
ÚVOD DO PROBLEMATIKY KYBERNETICKEJ BEZPEČNOSTI



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

1. Úvod do kybernetickej bezpečnosti (KB)
2. Informačná vs. kybernetická bezpečnosť
3. Kľúčové pojmy a definície
4. Legislatívny rámec
5. Zodpovednosť zamestnancov
6. Zásady bezpečného používania:
7. Zálohovanie údajov
8. Sociálne inžinierstvo a Phishing
9. Súhrn a záver

PREČO JE KYBERNETICKÁ BEZPEČNOSŤ DÔLEŽITÁ?

- V dobe digitálnej transformácie je väčšina našich činností prepojená s internetom.
- **Kybernetická bezpečnosť** je súbor opatrení, nástrojov a procesov na ochranu systémov, sietí a údajov pred hrozbami.
- Kybernetické útoky majú rôzne podoby – od škodlivých e-mailov až po sofistikované útoky na kritickú infraštruktúru (firmy, nemocnice, štátne inštitúcie).
- Každý, kto používa digitálne technológie, je súčasťou tohto prostredia a môže byť jeho slabinou, alebo naopak, silným článkom.

HROZBY A ICH NÁSLEDKY

- **Bežné zraniteľnosti:** Phishingové e-maily, podvodné odkazy, slabé heslá, neaktualizované zariadenia.
- **Ciele útočníkov:** Citlivé údaje, firemné systémy, alebo vaša osobná identita.
- **Možné následky útokov:**
 - Strata dát
 - Finančné škody
 - Poškodenie reputácie a mena organizácie
 - Ohrozenie zdravia alebo života ľudí

Informačná bezpečnosť	Kybernetická bezpečnosť
Širší pojem - ochrana všetkých informácií (digitálnych, papierových, v pamäti človeka).	Užší pojem - podmnožina informačnej bezpečnosti.
Ciel': Dôvernosc', Integrita, Dostupnosť (CIA).	Zameranie: Ochrana digitálneho prostredia (počítače, siete, servery, dáta).
Zahrňa: Fyzickú, organizačnú a technickú bezpečnosť.	Rieši: Hrozby ako hackeri, malvér, phishing, ransomvér.

INFORMAČNÁ VS. KYBERNETICKÁ BEZPEČNOSŤ

Aj keď sa tieto pojmy často zamieňajú, nie sú totožné.

KLÚČOVÉ POJMY I: ZÁKLADNÁ TROJICA (CIA)

- **Kybernetická bezpečnosť:** Zachovanie dôvernosti, dostupnosti a integrity informácií v kybernetickom priestore.
- **Dôvernost':** Prístup k informáciám majú len oprávnené osoby.
- **Integrita:** Miera bezchybnosti informácie; informácie neboli neoprávnene zmenené.
- **Dostupnosť:** Miera dostupnosti informácie pre používateľa vo chvíli, keď je potrebná.

KLÍČOVÉ POJMY II: RIZIKO, HROZBA, ZRANITEL'NOST'

- **Aktívum:** Všetko, čo má pre organizáciu hodnotu a je potrebné to chrániť (dáta, hardvér, softvér, ale aj reputácia).
 - **Zraniteľnosť:** Slabé miesto aktíva, systému alebo procesu, ktoré môže byť zneužitá.
 - **Hrozba:** Potenciálna udalosť, ktorá môže zneužiť zraniteľnosť a spôsobiť škodu.
 - **Riziko:** Pravdepodobnosť, že hrozba zneužije zraniteľnosť a spôsobí škodu.
-

LEGISLATÍVNY RÁMEC - NÁRODNÁ ÚROVEŇ

Bezpečnostné postupy sa riadia platnou legislatívou. Medzi kľúčové predpisy patria:

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- Vyhláška NBÚ č. 362/2018 Z. z. (obsah bezpečnostných opatrení a dokumentácie)
- Vyhláška NBÚ č. 164/2018 Z. z. (kritériá a hlásenie KB incidentov)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe

ZODPOVEDNOSŤ ZAMESTNANCOV - POVINNOSTI (1/2)

Každý zamestnanec je povinný:

- Zaisťovať nepretržitú ochranu zverených informačných aktív (dôvernosť, integrita, dostupnosť).
- Predchádzať vzniku bezpečnostných a kybernetických bezpečnostných incidentov.
- Spolupracovať pri riešení škôd a likvidácii následkov.
- Dodržiavať a presadzovať zásady informačnej a kybernetickej bezpečnosti v rámci svojich činností.

ZODPOVEDNOSŤ ZAMESTNANCOV - POVINNOSTI (2/2)

Každý zamestnanec je ďalej povinný:

- Oznamovať **včas a úplne** každé porušenie zásad KB a zistené bezpečnostné riziká.
- Plniť si povinnosti v oblasti KB vyplývajúce z pracovného pomeru.

Zamestnanec je oprávnený:

- Vyžadovať metodickú pomoc od manažéra kybernetickej bezpečnosti a IT oddelenia.

ZÁSADY POUŽÍVANIA PRACOVNEJ STANICE

- Pracovná stanica je pridelená konkrétnemu zamestnancovi a má sa používať s prístupom **bežného používateľa**.
- Vzájomné zdieľanie súborov sa musí realizovať cez **spoločný sieťový disk** s riadeným prístupom.
- Je **zakázané** vytvárať neschválené prístupové body do firemnej siete.
- Vzdialený prístup je možný výhradne cez zabezpečené spojenie (**VPN tunel**) a musí byť schválený.

