Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy KB hrozieb a útokov

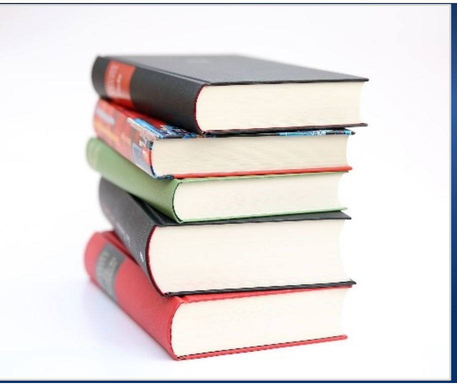
Bezpečnostné riziká, opatrenia a prevencia (Blok II)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

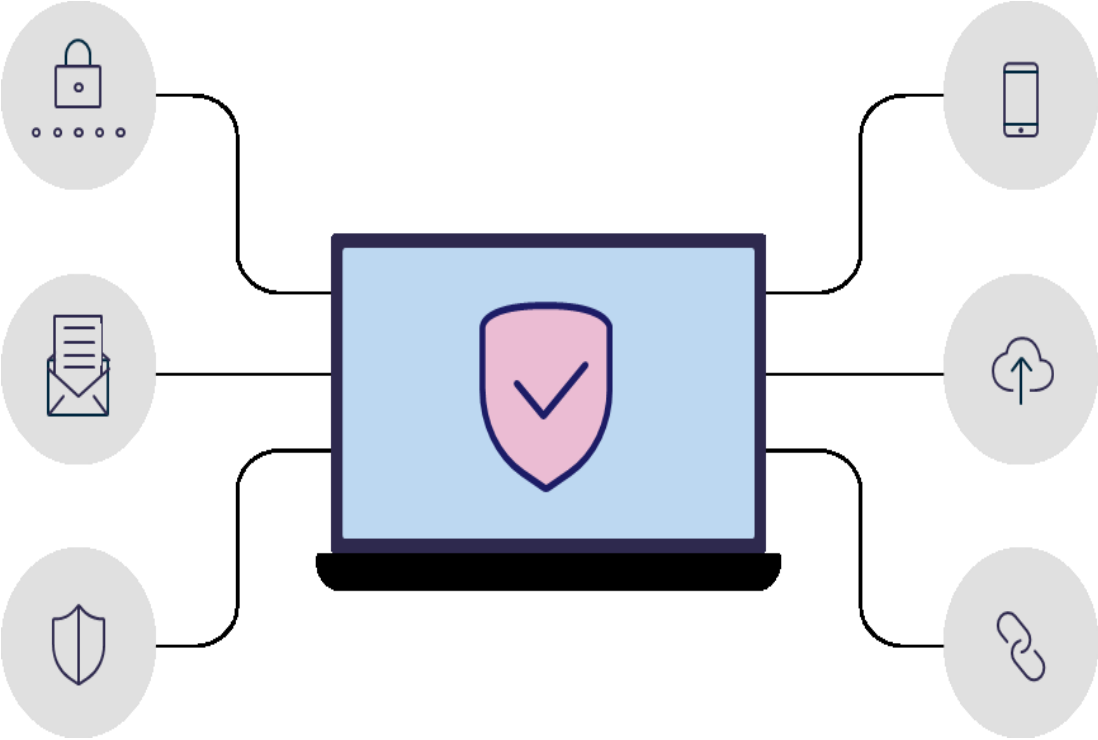
Ing. Nikola Štaffenová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

nikola.staffenova@fri.uniza.sk



Čo sa dozviete?



Zdroje a kategórie hrozieb
Pôvod, dopad fyzického prostredia, ľudské hrozby

Typy KB hrozieb
Malware, phishing, spam, DoS, DDoS, krádež identity, sieťové útoky

Vysvetlenie hrozieb v doménach KB
Ochrana sietí, údajov, aplikácií, správa identít a prístupov, reakcia na incidenty

ISO 27005
Zameranie na hrozby spôsobené zamestnancom

Základ
Stručný základ, detaily v ďalších kurzoch

Domény KB
Zameranie na najdôležitejšie domény

Absolvovali ste už v minulosti kurz alebo školenie v oblasti kybernetickej bezpečnosti?

01

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb

Informačná, kybernetická a fyzická bezpečnosť

1 INOFORMAČNÁ

- **Uchovávanie dôvernosti, integrity a dostupnosti informácií**
- Prístup k ochrane informácií
- Disciplína, ktorá využíva metódy z: Informatiky, manažmentu, práva, psychológie a softvérového inžinierstva
- Informácie – základný prvok

2 KYBERNETICKÁ

- Súbor technických, právnych, organizačných a vzdelávacích prostriedkov
- **Zaistenie ochrany kybernetického priestoru**
- Procesy, postupy, technologické riešenia na ochranu kritických systémov pred digitálnymi útokmi
- Ľudia, procesy, technologické riešenia

3 FYZICKÁ

- **Fyzické zabezpečenie podniku pred hrozbami**
  - Fyzická ochrana, mechanické zábrany, technické prostriedky, režimové opatrenia
  - Typ opatrenia – na základe vyhodnotenia rizík (vstupné karty, heslá, biometria...)
- Ochrana pred neoprávneným vstupom, prírodnými živlami...

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Informačná vs. kybernetická bezpečnosť

1 INOFORMAČNÁ

- Zabezpečuje prístup k údajom
- **Ochrana údajov pred akýmikoľvek formami hrozieb**
- Pre **informácie z akejkoľvek oblasti**
- Rieši neopravené prístupy, neoprávnenú úpravu informácií, ich zverejnenie a narušenie
- Zasahuje, keď je narušená bezpečnosť
- **Širšia škála hrozieb,** fyzické hrozby (krádeže), špionáže, ľudské chyby
- Využíva šifrovanie, riadenie prístupov, nástroje na predchádzanie state údajov
- **Ochrana informačných aktív,** údajov, informácií (duševné vlastníctvo, obchodné tajomstvá, dôverné a osobné údaje)
- Široká škála hrozieb, narušenie fyzickej bezpečnosti, vnútorné hrozby

2 KYBERNETICKÁ

- Chráni kybernetický priestor pred útokmi
- Pre **čokoľvek v kybernetickej oblasti**
- Rieši **kybernetické zločiny,** kybernetické podvody a kybernetické útoky
- Rieši hrozby, ktoré môžu, ale nemusia vzniknúť v kybernetickom priestore
- Prvá línia ochrany
- Predovšetkým **kybernetické hrozby**
- Využíva rôzne technológie, firewall, antivírusový SW
- **Ochrana údajov bez ohľadu na to, akým spôsobom sa prenášajú, alebo kde sú uložené**
- Neustále vyvíjajúce sa hrozby, nový malvér, nové techniky kybernetických útokov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Informačná vs. kybernetická bezpečnosť

1 INOFORMAČNÁ

2 KYBERNETICKÁ

Bezpečnosť všetkých typov informácií
(elektronická aj papierová forma)

Bezpečnosť výlučne v kybernetickom priestore
(len elektronická forma)

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – pôvod hrozieb

1 ÚMYSELNÉ

- Môžu mať za následok poškodenie alebo stratu základných služieb
- Označenie **D**

2 NEÚMYSELNÉ

- Používajú sa pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť informačné aktíva
- Označenie **A**

3 ENVIRONMENTÁLNE

- Používajú sa pre všetky incidenty, ktoré nie sú založené na ľudskej činnosti
- Označenie **E**

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – pôvod hrozieb

4 ĽUDSKÉ

- Všetko, čo môžu spôsobiť ľudia svojim správaním a konaním a ohrozuje to bezpečnosť

Za všetkým treba hľadať ľudí!

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – pôvod hrozieb

Fyzická škoda	Požiar, poškodenie vodou, znečistenie, väčšia nehoda, zničenie zariadenia alebo médií, prach, korózia, zamrznutie	**A, D, E**
Prírodné udalosti	Klimatické javy, seizmické javy, vulkanické javy, meteorologické javy, záplavy	**E**
Strata základných služieb	Zlyhanie klimatizácie alebo dodávky vody, strata dodávky elektrickej energie **(+E)**, zlyhanie telekomunikačného zariadenia	**A, D**
Porucha vplyvom radiácie	Elektromagnetické žiarenie, tepelné žiarenie, elektromagnetické impulzy	**A, D, E**
Technické zlyhanie	Zlyhanie zariadenia, nefunkčnosť zariadenia, preplnenie IS **(+D)**, nefunkčnosť SW, prelomenie udržateľnosti IS **(+D)**	**A**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – pôvod hrozieb

Ohrozenie informácií	Zachytenie rušivých ohrozujúcich signálov, diaľková špionáž, odpočúvanie, krádež médií alebo dokumentov, krádež zariadenia, znovuzískanie recyklovaných alebo vyhodených médií, odhalenie **(+A)**, dáta z nedôveryhodného zdroja **(+A)**, manipulovanie s HW, manipulovanie so SW **(+A)**, detekcia polohy	**D**
Neoprávnené činnosti	Neoprávnené použitie zariadenia, podvodné kopírovanie SW, použitie falšovaného alebo kopírovaného SW **(+A)**, poškodenie dát, nezákonné spracovanie dát	**D**
Ohrozenie funkcií	Chyba pri použití **(+A)**, zneužitie práv **(+A)**, falšovanie práv, odmietnutie činností, prelomenie osobnej dostupnosti **(+A,E)**	**D**

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – pôvod hrozieb

Ktoré z uvedených kategórií hrozieb vznikli dôsledkom ľudského faktora?

Spôsobili ste Vy alebo niekto z Vášho okolia niektorú z typov hrozieb?

- Fyzická škoda
- Technické zlyhanie
- Prírodné udalosti
- Ohrozenie informácií
- Strata základných služieb
- Neoprávnené činnosti
- Porucha vplyvom radiácie
- Ohrozenie funkcií

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – dopad fyzického prostredia na KB

- Označuje **všetky materiálne a vonkajšie faktory,** ktoré môžu ovplyvniť bezpečnosť IS
- Zameriava sa na fyzické zariadenia, infraštruktúru a priestor, kde sa tieto systémy nachádzajú

Fyzická bezpečnosť priestorov

Napr. budovy, miestnosti alebo dátové centrá, kde sú uložené servery a ďalšie technológie. Priestory musia byť zabezpečené pred **neoprávneným prístupom, vandalizmom alebo krádežou.**

Environmentálne faktory

Napr. teplota, vlhkosť, prach, svetlo alebo elektromagnetické rušenie, ktoré môžu **ovplyvniť výkon a životnosť hardvéru.**

Energetická infraštruktúra

Napr. **stabilita napájania** (napr. výpadky elektriny), **záložné zdroje energie** (UPS systémy) a klimatizácia, ktoré chránia zariadenia pred **prehriatím.**

Fyzické bezpečnostné opatrenia

Napr. zámky, bezpečnostné kamery, elektronické čítačky prístupových kariet alebo biometrické overenie, ktoré zabezpečujú ochranu zariadení pred **neoprávneným prístupom.**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – dopad fyzického prostredia na KB

Poškodenie zariadení a dátovej infraštruktúry

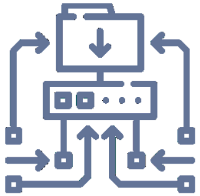
Prírodné katastrofy (zemetrasenie, povodne, búrky, požiare), ale aj **fyzické poškodenie** (vandalizmus, krádež) môže viesť k zničeniu alebo odcudzeniu HW.

Neoprávnený prístup k zariadeniam

Nedostatočná fyzická bezpečnosť priestorov môže spôsobiť prístup neautorizovaných osôb k citlivým dátam alebo zariadeniam.

Výpadky a poruchy infraštruktúry

Absencia záložných systémov (napájanie) môže pri výpadkoch poškodiť systémy. **Teplota a vlhkosť v miestnostiach** (chladenie a klimatizácia) ovplyvňuje životnosť zariadení.



Firemná kultúra a školenia

Nedostatočne školení zamestnanci môžu ľahko, rýchlo a jednoducho spôsobiť bezpečnostné incidenty (najmä tie neúmyselné).

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – ľudské hrozby

Ľudské hrozby

Riziká spojené s ľudským faktorom, ktoré môžu **ohroziť bezpečnosť informačných systémov a dát.** Tieto hrozby môžu byť spôsobené neúmyselnými chybami, nedostatočným školením alebo úmyselnými škodlivými činmi zamestnancov, dodávateľov alebo iných osôb s prístupom k citlivým informáciám.

Personálna bezpečnosť

Súbor procesov, ktorých zámerom je **minimalizovať riziko zneužitia prístupu k informačným prostriedkom** organizácie **zo strany** jej **zamestnancov** alebo kontrahujúcich strán na účely, ktoré sú **v rozpore s bezpečnostnou stratégiou organizácie.**

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – ľudské hrozby

Hacker	Výzva, ego, revolta, stav, peniaze	Hacking, sociálne inžinierstvo, zasahovanie do systému a jeho prelomenie, neoprávnený prístup k systému
Počítačový zločinec	Zničenie informácií, nezákonné prezradenie informácií, peniaze, neoprávnená zmena dát	Kybernetické sledovanie, podvod, informačná korupcia, falšovanie, zasahovanie do systému
Terorista	Vydieranie, zničenie, zneužitie, pomstychtivosť, politický zisk, reportáž	Bomba/terorizmus, informačná vojna, systémový útok (DoS, DDoS), preniknutie do systému, manipulácia so systémom
Priemyselná špionáž	Konkurenčná výhoda, hospodárska špionáž	Obranná výhoda, politická výhoda, hospodárske zneužitie, krádež informácií, zasahovanie do osob. súkromia, sociálne inžinierstvo, preniknutie do systému, neoprávnený prístup

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zdroje a kategórie kyberneticko-bezpečnostných hrozieb – ľudské hrozby

Osoba, ktorá sa vyzná

Kuriozita, ego, tajná služba, peniaze, pomsta, nezámerné chyby a vynechávanie (programovacia chyba, chybný vstup dát)

Napadnutie zamestnanca, vydieranie, zneužitie počítača, podvod a krádež, informačná korupcia, vstup falšovaných a narušených dát, škodlivý kód (vírus, logická bomba, trojský kôň), predaj osobných informácií, programové chyby systému, narušenie a sabotáž systému, neoprávnený prístup do systému

Ako predísť uvedeným hrozbám?

- Zvýšiť informovanosť o hrozbách
- Poskytnúť zamestnancom školenia
- Rozumne prideľovať práva, právomoci
- Zvýšiť a zlepšiť úroveň kontrol...

02

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – malware

MALWARE

malicious + software = MALWARE

- Škodlivý softvér
- **Zastrešujúci pojem pre všetky formy škodlivého softvéru/kódu** bez ohľadu na spôsob, akým postihuje obete, ako sa správe, alebo aké škody spôsobuje
- **Šíri sa prostredníctvom bezpečnostných zraniteľností** v systémoch, na ktorých neboli nainštalované potrebné záplaty či aktualizácie, obchádzajú bezpečnostné opatrenia, ukrývajú sa v pamäti alebo napodobňujú legitímne aplikácie s cieľom vyhnúť sa odhaleniu

Ochrana:

- Inštalácia antivírusového programu
- Implementácia rozšírenej ochrany e-mailov a koncových zariadení (skenovanie príloh v e-maile – MS Defender)
- Cloudové zálohy
- Offline zálohy
- Pravidelné aktualizácie zariadenia
- Pravidelné školenia

Viac v extra bloku VIII

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – malware

Základné typy malware:

- **Vírusy =** zásah do normálnej prevádzky zariadenia zaznamenaním, poškodením alebo odstránením údajov
- **Spyware =** nainštaluje sa **do zariadenia bez súhlasu danej osoby** a môže monitorovať správanie online, zhromažďovať citlivé informácie, meniť nastavenia zariadenia a znižovať výkon zariadenia
- **Adware =** nainštaluje sa do zariadenia bez súhlasu danej osoby, ale jeho cieľom je **zobrazovanie agresívnej reklamy,** často vo forme kontextovej ponuky, a získavanie peňazí za kliknutia
- **Ransomware =** po nainštalovaní do zariadenia **sa obeti vyhráža,** že jej zničí alebo zablokuje prístup ku kritickým údajom alebo systémom, kým nezaplatí výkupné
- **Rootkity = skrýva sa v systéme** tak, aby umožnil neautorizovaný prístup k počítačovým alebo sieťovým systémom bez toho, aby bol detekovaný
- **Trójske kone =** spoliehajú sa na to, že si ich používateľ stiahne nevedomky, pretože **sa tvária ako legitímne súbory** alebo aplikácie (stiahnuť ďalší vírus, odosielať informácie z PC, použiť PC na podvod...)
- **Červy =** väčšinou **sa nachádza v e-mailových prílohách,** textových správach, či sociálnych sieťach a v závislosti od typu môžu kradnúť citlivé informácie, meniť nastavenia zabezpečenia alebo vám zabrániť v prístupe k súborom

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – phishing

PHISHING

- Forma útoku s využitím metód tzv. sociálneho inžinierstva, pri ktorom **sa zločinec vydáva za dôveryhodnú osobu** alebo inštitúciu **s cieľom získať od obete citlivé informácie**

Ako ho odhaliť?

- Všeobecné alebo neformálne oslovenia
- Žiadosť o osobné informácie
- Slabá jazyková úroveň
- Neočakávaná korešpondencia
- Pocit naliehavosti
- Ponuka, ktorá sa nedá odmietnuť
- Podozrivá doména

Ochrana:

- Zvýšiť svoju informovanosť o phishingových technikách
- Byť obozretný pri poskytovaní osobných údajov
- 2-krát si premyslieť kliknutie na odkaz
- Pravidelne kontrolovať online účty
- Používať antivírusové programy

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – phishing

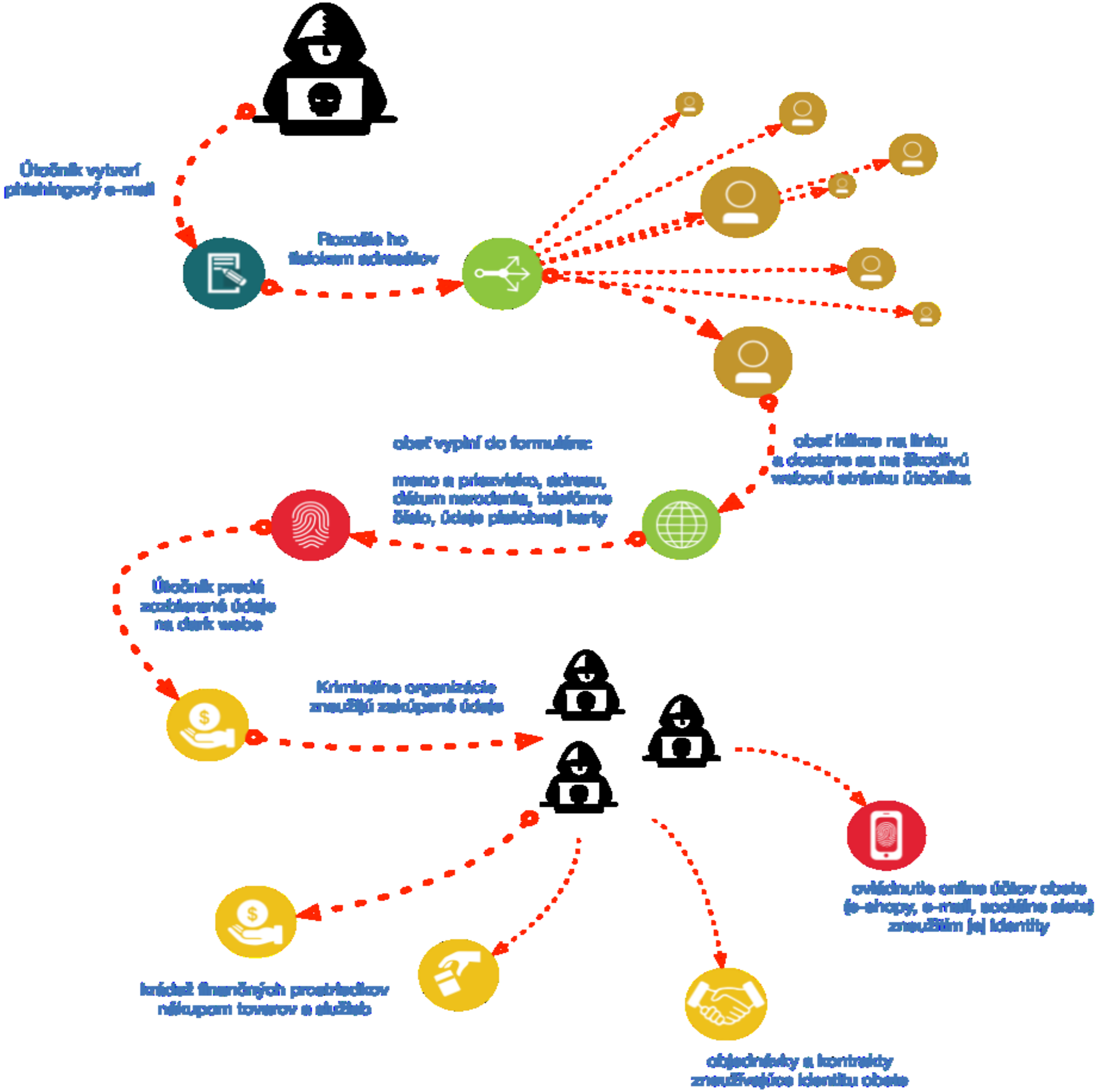
Základné typy phishingu:

- **Spear phishing = cielený pokus,** ktorý vyzerá dôveryhodne pre obete a má vyššiu pravdepodobnosť úspechu, zameraný na jednotlivca (zamestnanca)
- **E-mail phishing =** útočníci **rozosielajú e-mailové správy** miliónom kontaktov s cieľom priviesť ich na **falošnú verziu populárnej webovej stránky,** kde majú vyplniť svoje osobné údaje
- **Vishing a smishing =** phishing prostredníctvom **telefonických hovorov alebo SMS,** pri ktorých sa volajúci/píšuci vydáva za zamestnanca banky, polície alebo inej inštitúcie, pričom **číslo,** z ktorého volajú/píšu **je sfalšované** tak, že sa na displeji telefónu naozaj môže zobraziť, že vám volá banka
- **Skimming = v bankomate** nainštalované podvodné zariadenie na snímanie platobných kariet
- **Scam = podvodné alebo zavádzajúce správanie** alebo činnosť, je úmyselný a zameraný na podvod
- **Whaling =** zameriava sa na **najvplyvnejších ľudí** v organizáciách (generálni alebo výkonní riaditelia)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – phishing (proces)

1. Vytvorenie a odoslanie e-mailu (útočník)
2. Kliknutie na link v e-maile (obeť)
3. Vyplnenie údajov (obeť)
4. Predaj získaných údajov (útočník)
5. Zneužitie zakúpených údajov (útočník, kriminálne organizácie)



Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – phishing

Aktualizacia údajou

ATT00001.txt

nikola.staffenova@fri.uniza.sk v mene používateľa zamestnanec TB <tatrabanka@azet.sk>

Odoslané z verejne dostupnej e-mailovej služby

ATT00001.txt
441 B

Neobvyklá príloha

Vážený zákazník,

Všeobecné oslovenie

chceme vás upozorniť, že váš prístup do elektronického bankovníctva čoskoro vyprší. Aby ste mohli aj naďalej využívať všetky svoje výhody, vyplňte svoje osobné údaje na webe: www.tatrabanka.ssk

Odkaz na podozrivú doménu

Zmena,
Zákaznícky servis

Nezmyselná vetná formulácia

POZOR! Pokiaľ svoje údaje neaktualizujete, bude váš účet zrušení!

Rétorika naliehania

Tento e-mail sa posiela automaticky. Preto na ne není možné odpovedať.

Gramatické a štylistické chyby

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – spam

SPAM

- **Nevyžiadaná alebo nežiadúca e-mailová správa,** ktorá je hromadne rozposielaná zväčša náhodne vybraným príjemcom
- Zapĺňa e-mailové schránky, ovplyvňuje výkon servera a spotrebúva miesto na pevnom disku i pamäť
- Zvyčajne sa odosiela pre komerčné účely
- Môže byť odoslaný v masívnom objeme prostredníctvom botnetov

Ochrana:

- Nahlásiť správu ako „Spam“ svojmu e-mailovému klientovi
- Používať antispamového riešenia
- Byť opatrný pri zdieľaní kontaktných informácií
- Vzdelávať sa o problematike kybernetických útokov

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – spam

Základné typy spamu:

- **E-mailový spam = nevyžiadané e-maily,** ktoré sa často posielajú masovo, môžu zahŕňať reklamy, podvody, phishingové útoky, malware
- **Spam v sociálnych médiách =** nežiaduce **príspevky a správy na sociálnych sieťach** ako Facebook, Twitter a Instagram
- **SMS spam =** zahŕňa **nežiaduce textové správy,** ktoré sú zasielané na mobilné telefóny
- **Spam na blogoch a fórach =** zahŕňa **nežiaduce komentáre alebo príspevky na blogoch** a fórach, často s odkazmi na iné stránky

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – phishing vs. spam

	E-mail phishing	E-mailový spam
Cieľ	Kradnutie citlivých a osobných údajov	Reklama, predaj produktov alebo služieb
Personalizácia	Často personalizované, zamerané na jednotlivca	Zvyčajne nepersonalizované, posielané masovo
Riziko	Vysoké (krádež identity, finančné straty...)	Nízke (strata času, preplnenie schránky...)
Odkazy, prílohy	Falošné odkazy, netypické prílohy, žiadosť o osobné údaje	Reklamné odkazy (väčšinou bezpečné, ale otravné)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – botnety

BOTNET

robot + network = botnet

- **Skupina počítačov,** ktoré komunikujú medzi sebou a s riadiacimi (C&C) servermi a **ktorých bezpečnostná ochrana bola narušená** (je na nich spustený škodlivý kód)
- **Dôsledky:** generovanie spamu, šírenie ďalšieho škodlivého kódu alebo zahltenie siete či webového servera nadmerným množstvom požiadaviek s následným zlyhaním (DoS a DDoS útoky), phishing, prenos ukradnutých údajov...

Ochrana:

- Mať zavedený plán obnovy
- Používať firewall
- Byť opatrný pri otváraní e-mailových príloh a klikaní na neznáme odkazy
- Používať služby určené na ochranu pred botnet
- Dodržiavať bezpečnostné opatrenia – aktualizácie, pravidelné scany zariadenia

Sieť infikovaných zariadení, ktoré útočník ovláda.

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – DoS

ÚTOK ODMIETNUTIA SLUŽBY

- Typ kybernetického útoku, pri ktorom ide o pokus útočníka **zamedziť používateľom prístup k počítaču alebo sieti**
- Komunikácia medzi používateľmi je natoľko preťažená, že nemôže adekvátne prebiehať = napadnutý počítač je zvyčajne potrebné reštartovať, aby mohol poskytovať plnohodnotné služby
- **Motívy:** vyradiť webový server na určitú dobu z činnosti
- **Typy:** pretečenie vyrovnávacej pamäte, ICMP povodeň, TCP SYN povodeň, UDP povodeň

Ochrana:

- <u>Používať firewall a systémy na prevenciu prienikov</u>
- <u>Pravidelne aktualizovať zariadenie</u>
- Pravidelne sledovať a monitorovať premávku v sieti
- Mať nastavený plán obnovy a reakcie

Útok, ktorý prichádza z jedného miesta.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – DDoS

DISTRIBUOVANÝ ÚTOK ODMIETNUTIA SLUŽBY

- Typ kybernetického útoku, pri ktorom sa páchatelia snažia **narušiť alebo znefunkčniť webovú stránku, sieť či inú online službu** tým, že ju **preťažia veľkým množstvom falošných alebo nevyžiadaných požiadaviek**
- **Motívy:** zárobok z predaja útokov, vydieranie, výkupné, hacktivizmus, konkurenčná výhoda
- **Typy:** volumetrické útoky (veľké prenosové objemy dát), útoky na aplikačnej vrstve (útok na 7. vrstvu OSI modelu), protokolové útoky (zneužitie 3. a 4. vrstvy OSI modelu)

Ochrana:

- Monitorovať svoju sieťovú komunikáciu a rozpoznať v nej nezvyčajné správanie
- Mať zavedený plán obnovy
- Zvážiť presun dát do cloud
- Používať služby určené na ochranu pred DDoS
- Nedovoliť, aby sa Vaše zariadenie stalo súčasťou botnetu – dodržiavanie bezpečnostných opatrení, aktualizácie...

Útok, ktorý prichádza z viacerých miest naraz, takže je silnejší.

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – DoS vs. DDoS vs. botnet

	DoS	DDoS	Botnet
Počet zariadení	1 zdroj útoku (1 PC)	Viacero zdrojov útoku	Množstvo infikovaných PC
Komplexnosť	Relatívne jednoduché	Zložité, koordinované útoky	Vyžaduje infikovanie a kontrolu botov
Dosah útoku	Obmedzený zdroj útoku	Veľký dosah s vysokou intenzitou	Rozsiahle útoky s dlhodobým efektom
Cieľ	Zastavenie služby alebo servera	Zastavenie služby s väčším objemom požiadaviek	Využívanie zariadení na rôzne útoky
Detekcia, obrana	Pomocou jednoduchých filtrovaní	Ťažšie detekovateľné kvôli distribuovanému charakteru	Ťažko zistiteľné, útoky z rôznych IP adries

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – krádež identity

KRÁDEŽ IDENTITY

- Zločin, pri ktorom **útočník podvodom alebo oklamaním získa od obete jej osobné údaje alebo citlivé informácie,** ktoré následne použije, aby mohol konať v mene obete
- Úzko spätá s phishingom a technikami sociálneho inžinierstva
- **Proces:** zber osobných informácií, vydávanie sa za obeť, podvolené transakcie, ukývanie stopy
- **Motívy:** finančné prilepšenie útočníka
- **Dôsledky:** strata financií, poškodenie poveste, regulačné problémy...

Ochrana:

- Zabezpečiť svoje pripojenie
- Nepoužívať verejné wi-fi
- Zabezpečiť svoje zariadenie – viacvrstvové bezpečnostné riešenie
- Pravidelne aktualizovať svoje zariadenie
- Kontrolovať bankové účty
- Obozretná práca s osobnými a citlivými údajmi

Viac v bloku III

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – neautorizované činnosti

NEAUTORIZOVANÉ ČINNOSTI

- Útoky, ktoré sa **vykonávajú bez povolenia vlastníka systému alebo siete**
- Tieto činnosti môžu byť rôzne a zahŕňajú aktivity, ktoré **narúšajú alebo zneužívajú počítačové systémy, siete a dáta**
- **Motívy:** poškodenie obete, finančný zisk, vydieranie, vyhrážanie...
- **Dôsledky:** krádež citlivých údajov, poškodenie systému alebo získanie kontroly nad systémom
- **Typy:** hacking, phishing, malware, man in the middle (MitM), SQL injekcia

Ochrana:

- Používať silné a jedinečné heslá
- Inštalovať, používať a pravidelne aktualizovať antivírusový softvér
- Aktualizovať zariadenia
- Využívať firewall a šifrovanie
- Byť obozretný pri e-mailoch a správach
- Vytvárať si pravidelné zálohy
- Zúčastňovať sa školení

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – sieťové útoky

SIETOVÉ ÚTOKY

- Útoky zamerané na **narušenie alebo zneužitie počítačových sietí, infraštruktúry a komunikačných protokolov**
- **Motívy:** poškodenie obete, vydieranie, vyhrážanie, poškodenie mena...
- **Dôsledky:** získať nelegálny prístup k citlivým informáciám, poškodiť sieťovú infraštruktúru, alebo narušiť funkčnosť komunikácie v sieti
- **Typy:** na sieťovú infraštruktúru – DDoS útoky, spoofing (falšovanie identity), ransomware; na komunikačné protokoly – MitM, sniffing (odpočúvanie), session hijacking (preberanie relácie)

Ochrana:

- Inštalovať, používať a pravidelne aktualizovať antivírusový softvér
- Aktualizovať zariadenia
- Využívať firewall a šifrovanie v komunikácii
- Používať silné autentifikačné metódy
- Používať VPN
- Pravidelne sa školiť

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – útoky na mobilné a bezdrôtové zariadenia

DISTRIBUOVANÝ ÚTOK ODMIETNUTIA SLUŽBY

- Útoky **využívajú špecifické zraniteľnosti v hardvéri, softvéri a komunikačných protokoloch mobilných a bezdrôtových zariadení**
- **Motívy:** poškodenie obete, vydieranie, vyhrážanie, poškodiť dobré meno...
- **Dôsledky:** získať neautorizovaný prístup, krádež citlivých údajov, narušenie funkčnosti zariadení
- **Typy:** wi-fi hacking, bluejacking, bluesnarfing, jamming (rušenie signálu), útoky na WPS PIN, sniffing

Ochrana:

- Inštalovať, používať a pravidelne aktualizovať antivírusový softvér/bezpečnostné aplikácie
- Aktualizovať zariadenia
- Inštalovať aplikácie z dôveryhodných zdrojov
- Používať silné autentifikačné metódy
- Vypínať nepotrebné bezdrôtové funkcie
- Šifrovať komunikáciu

Viac v bloku VI

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – zaujímavosti

49 miliónov obetí v roku 2021

v USA z dôvodu **krádeže identity,** spôsobilo celkový finančný dopad viac ako 52 miliárd $

22 % incidentov v roku 2022

sa týkalo **neautorizovaných činností** (vrátane interných útokov zamestnancov a zneužitia prístupových práv)

62 % organizácií v roku 2020

sa stalo obeťami **sieťových útokov** najmä formou DDoS útokov, útokov na firewall, či na exploity zraniteľnosti v protokoloch

40 % mobilných zariadení v roku 2021

čelilo min. jednému útoku formou **mobilných malware alebo phishingových** útokov

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – zraniteľnosť aplikácií

SIETOVÉ ÚTOKY

- Rôzne spôsoby, ako útočníci môžu **zneužiť bezpečnostné zraniteľnosti aplikácií** na nekalé úmysly, pričom tieto **útoky sú zamerané na rôzne úrovne aplikácie,** ako je jej kód, serverová infraštruktúra, alebo spôsob, akým sa aplikácia komunikuje so servermi a používateľmi
- **Motívy:** poškodenie mena, zneužitie údajov...
- **Dôsledky:** získať neautorizovaný prístup, krádež citlivých údajov, manipulácia s aplikáciou alebo jej narušenie
- **Typy:** SQL injekcia, XSS, CSFR, IDOR, DDoS, pretečenie zásobníka, eskalácia privilégií, malware, keylogging

Ochrana:

- Inštalovať, používať a pravidelne aktualizovať antivírusový softvér
- Aktualizovať zariadenia
- Používať firewall a iné služby na ochranu pred útokmi
- Využívať dvojfaktorovú autentifikáciu
- Používať šifrovanie na prenos dát

Typy úmyselných kybernetických hrozieb a útokov, spôsob ich šírenia a dôsledky – zraniteľnosť aplikácií

Zraniteľnosť formou slabých hesiel

- Ide o **útok na webovú aplikáciu**
- Za zraniteľnosť **nesie zodpovednosť používateľ,** nie autor webovej aplikácie
- Dôvodom je **používanie predvídateľných a jednoduchých hesiel**

Riešenie:

- Znížiť počet pokusov o prihlásenie
- Vložiť časový interval medzi jednotlivé pokusy o prihlásenie
- Stanoviť explicitný tvar hesla

8-znakové heslo	
Len čísla	**Okamžite** až 2 hod.
Len malé písmená	**3 min.** až 4 mesiace
Len malé a veľké písmená	**11 hod.** až 92 rokov
Čísla + malé a veľké písmená	**2 dni** až 375 rokov
Čísla + malé a veľké písmená + symboly	**5 dní** až 989 rokov

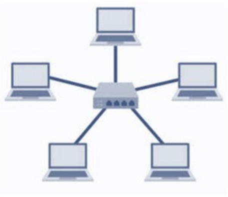
03

Vysvetlenie hrozieb a útokov v rôznych doménach kybernetickej bezpečnosti

Domény kybernetickej bezpečnosti a hrozby v nich

Sieťová bezpečnosť

- Ochrana siete pred útokmi a neautorizovaným prístupom
- Zabezpečiť integritu a dostupnosť dát pri ich prenose
- **Hrozby –** DoS/DDoS, MitM, spoofing, neautorizované prístupové body
- **Ochrana –** protokoly, šifrovanie, firewall, DDoS ochrana, IDS/IPS



Aplikačná bezpečnosť

- Ochrana SW aplikácií pred zraniteľnosťami, ktoré môžu byť zneužité na získanie prístupu k systému alebo dátam
- **Hrozby –** SQL injekcia, XSS, CSFR, pretečenie zásobníka
- **Ochrana –** testovanie zraniteľností, zabezpečenie databáz, bezpečné programovanie

Bezpečnosť koncových zariadení

- Ochrana zariadení, ktoré sa pripájajú do siete (PC, smartfóny, tablety, server...)
- **Hrozby –** malware, keylogger, zraniteľnosť OS
- **Ochrana –** antivírus, antimalware, šifrovanie, zabezpečenie mobilných zariadení, správa mobilných zariadení

Domény kybernetickej bezpečnosti a hrozby v nich

Bezpečnosť v cloude

- Ochrana dát a aplikácií, ktoré sú uložené v cloudových prostrediach (verejné, súkromné, hybridné)
- **Hrozby –** útok na API, únik dát, neautorizovaný prístup
- **Ochrana –** šifrovanie dát, správa prístupov, zabezpečenie API rozhraní, bezpečnosť pri migrácií do cloudu

Bezpečnosť prístupu a identity

- Správa a kontrola prístupových práv a autentifikácia používateľov a systémov
- **Hrozby –** phishing, stuffing, hrubá sila
- **Ochrana –** viacfaktorová autentifikácia, správa používateľských práv, systémy na jednotné prihlásenie, kontrola prístupu na báze rolí

Bezpečnosť dát

- Ochrana dát počas ich životného cyklu (ukladanie, prenos, spracovanie)
- **Hrozby –** malware, MitM, vnútorné útoky, neoprávnený prístup
- **Ochrana –** šifrovanie, zálohovanie, obnova, ochrana pred krádežou, politiky ochrany údajov (GDPR, HIPAA)

Domény kybernetickej bezpečnosti a hrozby v nich

Manažment a riadenie incidentov

- Spracovanie a riešenie kybernetických útokov a incidentov, aby sa minimalizovali škody a zistili príčiny útokov
- **Hrozby –** zero-day útoky, sociálne inžinierstvo, APT
- **Ochrana –** monitorovanie a detekcia, forenzná analýza, obnova po útoku, tvorba plánov reakcie na incidenty

Riadenie rizík

- Proces pozostávajúci z identifikácie, hodnotenia a zmierňovania rizík, ktoré môžu ohroziť informačné systémy organizácie
- **Hrozby –** slabá bezpečnostná politika, nedostatočná pripravenosť na incidenty
- **Ochrana –** hodnotenie zraniteľností, analýza rizík, tvorba bezpečnostných politík a stratégií

Fyzická bezpečnosť

- Ochrana fyzických zariadení a infraštruktúry, aby sa zabránilo krádeži alebo sabotážam
- **Hrozby –** krádež, vandalizmus, sabotáž, zneužitie práv
- **Ochrana –** kontrola prístupu, ochrana pred fyzickým prienikom, zabezpečenie záložných systémov

Domény kybernetickej bezpečnosti a hrozby v nich

Bezpečnosť v IoT

- Ochrana zariadení pripojených k internetu (inteligentné zariadenia, senzory, vozidlá...)
- **Hrozby –** botnety, nebezpečné zariadenia, zachytávanie údajov
- **Ochrana –** zabezpečenie komunikačných kanálov, ochrana pred botnetmi, správa a monitorovanie zariadení

Bezpečnosť v mobilných zariadeniach

- Ochrana smartfónov, tabletov a iných prenosných zariadení pred útokmi a zneužitím
- **Hrozby –** malware, phishing, zneužitie nešifrovaných dát
- **Ochrana –** bezpečnosť aplikácií pre mobilné zariadenia, šifrovanie dát, prevencia pred stratou

Bezpečnosť prevádzkových technológií

- Ochrana technologických systémov a infraštruktúry, ktoré sú prepojené s priemyselnými procesmi
- **Hrozby –** sabotáže, útok na priemyselné systémy
- **Ochrana –** zabezpečenie priemyselných kontrolných systémov, detekcia útokov, prevencia pred sabotážou

Prečo ste sa zúčastnili kurzu?

43 % organizácií v roku 2017

bolo hodnotených ako extrémne málo pripravených na kybernetické útoky

40% nárast útokov v roku 2020

bolo zaznamenaných práve na cloudové služby

73 % útokov v roku 2017

bolo realizovaných na základe zraniteľností webových aplikácií

25 % útokov vo svete v roku 2021

využívalo botnety, ktoré následne spustili DDoS útoky či ransomware

1,4 mil. stránok v roku 2017

vzniklo každý mesiac ako nové phishingové stránky

36 % útokov vo svete v roku 2023

bolo spôsobených rôznymi formami phishingu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť!

Typy KB hrozieb a útokov

Bezpečnostné riziká, opatrenia a prevencia (Blok II)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ing. Nikola Štaffenová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

nikola.staffenova@fri.uniza.sk