

Požadavky paragrafu:

- Kybernetická ochrana průmyslových a řídících systémů
- Použít technické a programové prostředky přímo určené do průmyslového prostředí
- Oddělit tyto systém od ostatní infrastruktury
- Chránit před zranitelnostmi
- Omezit vzdálený přístup

Technická řešení:

NGFW – ruggedized

Specialized XIoT systems (OT, IoMT)

Zásadní změny v technických opatřeních NIS2

Dva režimy vyhlášky

Vyšší režim pro základní subjekty subjekty (18 měsíců retence, mají § 24 Vyhodnocování kybernetických bezpečnostních událostí)

Nižší režim pro důležité subjekty (12 měsíců retence, chybí § 24 Vyhodnocování kybernetických bezpečnostních událostí)

Základní subjekty by tak měly podléhat komplexnímu režimu dohledu ex ante a ex post, zatímco důležité subjekty by měly podléhat mírnému režimu

§21 Ochrana před škodlivým kódem se v NIS2 sloučil s paragrafem "Detekce kybernetických bezpečnostních událostí"

Návrh nové vyhlášky - §21/25 Aplikační bezpečnost

Paragraf „Aplikační Bezpečnost“ se zásadním způsbem rozšířil:

- Provozovat aktiva na výrobcem podporovaných platformách
- Provádět bezpečnostních aktualizací
- Skenování zranitelností (alespoň jednou ročně)
  - Zohlednit výsledky skenování
- Přiměřeně provádí penetrační testy (pro významná aktiva)

Případová studie – finanční náročnosti z pohledu produktů a služeb kybernetické bezpečnosti

Profil subjektu

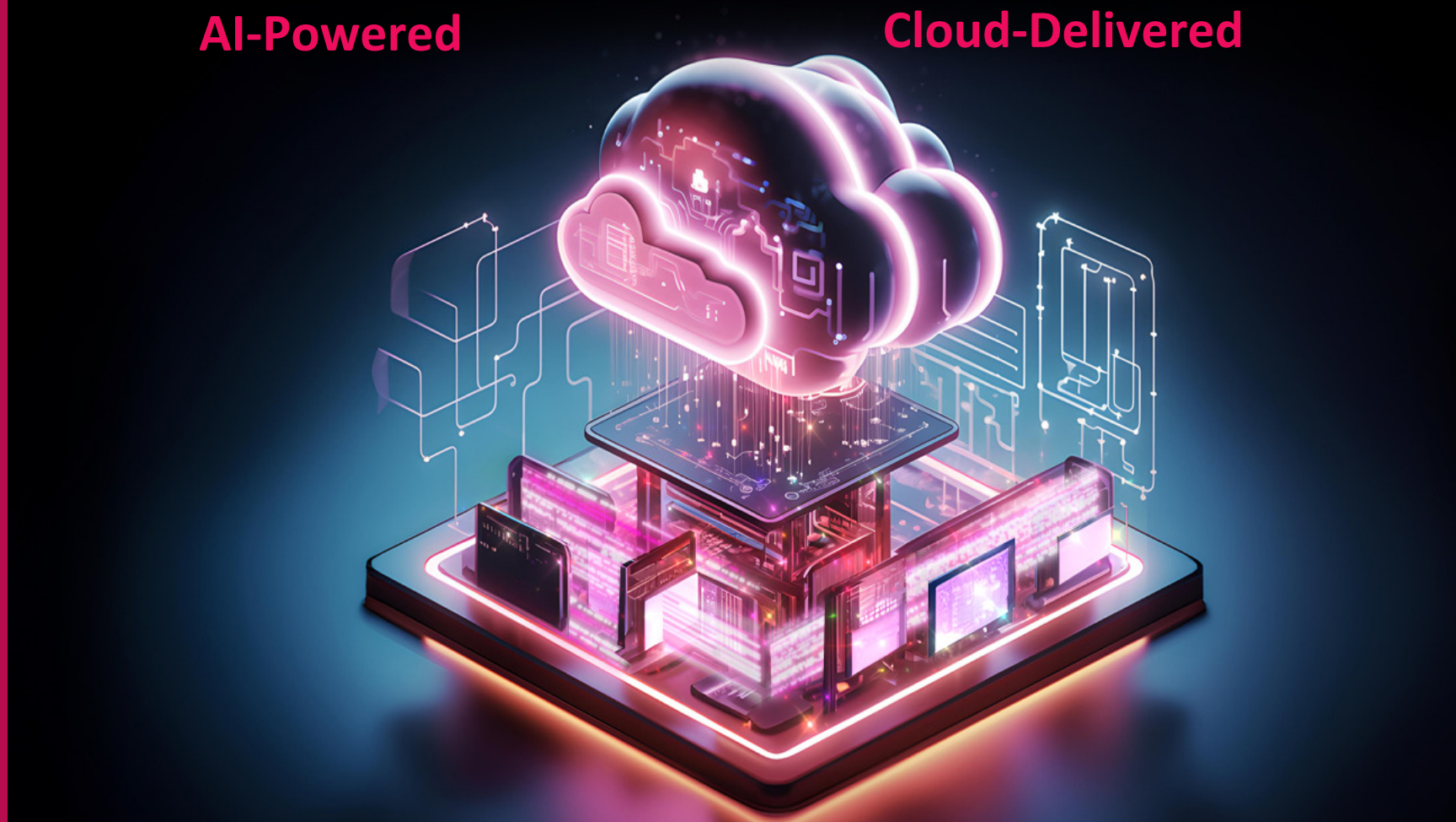
- Výrobní závod 150FTE
- 50 uživatelů využívajících IT
- Signaturní antivir, jeden firewall, žádná segmentace sítě, minimální vysoká dostupnost na úrovni infrastruktury
- 1 fyzický (3virtuální) server
- 2 lidé v IT

Výsledek:

- 2x NGFW firewall
- EDR pro koncové uživatel
- Ochrana mobilních zařízení
- Ochrana emailů

= 280 000,- Kč na tři roky v produktech a službách

Collaboration
Is the only way
to gain advantage
over the attacker



CHECK POINT

Thank You!

YOU DESERVE THE BEST SECURITY