POVINNOSTI PRI POUŽÍVANÍ PRACOVNEJ STANICE

- **Chráňte svoje prístupové údaje** a neumožnite inej osobe prístup pod vaším kontom.
- **Zamykajte pracovnú stanicu** pri každom opustení pracoviska (napr. klávesovou skratkou **Win+L**).
- **Nevykonávajte neoprávnené činnosti**, ako je obchádzanie bezpečnostných opatrení, pokusy o získanie cudzích hesiel alebo maskovanie vlastnej identity (napr. zmena IP/MAC adresy).
- **Nemeňte svojvoľne konfiguráciu** pracovnej stanice (sieťové nastavenia, firewall, bezpečnostné politiky).

ZÁSADY POUŽÍVANIA POUŽÍVATEĽSKÉHO KONTA

- Používateľské konto je vaša **digitálna identita**.
- Ste **zodpovední** za všetky operácie, ktoré sa vykonajú pod vaším účtom.
- **Je zakázané:**
 - Zdieľať svoje konto s kýmkoľvek.
 - Používať rovnaké heslo vo viacerých systémoch.
 - Ukladať si heslá na viditeľných a nechránených miestach (papieriky na monitore a pod.).

OCHRANA POUŽÍVATEĽSKÉHO KONTA - HESLÁ

- **Používajte silné heslo:**
 - Minimálne 12 znakov (podľa politiky organizácie).
 - Kombinácia veľkých a malých písmen, číslíc a špeciálnych znakov.
- **Nikdy nezdieľajte svoje heslo**, ani s kolegami či IT oddelením.
- V prípade podozrenia na prezradenie hesla ho **bezodkladne zmeňte** a informujte manažéra KB a IT oddelenie.

OCHRANA PRED ŠKODLIVÝM KÓDOM (MALVÉR)

- **Malvér (Malicious software)** je akýkoľvek softvér, ktorého cieľom je spôsobiť škodu na dátach alebo systéme.
- **Druhy podľa spôsobu šírenia:**
 - **Vírus:** Vloží sa do iného programu a aktivuje sa jeho spustením.
 - **Červ (Worm):** Samostatne sa replikuje a šíri po sieti.
 - **Trójsky kôň:** Tvári sa ako užitočný program, no v skutočnosti škodí.

DRUHY MALVÉRU PODĽA AKTIVITY

- **Ransomvér:** Zašifruje dáta a požaduje výkupné za ich obnovenie. Je to jedna z najčastejších a najnebezpečnejších hrozieb.
- **Spyware:** Špehuje vašu aktivitu a zhromažďuje informácie.
- **Adware:** Zobrazuje nevyžiadané reklamy.
- **Bot/Botnet:** Ovládne počítač a zaradí ho do siete infikovaných zariadení, ktoré útočník využíva na ďalšie útoky.

AKO SA CHRÁNIŤ PRED MALVÉROM?

- **Umožnite automatické aktualizácie** operačného systému a antivírusového softvéru.
- **Majte vždy spustenú rezidentnú ochranu** antivírusového programu.
- **Neotvárajte správy a prílohy** od neznámych odosielateľov.
- **Nesťahujte a neinštalujte** nelegálny alebo neschválený softvér.
- **Nepripájajte neznáme médiá** (napr. nájdený USB kľúč) do pracovného počítača.
- **Vždy kontrolujte** antivírusom všetky pripojené médiá (CD, DVD, USB).

ČO ROBIŤ PRI DETEKCI MALVÉRU?

1. **Zachovajte pokoj.** Nepovoliť žiadnu automatickú inštaláciu.
2. Neotvárajte označený súbor a neposielajte infikovanú správu ďalej.
3. **Okamžite oznámte** skutočnosť manažérovi KB a IT podpore.
4. Riad'te sa pokynmi antivírusového programu (vymazať, dať do karantény).
5. Nahláste udalosť ako **bezpečnostný incident**.

ZÁSADY BEZPEČNÉHO POUŽÍVANIA E-POŠTY

- Služobný e-mail je určený na plnenie **pracovných úloh**.
- E-mailová komunikácia sa považuje za pracovnú a je **monitorovaná**.
- **Neposielajte citlivé informácie** (heslá, osobné údaje, dôverné dokumenty) nešifrovaným spôsobom. V prípade potreby použite šifrovanie správy alebo zaheslovanú prílohu (heslo pošlite iným kanálom).
- Nezúčastňujte sa na preposielaní "**reťazových správ**".
- Nepoužívajte súkromný e-mail na pracovné účely.

BEZPEČNÁ E-POŠTA: POZOR NA PHISHING!

- **Pozorne si všímajte odosielateľa.** Dajte si pozor na napodobeniny firemných adries (napr. info@firrn.sk namiesto info@firma.sk).
- **Neklikajte bez rozmyslu** na odkazy a prílohy, aj keď je e-mail od známeho kontaktu.
- **Odporúča sa používať dvojfaktorovú autentifikáciu (2FA)** na ochranu e-mailového konta.
- Ak máte podozrenie, **nahláste e-mail IT oddeleniu.** Lepšie nahlásiť zbytočne, ako nechať hrozbu šíriť sa ďalej.

ZÁSADY BEZPEČNÉHO POUŽÍVANIA INTERNETU

- Prístup na internet je poskytovaný na **plnenie pracovných povinností** a je **monitorovaný**.
- Organizácia používa **webovú filtráciu** na obmedzenie prístupu na stránky nesúvisiace s prácou.
- Je **zakázané**:
 - Sťahovať, reprodukovat' alebo distribuovať materiál chránený autorskými právami (hudba, filmy, softvér).
 - Navštevovať stránky s nevhodným alebo nelegálnym obsahom.
 - