POZVÁNKA

AmCham Slovakia

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

ZÁKLADY KYBERNETICKEJ BEZPEČNOSTI PRE MALÉ A STREDNÉ PODNIKY

AMCHAM SLOVAKIA

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Embassy of the United States of America · Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · SBA Slovak Business Agency · accenture · SIEMENS Healthineers · Void

AGENDA

09:00 **Otvorenie**

09:15 **GOVERN – Riadenie**

09:45 **IDENTIFY - Identifikácia**

10:15 **PROTECT – Ochrana**

11:15 **Prestávka**

11:45 **DETECT – Objavenie**

12:15 **RESPOND - Reakcia**

12:40 **RECOVER - Obnova**

AmCham Slovakia

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Embassy of the United States of America | Kompetenčné a certifikačné centrum kybernetickej bezpečnosti | SBA Slovak Business Agency | accenture | SIEMENS Healthineers | Void

MICHAL KOSORÍN
Siemens Health

MARTIN LOHNERT
Void

MATEJ SPIŠÁK
Accenture

SIEMENS Healthineers

Siemens Healthineers

Slovakia

Michal Kosorín
SHS IT DEI CYS PRO CSA
Jún 2025

We pioneer breakthroughs in healthcare.
For everyone. Everywhere. Sustainably.

SIEMENS Healthineers

Viac ako 1000 zamestnancov

3 pobočky na Slovensku

Návrh a vývoj špecializovaného medicínskeho softvéru

Líder na trhu vo väčšine modalít

Vyše 800 inštalovaných modalít

SIEMENS Healthineers

61,2 % podiel na trhu medicínskej techniky

Najrýchlejší a najspoľahlivejší servis diagnostických prístrojov

Obrat viac ako 159,6 mil. €

Najvyšší počet servisných technikov na Slovensku

Lokálni aplikační špecialist

Rozsah aktivít Siemens Healthineers na Slovensku:

Najsilnejší partner pre zdravotníctvo budúcnosti

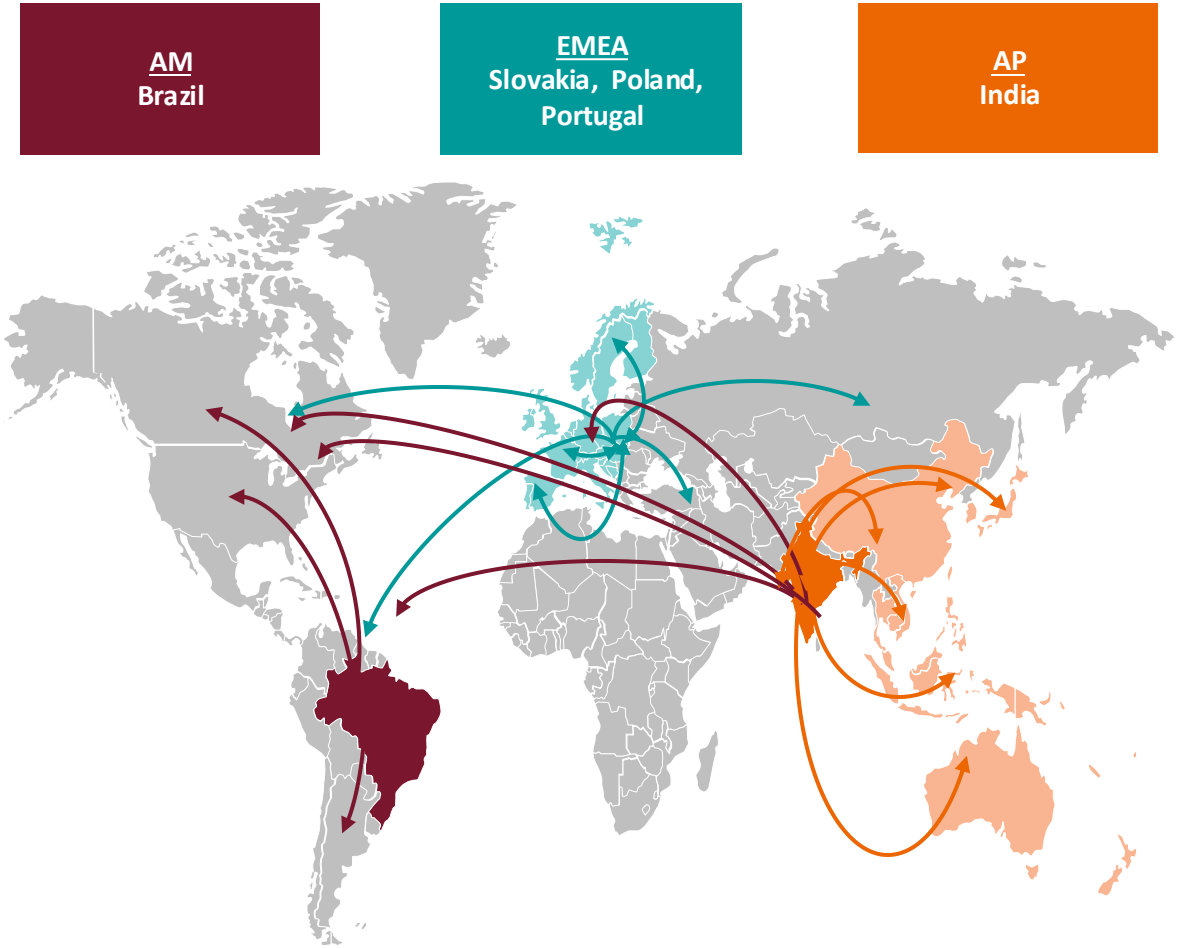
Bratislava
Lamačská cesta 3/B
841 01 Bratislava

Žilina
Legionárska 1
010 01 Žilina

Košice
Trieda SNP 37
040 11 Košice

Global Delivery Center

Hrá kľúčovú úlohu v globálnej stratégii IT organizácie, ktorej hlavnými cieľmi sú digitálna IT transformácia, inovácie pre užívateľov a Cybersecurity pre viac ako 71 000 zamestnancov spoločnosti Siemens Healthineers po celom svete.



Ing. Michal Kosorín, CISA, CISM, CEH, ECSA

SIEMENS Healthineers

CyberSecurity Architect v Siemens Healthineers (od 12/2021)
- Architekt pre Zero Trust Architektúru

Cyber Security Architect v Clarios (03/2020 – 11/2021
- Zodpovedný za posudzovanie, navrhovanie, riešenie a integráciu kybernetickо-bezpečnostných riešení s globálnym dosahom v rámci koncernu Clarios

Senior Specialist – Information Security v Linde (05/2014 – 02/2020)
- Zodpovedný za celkový proces interného penetračného testovania + výkon penetračného testovania s globálnym dosahom v rámci koncernu Linde
- Zodpovedný za dizajn bezpečnostného incident reporting
- Spravoval IDS riešenia

Information Security Officer v Allianz (09/2011 – 04/2014)
- Celková zodpovednosť za Information Security program, BCP & DR programy lokálnej pobočky s regionálnym dosahom (CEEMA)
- Manažment/správa väčšiny lokálnych kybernetickо-bezpečnostných riešení

Security Officer v ING Bank Slovakia (06/2007-08/2011)
- Prvá pracovná skúsenosť s kybernetickou bezpečnosťou
- BIA/ITRC analýzy pre lokálnu pobočku ING Bank
- Podpora BCP procesov
- Podpora IAM procesov

Bratislava
Lamačská cesta 3/B
841 01 Bratislava

Žilina
Legionárska 1
010 01 Žilina

Košice
Trieda SNP 37
040 11 Košice

void SOC

- Špecializované dohľadové stredisko digitálnej bezpečnosti
- Nepretržitý monitoring 24/7/365
- Špičkové technológie
- Certifikovaní špecialisti na:
  - Etický hacking
  - Forenzné vyšetrovanie
  - Analýzu incidentov
- Procesy, postupy a skúsenosti
- Člen SOITRON Group

www.voidsoc.com

What sets us apart

Global Focus

We serve more than **9.000 clients** in **120+ countries**

Technology leadership

We´re the **#1 largest** independent technology services provider

>799.000

professionals worldwide

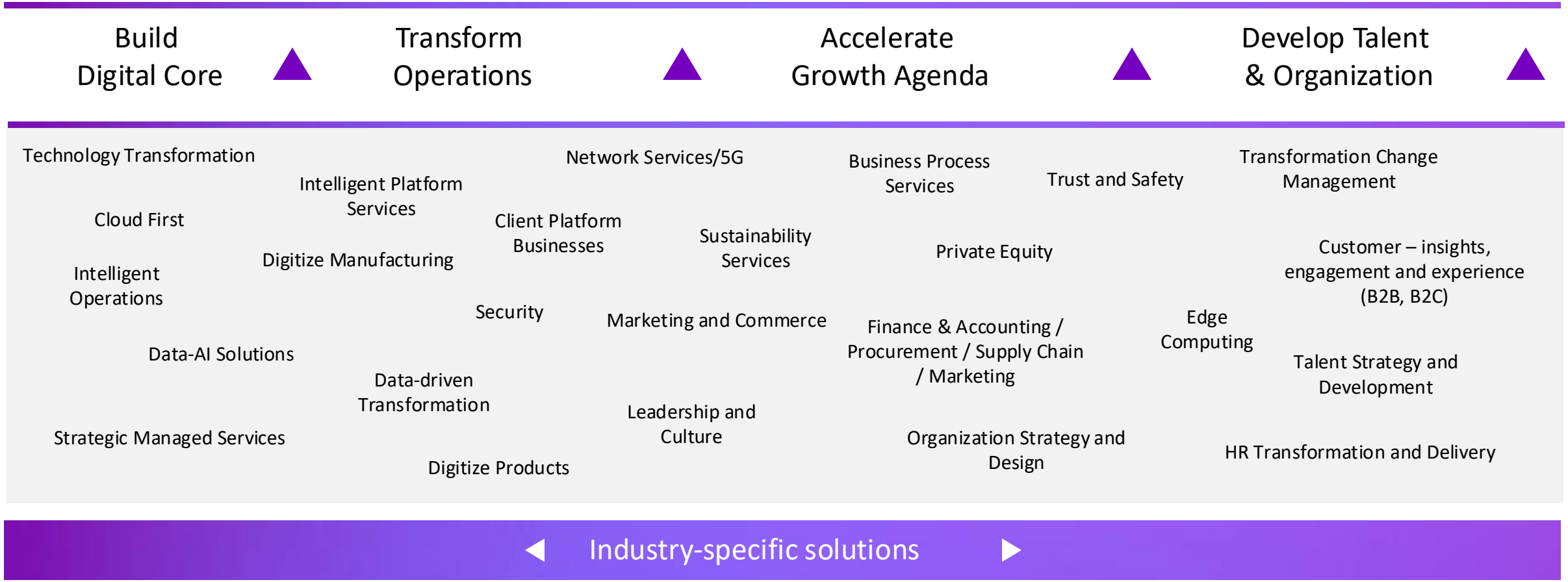
Industry differentiation

We have expertise in more than **40 industries** across **19 industry groups**

Trusted client relationships

of our top **100 clients** have been our clients for at least **10 years**

We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Song



Matej Spišák

Accenture

NIST CYBERSECURITY FRAMEWORK 2.0

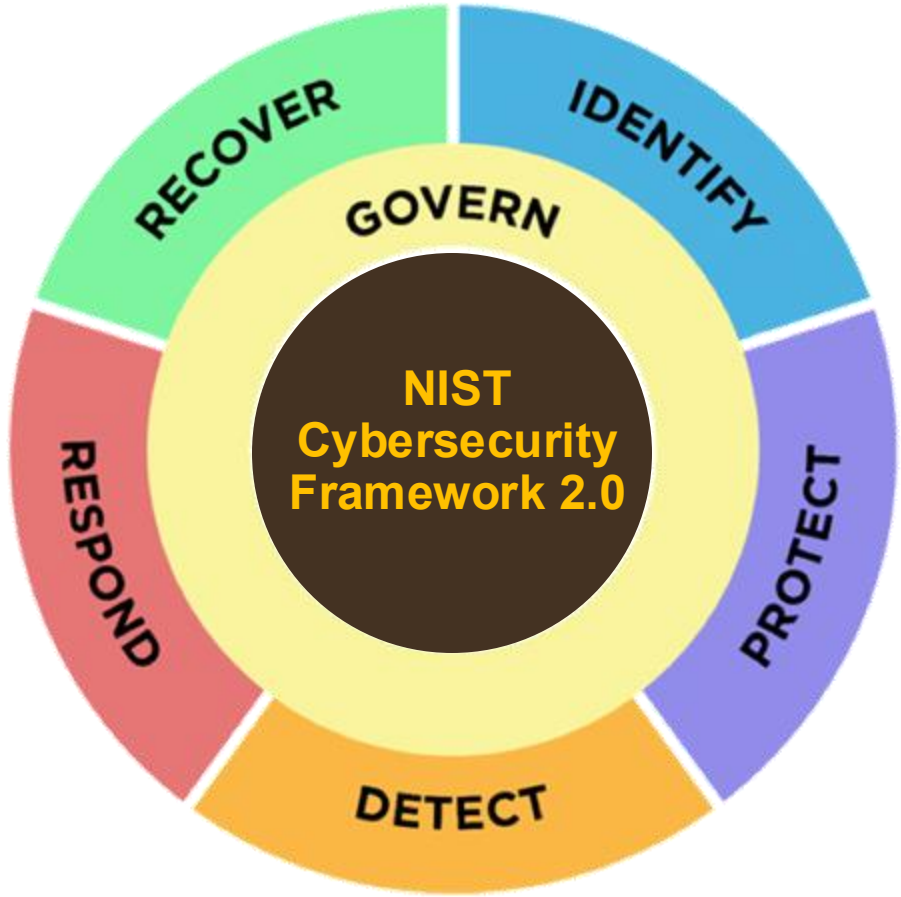
AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Jadro NIST CSF

- Od toho, čo urobíme počas funkcie GOVERN, sa bude odvíjať všetko ostatné
- **Cieľ**: stanoviť si priority v oblasti kybernetickej bezpečnosti
- **Výstup**: základy pre stratégiu kybernetickej bezpečnosti, politiky, štruktúru riadenia
- **Kľúčové kategórie**: organizačný kontext, riadenie rizík, právne prostredie, úlohy, politiky

GOVERN



AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Čo potrebujeme vedieť pri vytváraní nášho programu kybernetickej bezpečnosti?

Organizačný kontext – poslanie

- **Určime si:**
  - Aké je poslanie našej spoločnosti
  - Čo sú kľúčové služby, ktoré poskytujeme
  - Na čom sú tieto služby závislé
  - Čo nám môže zabrániť v ich poskytovaní

GOVERN

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

GOVERN

Aké je poslanie vašej firmy?

Aké kybernetické riziká vám môžu zabrániť v dosahovaní vášho poslania?

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

GOVERN

Čo potrebujeme vedieť pri vytváraní nášho programu kybernetickej bezpečnosti?

Legislatívne, zmluvné a regulačné požiadavky:

- Aké zákony ovplyvňujú to, čo potrebujeme v oblasti kybernetickej bezpečnosti robiť?
- Aké zmluvné podmienky upravujú fungovanie s našimi partnermi?
- Aké sektorové regulácie v oblasti kybernetickej bezpečnosti sa nás týkajú?

Týka sa vás napríklad zákon o kybernetickej bezpečnosti? Indikatívna pomôcka na určenie subjektu ako poskytovateľa základnej služby

KCCKB workshop k NIS2 Webináre NIS2 - Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Čo potrebujeme vedieť pri vytváraní nášho programu kybernetickej bezpečnosti?

Organizačný kontext – riadenie rizík:

- Riziká musíme prioritizovať
- Musíme si zvoliť prístup
- Potrebujeme riadiť aj riziká spojené s dodávateľmi
- Kybernetické riziká musíme zakomponovať do podnikového riadenia rizík a informovať vedenie

G O V E R N

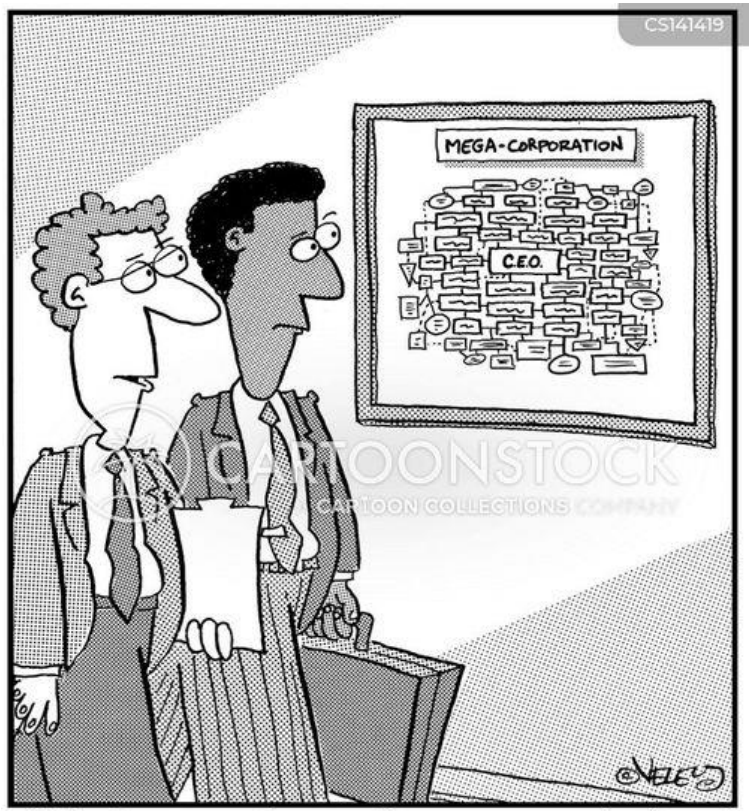
AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

GOVERN

Čo potrebujeme vedieť pri vytváraní nášho programu kybernetickej bezpečnosti?

Role, zodpovednosti, politiky:

- Jasne stanovené a komunikované úlohy
- Povinnosti a očakávané správanie sú definované
- Všetko je dokumentované v politikách



"The key to understanding our organizational structure is in the boss's personal motto: 'Keep your friends close, and your enemies closer!'"

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Náš prístup ku kybernetickej bezpečnosti sa mení v čase

- Pri zmenách v našej spoločnosti
- Pri nových požiadavkách
- Pri zmenách bezpečnostného prostredia
- Po významných incidentoch
- Na základe merateľných ukazovateľov

GOVERN

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

GOVERN

Odporúčania pri funkcii GOVERN

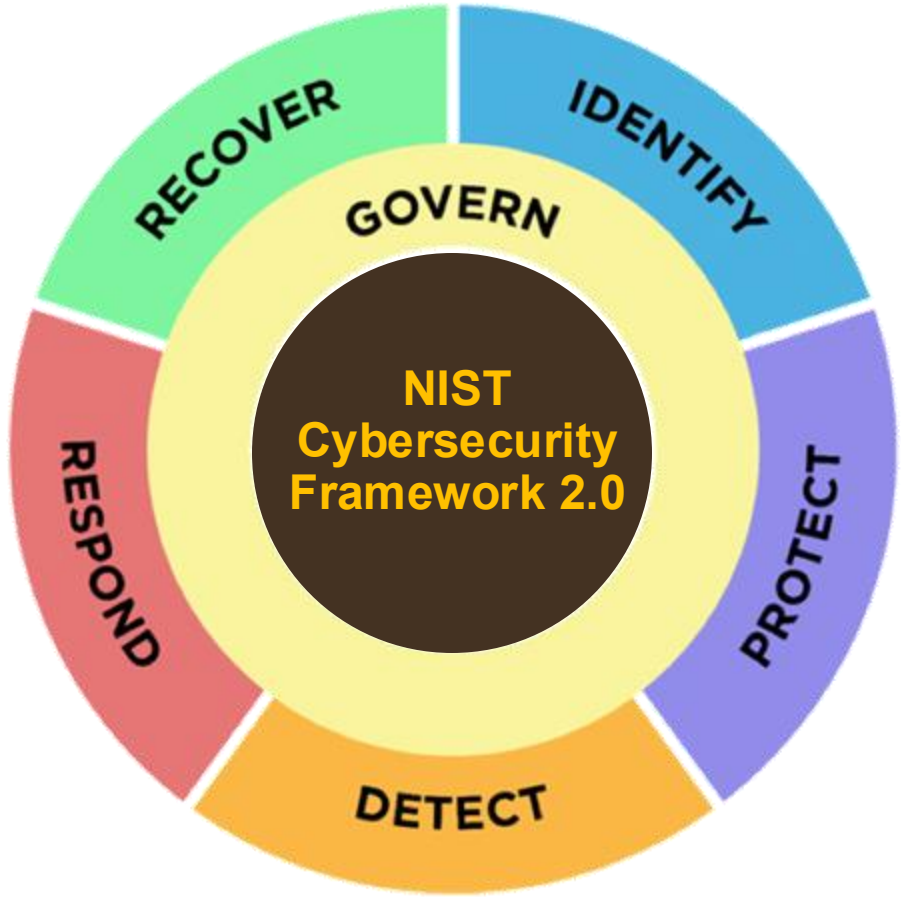
- Čo robíme?
- Čo potrebujeme k tomu aby sme to mohli robiť?
- Ako nám v tom dokážu zabrániť riziká v oblasti kybernetickej bezpečnosti?
- Ako k rizikám pristupujeme?
- Ako nás ovplyvňujú právne požiadavky?
- Kto je vo firme zodpovedný za ktorú oblasť kybernetickej bezpečnosti?
- Aké sú naše plány a naše očakávania a kde sú definované?

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

IDENTIFY

- **Cieľ:** Pochopiť aktíva organizácie, riziká a obchodné prostredie
- **Výstup:** Informované rozhodnutia o riadení rizík
- **Kľúčové kategórie:** Správa aktív, Hodnotenie rizík, Zlepšenia Cybersecurity procesov
- **Poznanie vášho digitálneho prostredia:** Identifikácia je o pochopení, aké digitálne aktíva vaša firma má a akým rizikám čelí. Jednoducho povedané – "Nemôžete chrániť to, o čom neviete, že to máte."



Správa aktív

- **Účel:** Viesť evidenciu aktív (hardvér, softvér, dáta, ľudia)
- **Čo sú Vaše aktíva?**
- **Aké sú Vaše najkritickejšie podnikové aktíva** (údaje, hardvér, softvér, systémy, zariadenia, služby, ľudia atď.), **ktoré potrebujete chrániť?**
- **Ako na to:**
  - Príklad HW+SW inventára: CIS Hardware and Software Asset Tracking Spreadsheet
  - Ak chcete open-source aplikáciu: GitHub - snipe/snipe-it: A free open source IT asset/license management system
  - Kompletný metodický postup na správu IT aktív napr. tu: SP 1800-5, IT Asset Management | CSRC
  - Viete, čo všetko máte na firemnej sieti? Nmap: the Network Mapper - Free Security Scanner

Program kyberbezpečnosti, aký by si ste si želali

Program kyberbezpečnosti, na aký máte zdroje

Správa aktív

Aké sú Vaše top 3 najcennejšie firemné aktíva?

IDENTIFY

Hodnotenie rizík

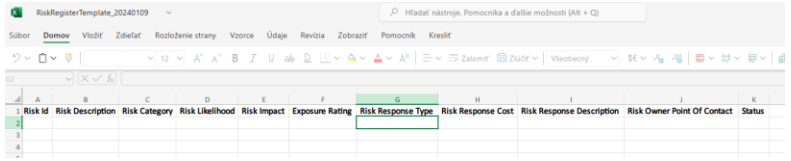
- **Účel:** Identifikovať kybernetické riziká a zraniteľnosti
- **Kľúčové aspekty:**
  - Hodnotenie zraniteľností
  - Identifikácia externých a interných hrozieb
  - Hodnotenie rizík
  - Používanie metodík hodnotenia rizík
- **Čo by sa mohlo pokaziť?**
  - Identifikujte potenciálne hrozby: Kybernetické útoky (ransomvér, phishing), narušenie údajov, náhodná strata údajov, zlyhanie zariadenia.
  - *Príklad:* "Čo najhoršie by sa mohlo stať, ak by vám ukradli údaje o zákazníkoch?"
- **Posúďte zraniteľnosti:** Zastaraný softvér, slabé heslá, nedostatok záloh.
- *Príklad:* "Používate rovnaké heslo pre všetko? To je zraniteľnosť."
- **Zvážte dopad:** Ako by kybernetický útok alebo strata údajov ovplyvnila vaše podnikanie?
- *Príklad:* "Mohli by ste fungovať bez počítačov deň, týždeň alebo mesiac?"

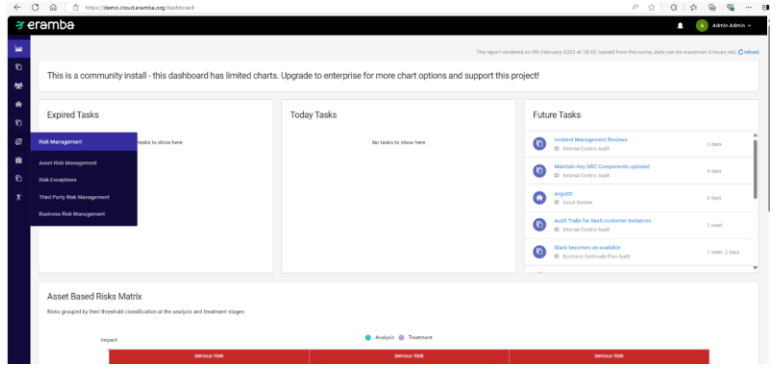
IDENTIFY

Riadenie kybernetických rizík

Hodnotenie rizík

1. **Identifikácia**
2. **Rozhodnutie**
   - Reakcia na riziko: zamedzenie, redukcia, akceptovanie, presun
3. **Ako na to:**
   - Databázy zraniteľností: CVE, NVD, OpenVAS Skener
   - Top hrozby pre kybernetickú bezpečnosť: ENISA Threat Landscape 2024, Foresight Cybersecurity Threats For 2030
   - Dopad útokov: IBM: Cost of a data breach 2024
4. **Nástroje na hodnotenie rizík:**
   - NIST: Vzorová tabuľka na správu rizík a Príručka
   - Nástroj: napr. Eramba Community

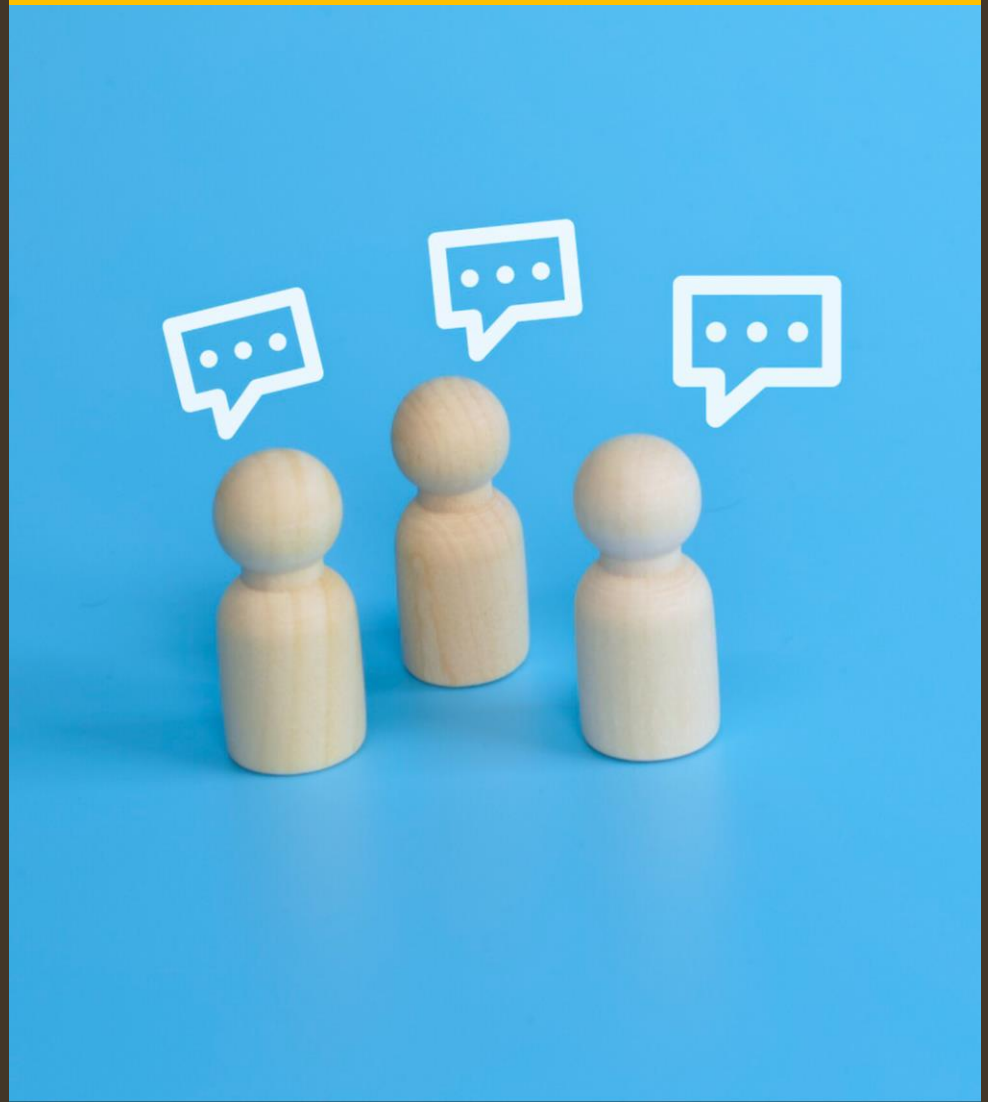




Hodnotenie rizík

Aké sú podľa Vás top 3 najväčšie kyber hrozby pre Vaše podnikanie?

IDENTIFY



Praktické kroky - Zhrnutie

Pochopiť

- Pochopte, na akých aktívach závisí vaše podnikanie, vytvorením a udržiavaním inventára hardvéru, softvéru, systémov a služieb. (ID.AM-01/02/04)

Posúdiť

- Posúďte svoje aktíva (IT a fyzické) z hľadiska potenciálnych hrozieb. (ID.RA-01)
- Posúďte efektívnosť kybernetického bezpečnostného programu podniku, aby ste identifikovali oblasti, ktoré potrebujú zlepšenie. (ID.IM-01)

Prioritizovať

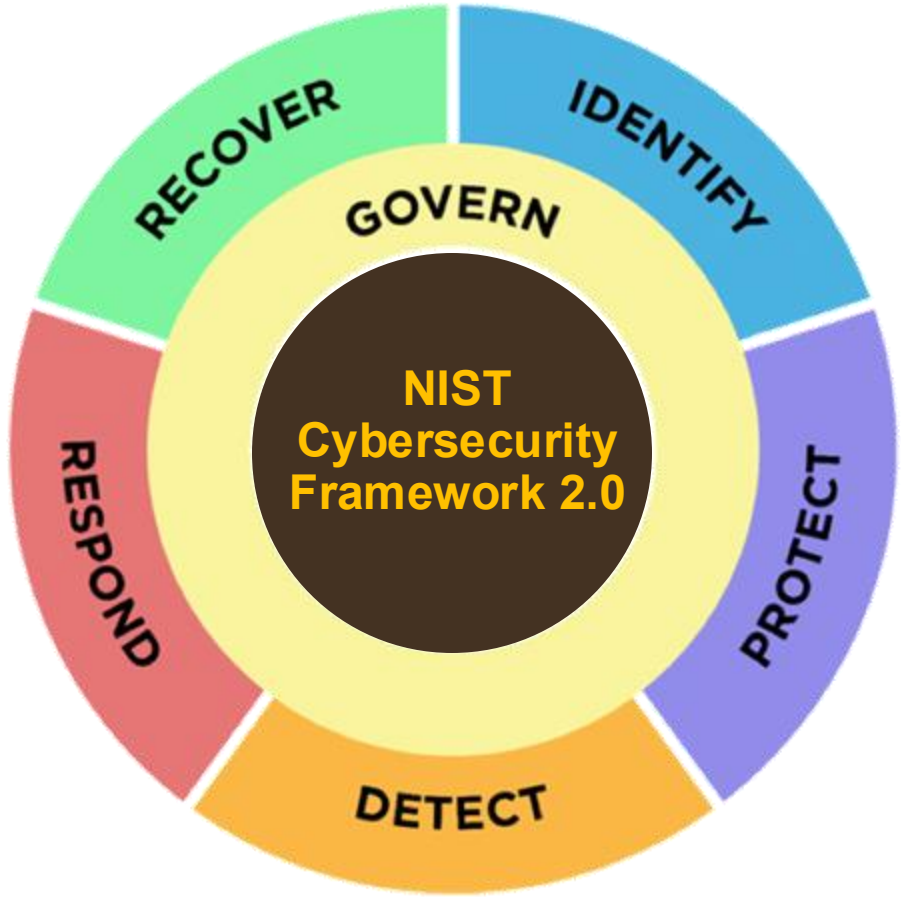
- Prioritizujte na základe inventarizácie a klasifikácie aktív vášho podniku. (ID.AM-07)
- Prioritizujte dokumentovanie interných a externých kybernetických hrozieb a súvisiacich reakcií pomocou registra rizík. (ID.RA)

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

- **Cieľ:** Implementovať opatrenia na ochranu kritických aktív a zabezpečenie kontinuity podnikania
- **Kľúčové kategórie:** Riadenie prístupu, Osveta a školenia, Ochrana údajov, Ochrana technológií, Odolnosť technologickej infraštruktúry
- **Výstup:** Ochrana znamená implementáciu bezpečnostných opatrení na základe toho, čo ste identifikovali v predchádzajúcom kroku.

PROTECT

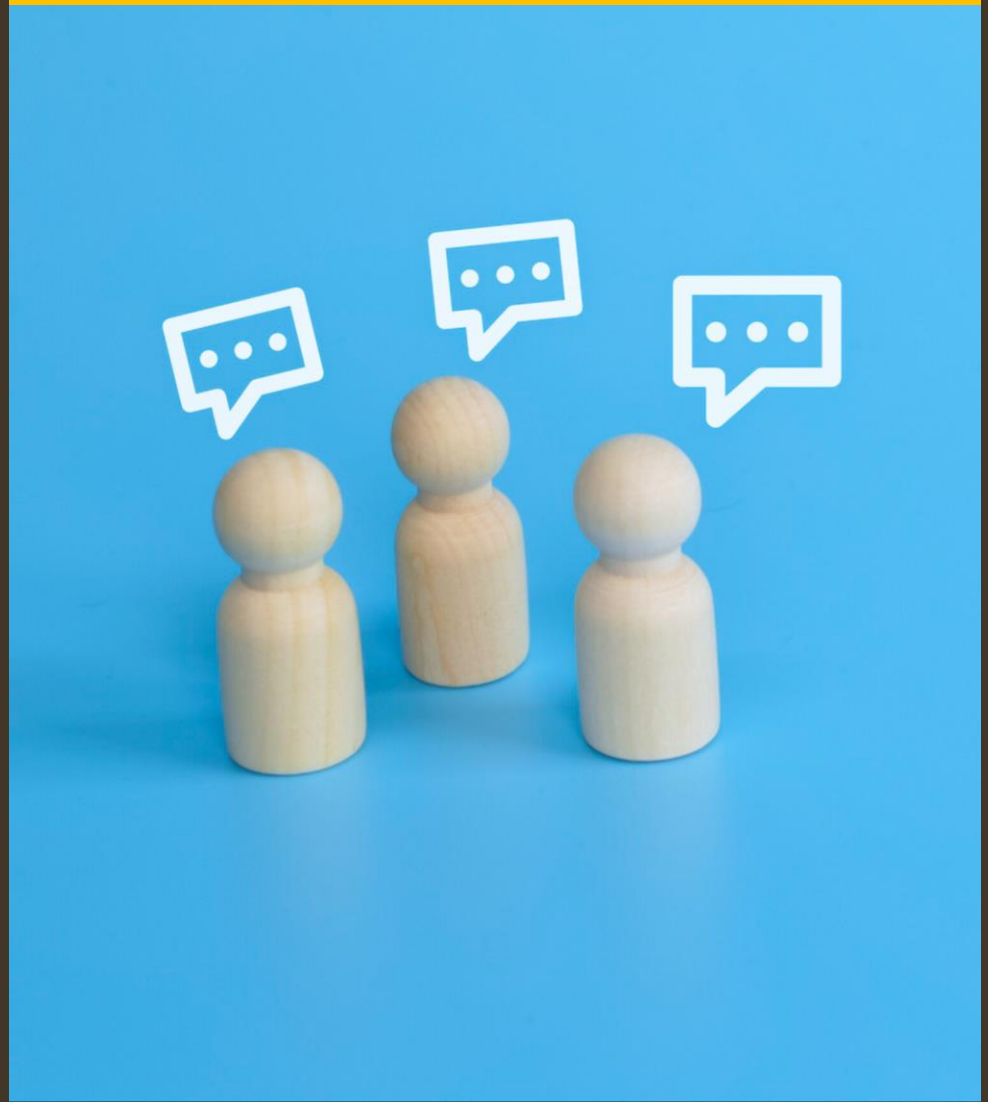


Riadenie prístupu

Rozcvička s rukami

- Kto si zapisuje heslá na papier alebo do Excelu/Wordu/Notepadu vo svojom/firemnom počítači?
- Kto z Vás používa ako základ svojho hesla niečo, čo je Vám blízke? (meno psa, názov firmy, názov systému do ktorého pristupujete, atď.)
- Kto z Vás sa prihlasuje do svojho počítača s admin privilégiami?
- Kto z Vás ma najvyššie administrátorské privilégia (global admin) vo Vašej firme?

PROTECT



Riadenie prístupu

Kto sa dostane dnu?

- Princíp najmenších privilégií.
- Používajte silné, jedinečné heslá pre všetky účty.
- *Príklad:* "Správca hesiel vám s tým môže pomôcť."

Viacfaktorová autentifikácia (MFA) vždy, keď je to možné. *Príklad:* „Predstavte si to ako pridanie ďalšieho zámku na vaše dvere.“

Kam presne sa viem dostať?

- Obmedzte prístup k citlivým údajom – dajte zamestnancom prístup len k tomu, čo potrebujú pre svoju prácu.

P R O T E C T

PROTECT

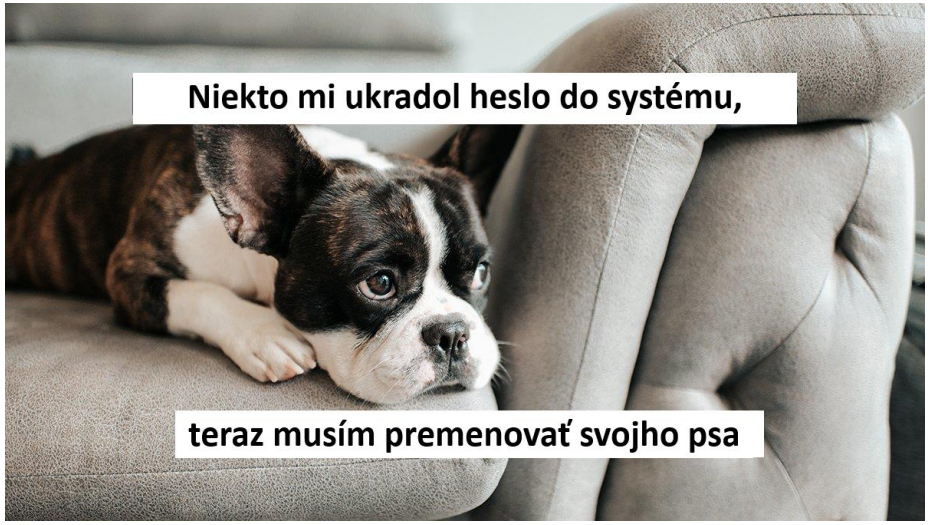
Riadenie prístupu - Heslá

Definícia problému

- 99% útokov na identitu sú založené na útokoch na heslá*
- Útočník zneužíva očakávateľné vzory ľudského správania:
  - Slabé heslá
  - Opakujúce sa heslá
  - Náchylnosť podľahnúť phishingovým útokom

Riešenie problému

- Silné Heslá, MFA alebo dokonca aj Password-less autentifikácia
- Vzdelávanie zamestnancov
- Princíp minimálneho prístupu



* 10 essential insights from the Microsoft Digital Defense Report 2024 | Security Insider

PROTECT

Riadenie prístupu - Heslá

Slabé Heslá*

Findings — Slovakia

Rank	Password	Time to crack it	Count
1	123456	< 1 second	1,521
2	123456789	< 1 second	790
3	qwerty123	< 1 second	372
4	qwerty1	< 1 second	329
5	12345	< 1 second	248
6	super123	< 1 second	223
7	heslo	10 seconds	192
8	12345678	< 1 second	189
9	password	< 1 second	188
10	000000	< 1 second	183

*Top 200 Most Common Passwords | NordPass

PROTECT

Riadenie prístupu - MFA

- Multifaktorová autentifikácia (Multi-Factor Authentication)
- Faktory:
  - „Niečo, čo som“ - biometria
  - „Niečo, čo mám“ – HW token
  - „Niečo, čo viem“ – heslá, PIN, OTP
  - Existuje rôzne silná „MFA“
- Príklady:
  - Heslo + PIN = Single Factor
  - Tvár + Počítač = MFA
  - Otlačok prsta + Mobil = MFA
  - Heslo = Single Factor
- Ako implementovať MFA:
  - Závisí od konkrétnej použitej technológie, napr. PHP, WordPress, ASP.NET, ...

PROTECT

Riadenie prístupu - Princíp minimálneho prístupu

1. Identifikácia potrieb
2. Vytvorenie rolí
   - Ochrana Admin účtov, napr. v M365 prostredí
3. Implementácia prístupových práv
4. Pravidelný audit
5. Vzdelávanie zamestnancov
6. Monitorovanie a reakcia

Povedomie a školenia

Otázka:

- Prihláste sa, kto ste za posledný rok absolvovali školenie o cybersecurity?

Vzdelávanie:

- Zdôrazňujte dôležitosť školenia o kybernetickej bezpečnosti. Naučte zamestnancov o phishingových podvodoch, silných heslách a bezpečných internetových praktikách.
- *Príklad:* "Krátke, pravidelné školenie je lepšie ako žiadne."

Vytvorte kultúru povedomia o bezpečnosti.

PROTECT

Povedomie a školenia

Útočníci zneužívajú:

- Vaše emócie: Strach, Eufória, Zvedavosť, „no nekúp to“
- Rôzne spôsoby doručenia:
  - SMS alebo chat správy
  - Emaily - Phishing testovanie - Jigsaw Phishing Quiz, Phishingový Online Test SAFELab
  - Nevyžiadané telefonáty - "We Are from Microsoft"

Užitočné nástroje:

- VirusTotal – Home, Windows Sandbox

PROTECT

PROTECT

Povedomie a školenia

Vzdelávanie

- Zdrojov je nepreberné množstvo:
  - hlavne v EN, napr. NIST
  - V SK napr. SAFELab alebo TATRA Banka
- Pre aké účely/role to potrebujete:
  - Administrátor
  - Bežný zamestnanec
  - Vrcholový manažment
  - Školenia na konkrétne situácie
- Metodický postup napr. Building a Cybersecurity and Privacy Learning Program od NIST

Zabezpečenie údajov

Ochrana vašich údajov:

- Šifrujte citlivé údaje (statické alebo v pohybe).
  - *Príklad:* "Najmä údaje o zákazníkoch a finančné záznamy."
- Používajte antivírusový a anti-malvérový softvér.
- (Bezpečne) sa zbavte toho, čo nepotrebujete

Účel:

- Chrániť dôvernosť, integritu a dostupnosť údajov

Otázky:

- Viete, čo všetko sa dá o Vás a o Vašej firme nájsť na webe?

Bezpečnosť platforiem

Hardvér, softvér (napr. firmvér, operačné systémy, aplikácie) a služby fyzických a virtuálnych platforiem sú spravované v súlade so stratégiou rizík organizácie na ochranu ich dôvernosti, integrity a dostupnosti. Súčasťou zabezpečenia platforiem sú nasledovné aktivity:

- Riadenie konfigurácie - CIS Benchmarks
- Manažment softvéru
- Manažment hardvéru
- Logging a monitoring
- Neautorizovaný SW/HW
- Bezpečný vývoj SW

PROTECT

Odolnosť technologickej infraštruktúry

Ochrana siete

Firewall

Bezplatné zabezpečenie Wi-Fi

- WEP, WPA1-3
- WPA EAP
- Otázka: Akú ochranu používate na firemnej sieti? AK WPA1-3, kedy ste naposledy menili heslo?
- Tipy pre pokročilých: Ako zabezpečiť a správne nastaviť Wi-Fi site

Bezpečné surfovanie po webe

Fyzická ochrana

- Fyzické zabezpečenie – zámky, mreže, investujte podľa výšky rizika/hodnoty majetku
- Požiare/záplavy/dažde a iné environmentálne riziká
- Umiestnenie zariadení v budove na rôznych poschodiach

