Kybernetická bezpečnosť

Miroslav Hájek

Obsah

V čom spočíva kyberbezpečnosť?

- **Úlohy:** ochrana informačných systémov pred ukradnutím, zničením, ohrozením majetku
- Systémy, ľudia, aktíva, údaje a schopnosti
- **Kyberpriestor** – doména digitálnych vecí / internet
  - Závislosť od digitálneho priestoru = kybernetické útoky môžu spôsobiť značné škody
- Nevyhnutná v znalostnej spoločnosti

Riadenie rizík kybernetickej bezpečnosti

- Malé podniky môže vyradiť jediný útok!
- Rámec kybernetickej bezpečnosti Národného inštitútu pre štandardy a technológie (NIST)
  1. **Ochrana** (Prevencia)
  2. **Detekcia**
  3. **Reakcia**
  4. **Obnova**

- **Odstránenie následkov útoku**
  1. odrazenie útok
  2. obnovenie postihnutých systémov
  3. zotavenie sa z incidentu

Aké aktíva chránime?

- **CIA triáda bezpečnosti**
  - Dôvernosť
  - Integrita
  - Dostupnosť
- **CIAAA**
  - Zodpovednosť (Accountability)
  - Audit

Kyberbezpečnosť podľa sektorov hospodárstva

Najlepšie sektory

1. Plynárenstvo
2. Bankovníctvo
3. Elektronické komunikácie

Najhoršie sektory

1. Teplárenstvo
2. Verejná správa
3. Doprava

Správe o kybernetickej bezpečnosti za rok 2022
Národný bezpečnostný úrad

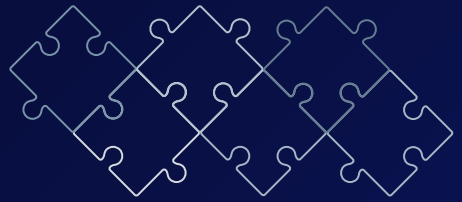
Ako vnímajú firmy kyberbezpečnosť?

- Malé a stredné podniky **podceňujú svoju atraktivitu** pre útočníkov
  - Presvedčenie, že nie sú zaujímavým cieľom

- **Vzdelávanie** má byť určené všetkým zamestnancom využívajúcich IT.
  - Štatutári organizácií - akoby ich bezpečnosť doslova obťažovala

- Kybernetická bezpečnosť sa stala zaujímavou **obchodnou komoditou**
  - Zakúpenie zbytočnej služby zvyšuje nechuť riešiť kyberbezpečnosť

Výzvy pre firmy



Prečo je silná kybernetická bezpečnosť rozhodujúca pre úspech firiem?

- Životná závislosť podnikov od technológií
- Dáta sú jedným z najcennejších aktív
- Malvér vytváraný rýchlejšie a ťažšie odhaliteľný
- Regulácie pre štandardy kybernetickej bezpečnosti
- Očakávania od spotrebiteľov a partnerov na ochranu dát

Benefity pre firmy

Kyberbezpečnosť prispieva ku kľúčovým obchodným prioritám:

- dôvera zákazníkov
- reputácia značky
- prevádzková stabilita

Program kybernetickej bezpečnosti ako:

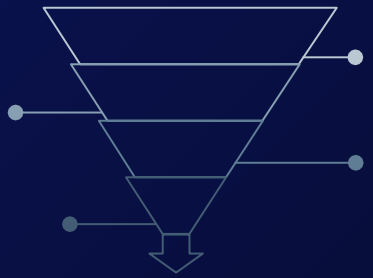
- prostriedok na umožnenie chodu biznisu
- nielen ako prostriedok na predchádzanie stratám

★ ★ ★ ★ ☆

Hrozby pre firmy

Straty

- Finančné
- Dôvery a reputácie
- Duševného vlastníctva



Následky

- Zníženie produktivity
- Právne následky: zákony a zmluvné záväzky
- Riziká národnej bezpečnosti: kritická infraštruktúra
- Psychické a emocionálne následky

Najbežnejšie hrozby

- Sociálne inžinierstvo
- Ransomvér
- Malvér
- Trojské kone

- Phishing
- Spam
- Cookie sledovanie
- Krádež identity

Kritické výzvy informačnej bezpečnosti

EY Global Information Security Survey 2021 *(Ernest and Young, 1400 resp.)*

- **Výrazná podfinancovanosť kybernetickej bezpečnosti**
  - 2 až 5 % ročných príjmov firmy
  - 36 % - očakáva, že utrpí útok, ktorému by sa predišlo investíciami
- **Fragmentácia regulácií**
  - 49 % - dodržiavanie predpisov je najstresujúcejšie
  - Očakáva sa väčšia fragmentácia
- **Vzťahy CISO vo firmách sú slabé**
  - 44 % - problém s potrebou komerčných konzultácií
  - 29 % - vie kvantifikovať efektívnosť výdavkov

Rýchly nástup nových technológií

Reakcia

- 77 % - nárast počtu rušivých útokov. (z 59 % na 77 %)
- 43 % - sa viac obáva o schopnosť firmy zvládať kybernetické hrozby
- 56 % - nevie dostatočnú silu obranu pre nové stratégie hackerov

Prevencia

- Board má kyberbezpečnosť na programe aspoň štvrťročne: z 29% na 39% (2020 - 2021)
- 58 % - časové plány sú príliš krátke na hodnotenie kyberbezpečnosti

Následky útokov celosvetovo (1)

Bezpečnostná správa Fortinet

- 78 % s prevádzkou technológií - aspoň 3 útoky / 12 mesiacov
- 2021 - 64 incidentov v priemysle
  - 22 - kyberútoky so fyzickými následkami
  - 144-% medziročný nárast

IBM "Cost of a Data Breach Report 2023"

- náklady na porušenie ochrany údajov,
- 553 organizácií, 4,45 milióna dolárov
- 2% v 2022 nárast oproti 2021
- 15% nárast oproti úrovni z roku 2020

Následky útokov celosvetovo (2)

- **Prieskum digitálnej dôvery PwC:**
  - náklady na kybernetický útok: 4,4 milióna dolárov,
  - 36 % respondentov - únik údajov - 1 milión dolárov / 3 roky

- **The State of Ransomware 2023** (Sophos, 3000 resp.)
  - Výkupné: 1,54 milióna dolárov / 12 mesiacov .
  - Celosvetové náklady na počítačovú kriminalitu
    - 2023: 8,15 bilióna dolárov
    - 2028: 13,82 bilióna dolárov

Následky podľa skutočných príbehov

- **Ransomvér Black Basta**
  - energetický konglomerát Hitachi Energy (ABB)
- **Ransomvér, Colonial Pipeline,** 2021
  - výpadky dodávok plynu
  - 4,4 milióna $
- **Ransomvér, MGM Resorts,** 2023,
  - prerušenie služieb a krádež osobných údajov
  - 100 miliónov $
- **Malvér, AP Moller-Maersk**, 2017,
  - vypol SW na prepravných termináloch celosvetovo
  - 300 miliónov $

Osobná kyberbezpečnosť - Hrozby

- Kyberútoky
- Scamy
- Online stalking
- Kyberšikana

- **Osobné údaje**
  - Krádež idenity: podvodné transakcie
  - Strata prístupu do online účtov
  - Cielená reklama

Zber informácií a špehovanie všetkých (Ed Snowden)

Osobná kyberbezpečnosť – Čo chrániť?

“Nemám čo skrývať“

Aké údaje si treba chrániť a prečo na tom záleží?

- Navštívené webstránky

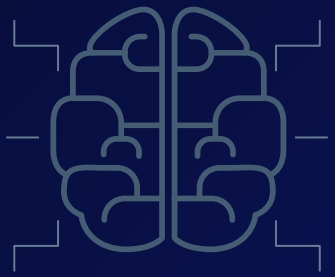
- Správy a obsah emailov: cesta k ostatným účtom

- Telefónne číslo

- Online nákupy: hlavne pri zadávaní karty

- Zdravotné údaje a DNA

Otázky do diskusie



1. Myslíte si, že sa dá vyhnúť v dnešnej dobe kyberútokom?
2. Kde kladiete osobný najväčší dôraz pri vašej osobnej kybernetickej bezpečnosti?
3. Ako by ste presvedčili kolegov, že zavedené kyberbezpečnostné pravidlá nie sú len na zbytočné skomplikovanie ich práce?

Zdroje

1) Miroslav Lukáč; Čo je kybernetická bezpečnosť a prečo sa o nej toľko hovorí?; 2019; https://www.bezpecnostvpraxi.sk/clanok-z-titulky/co-je-kyberneticka-bezpecnost-a-preco-sa-o-nej-tolko-hovori.htm
2) Povedzme si pravdu: Tu máme problém v oblasti kyberbezpečnosti; 2023; https://zive.aktuality.sk/clanok/3A6V5Sz/povedzme-si-pravdu-tu-mame-problem-v-oblasti-kyberbezpecnosti/
3) Zdvorilé mlčanie? To bezpečnosť vo výrobných linkách nezlepší; 2023; https://hnonline.sk/hn-special/96085155-zdvorile-mlcanie-to-bezpecnost-vo-vyrobnych-linkach-nezlepsi
4) Stanislav Smolár; Je nevyhnutné, aby Slovensko začalo hneď investovať do industriálnej bezpečnosti; 2023; https://hnonline.sk/hn-special/96085166-je-nevyhnutne-aby-slovensko-zacalo-hned-investovat-do-industrialnej-bezpecnosti
5) Quensland Goverment; Cyber security – protect your online business activity; 2022; https://www.business.qld.gov.au/running-business/digital-business/online-risk-security/cyber-security
6) Federal Communications Commision; Cybersecurity for Small Businesses; 2024; https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses
7) Steve Ursillo, Jr., Christopher Arnold; Cybersecurity Is Critical for all Organizations; 2023; https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small
8) Kala, E. (2023) The Impact of Cyber Security on Business: How to Protect Your Business. *Open Journal of Safety Science and Technology*, 13, 51-65. doi: 10.4236/ojsst.2023.132003.; https://www.scirp.org/journal/paperinformation?paperid=126109
9) Mary K. Pratt, Why effective cybersecurity is important for businesses; 2024; https://www.techtarget.com/searchsecurity/feature/Why-effective-cybersecurity-is-important-for-businesses
10) Charlie Osborne; Cybersecurity 101: Everything on how to protect your privacy and stay safe online; 2023; https://www.zdnet.com/article/cybersecurity-101-everything-on-how-to-protect-your-privacy-and-stay-safe-online/
11) EY Global Information Security Survey 2021; 2021; https://assets.ey.com/content/dam/ey-sites/ey-com/en_tn/giss/ey-giss-2021-insights-deck.pdf