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

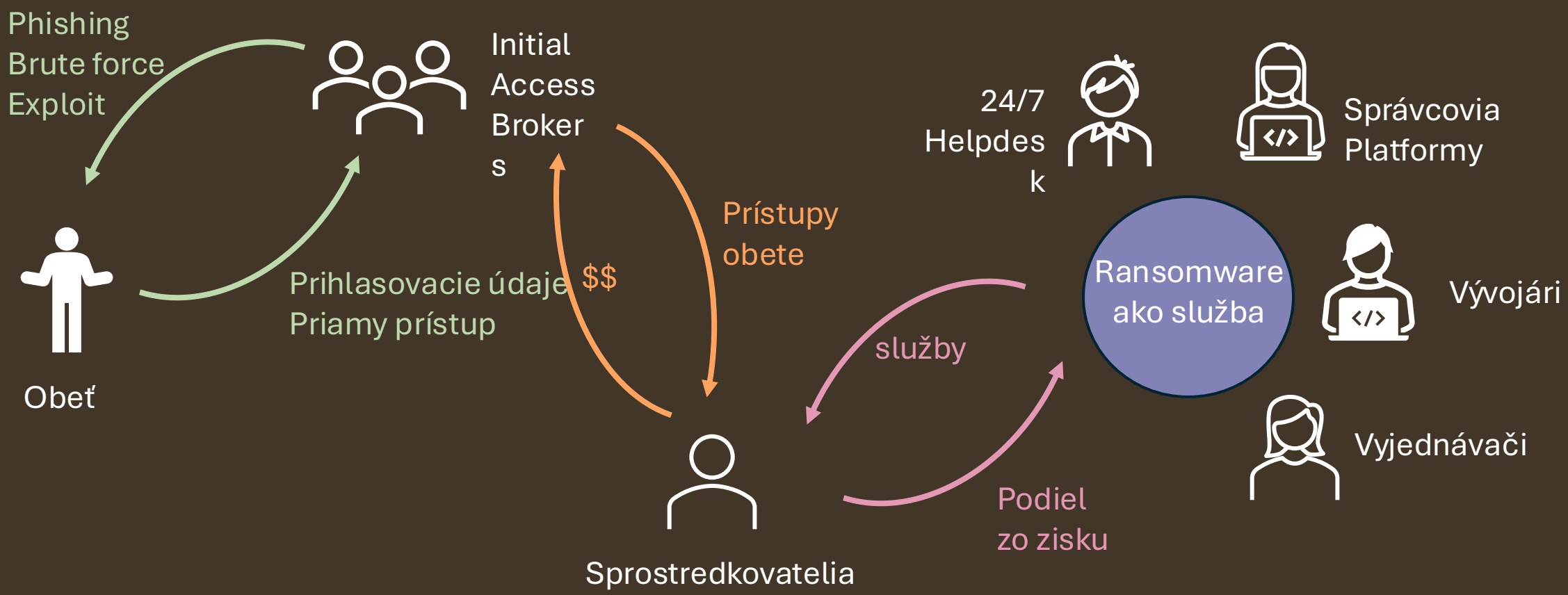
Zhrnutie

- Pochopiť
- Posúdiť
- Prioritizovať
- Komunikovať

P R O T E C T

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Zločinecký “ekosystém” ’25



AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

DETECT

Aby ste dokázali **nájsť a odhaliť možné kybernetické útoky**

DETECT

Aby ste dokázali nájsť a odhaliť možné kybernetické útoky

Čo potrebujeme detegovať?
Udalosti a anomálie

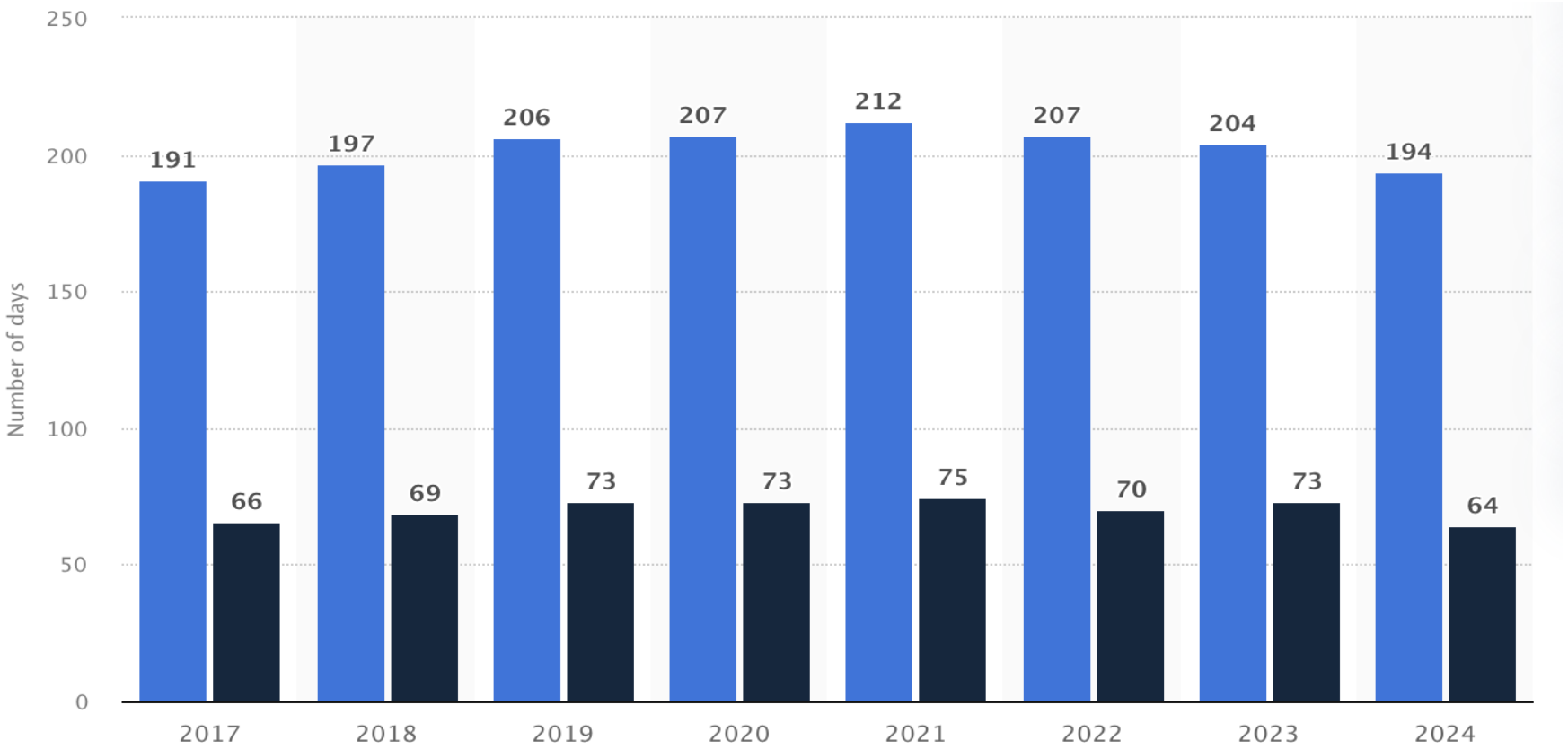
Prečo?
Incidentom nie je možné sa úplne vyhnúť
Skoré odhalenie pomôže minimalizovať škody

Ako?
Manuálne aj automaticky

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

DETECT

PREČO



Stredný čas, ktorý trvalo obetiam

Identifikovať narušenie

Obmedziť dopad narušenia

https://www.statista.com/statistics/1417455/worldwide-data-breaches-identify-and-contain

DETECT

ČO MÔŽE BYŤ ZNAKOM ZAČÍNAJÚCEHO ALEBO PREBIEHAJÚCEHO KYBER-ÚTOKU?

UDALOSTI, ANOMÁLIE A ZRANITEĽNOSTI

Napríklad:

- Opakované (neúspešné) pokusy o prihlásenie
- Spomalená sieť, systémy, aplikácie
- Strata prístupu k dátam či aplikáciám
- Upozornenia bezpečnostných aplikácií (napr. antivírus)
- Podozrivé emaily a notifikácie
- Netypické aktivity (prihlásenia z “exotických“ krajín)
- Známe zraniteľnosti

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

DETECT

Aby ste dokázali nájsť
a odhaliť možné kybernetické útoky

manuálne + automaticky

DETECT

Manuálna detekcia

- Definujte ”normál”
- Pravidelné kontroly (logy, účty…)
- Čítanie notifikácií
- Zvyšovanie povedomia užívateľov
  - Pravidelne vzdelávajte o hrozbách
  - Podporujte zdravú opatrnosť
  - Nebáť sa ohlásiť
  - Testujte

DETECT

Automatická detekcia – nepretržitý monitoring (DE.CM)

- 24/7 dohľad s využitím:
  - Antivírus, Antimalware, EDR
  - Sieťového IDS (open-source napr. Snort, Suricata)
  - Host IDS (OSSEC, Wazuh)
  - SIEM (Elastic, Wazuh)
  - Cloud nástrojov (v M365, AWS a pod.)
- Ak nie interne, zvážte poskytovateľov služieb SOC

DETECT

Aby ste dokázali nájsť a odhaliť možné kybernetické útoky

Čo potrebujeme detegovať?
Udalosti a anomálie

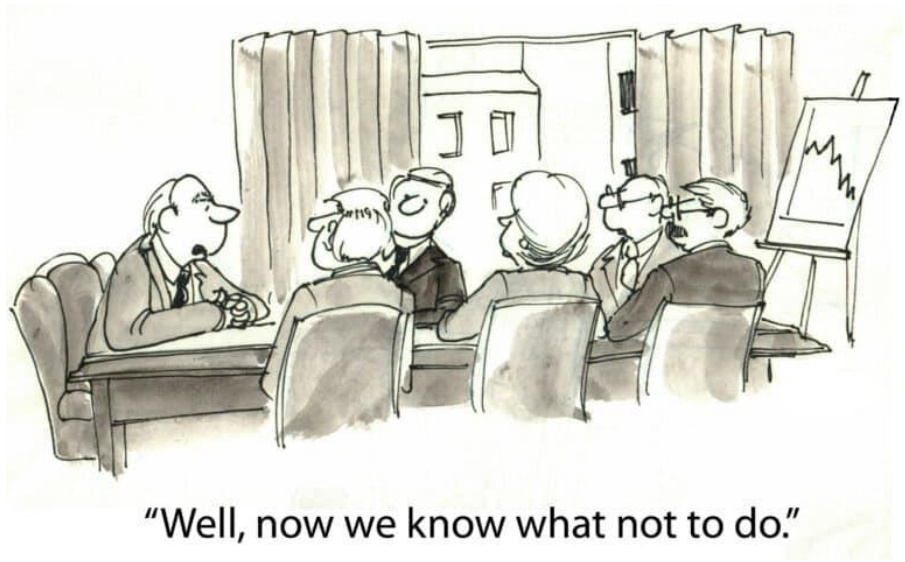
Prečo?
Incidentom nie je možné sa úplne vyhnúť
Skoré odhalenie pomôže minimalizovať škody

Ako?
Manuálne aj automaticky

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

Ako správne reagovať na kybernetické incidenty

RESPOND



RESPOND

Ako správne reagovať na kybernetické incidenty

- Reakcia na zistené incidenty a obmedzenie ich dopadu
- Fázy: Identifikácia, obmedzenie škôd, odstránenie a obnova

RESPOND

Incident Response Plan

- Písomný plán s jasne definovanými postupmi a rolami
- Typicky:
  - Príprava: Nástroje, kontakty, komunikačné kanály
  - Identifikácia: Kritériá pre určenie incidentu (závažnosť)
  - Obmedzenie a odstránenie hrozieb: Okamžité kroky pre minimalizáciu škôd
  - Obnova: Postupy pre návrat do normálneho stavu a overenie bezpečnosti
  - Poučenie: Analýza a zlepšenie po incidente

RESPOND

Komunikácia

- **Interná**
  - Kto a ako (kadiaľ) bude komunikovať so zamestnancami? (sms, telefón)
  - Vedenie
- **Externá**
  - Informovanie médií a príslušných orgánov (OČTK, NBÚ, ÚOOÚ, atď.)
  - Klienti, dodávatelia, partneri
  - Poskytovatelia služieb
- **Krízová komunikácia**
  - Určite hovorcu / eskalačné cesty
  - Čo budeme komunikovať?
  - Predpripravte si “šablóny”
  - Zoznamy kontaktov, adries, čísiel a pod.

RESPOND

Tipy pre Vás

- Určite, kto bude mať aktualizovaný IRP na starosti
- Spíšte, kto je súčasťou plánu, ich kontakty a zodpovednosti
- Aké máte povinnosti zo zákona, materskej firmy a pod.
- Platí aj pre funkciu Recover
- Zorganizujte cvičenie
  - "Zahrajte" sa s kľúčovými ľuďmi na incident
  - Overte si ich správanie
  - Aktualizujte plán podľa zistení

Contact	Phone
Business Leader:	
Technical Contact:	
State Police:	
Legal:	
Bank:	
Insurance:	

RESPOND

Bezplatné zdroje

Incident Response Plan Basics

https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Stop Ransomware návod

https://www.cisa.gov/resources-tools/resources/stopransomware-guide

Incident Response Plan

ACSC Emergency Response Guide

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

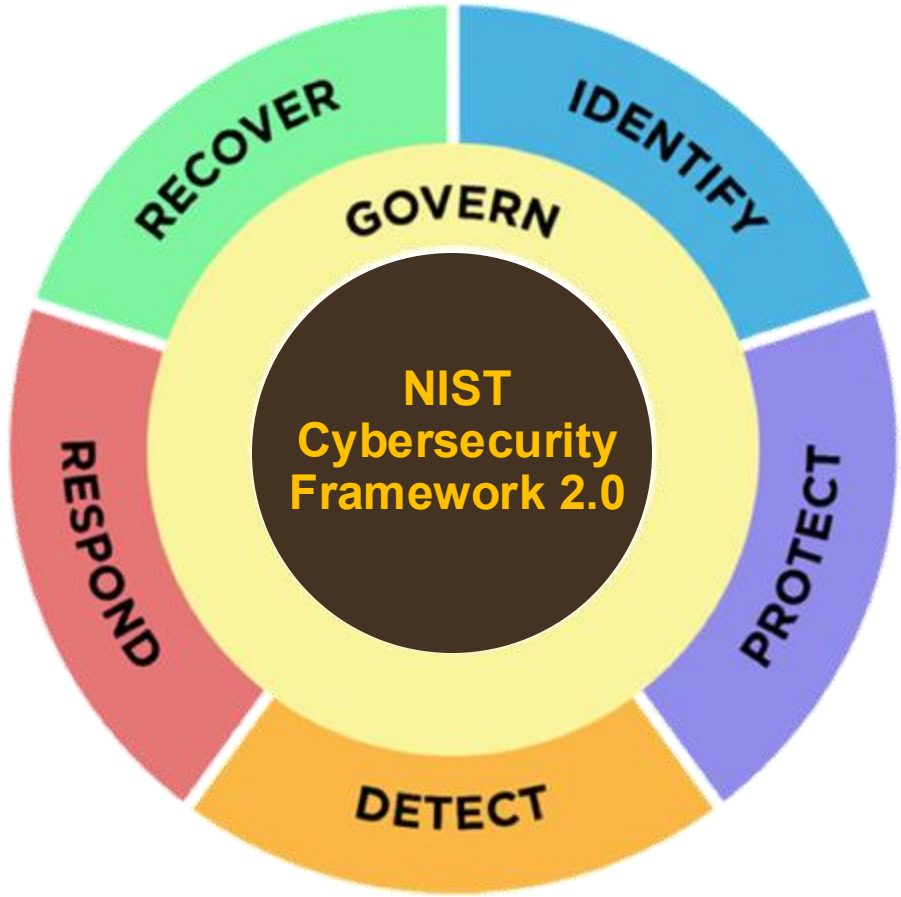
AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

RECOVER

Funkcia **RECOVER** nám slúži na to, aby sme sa dokázali zotaviť z kybernetického incidentu

- Logicky nasleduje po fáze RESPOND, v ktorej na kybernetický incident reagujeme
- Cieľ: celá funkcia RECOVER nám má pomôcť vrátiť sa do normálu
- Výstup: pripravený plán obnovy – ktoré systémy obnovovať v akom poradí, s kým komunikovať, akým spôsobom

Aby sme boli schopní efektívne obnovovať svoje služby, musíme mať vopred pripravený plán, s ktorým budeme následne pracovať.



AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

RECOVER

Na čo myslieť pri zálohách:

- Pravidelne zálohujte svoje údaje
- Svoje zálohy si testujte – ako dlho vám trvá obnova?
- Pravidlo zálohovania 3-2-1: 3 kópie vašich údajov na 2 rôznych médiách s 1 kópiou mimo pracoviska
- RTO – aký bude finančný a nefinančný dopad, ak budú dáta istý čas nedostupné?
- RPO – aký bude finančný a nefinančný dopad, ak dôjde k strate dát za isté obdobie?

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

RECOVER

Kedy máme začať s obnovou?

- Je to na našom rozhodnutí
- Z fázy RESPOND musíme byť schopní prejsť plynule do fázy RECOVER – môže to byť ešte počas incidentu, alebo až po jeho úplnom vyriešení
- Zvyčajne sa to robí vtedy, keď je to bezpečné

Ktoré systémy majú pri obnove prioritu

- Potrebujeme vedieť, ktoré systémy či služby majú pre nás prioritu
- Aké sú závislosti medzi našimi systémami?
- Na základe toho dokážeme plánovať a alokovať zdroje
- Potrebujeme najskôr sfunkčniť náš web alebo databázu, ktorú používame pri procesovaní transakcií?
- Cieľom je minimalizovať dopad na našu spoločnosť

RECOVER

Zistite či neboli zasiahnuté zálohy, z ktorých budete obnovovať

- Predtým, ako začnete obnovovať zo záloh, si musíte overiť či neboli kompromitované
- Aktualizácia, záplatovanie, AV – odstrániť zraniteľnosti a overiť prítomnosť hrozby
- V opačnom prípade ste tam, kde ste boli
- Celý proces obnovy potrebujete dokumentovať
- Všetko, čo sa počas tohto procesu udeje, je lesson learned – viete sa z toho poučiť a upraviť to, čo nefungovalo
- Backup and Recovery technológie
  - https://www.bacula.org/
  - https://www.bareos.com/

RECOVER

Záverečné tipy, ako si nastaviť svoj plán obnovy:

- Súbor formálnych procesov
- Dokumentácia kritickosti systémov - dokumentácia systémov, ktoré spracúvajú a uchovávajú kľúčové aktíva
- Zoznam pracovníkov, ktorí budú zodpovední za definovanie a implementáciu plánov obnovy
- Komplexný komunikačný plán obnovy

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

POZVÁNKA

AmCham Slovakia

AKO OCHRÁNIŤ FIRMU V ROKU 2025 S MINIMÁLNYM ROZPOČTOM?

ZÁKLADY KYBERNETICKEJ BEZPEČNOSTI PRE MALÉ A STREDNÉ PODNIKY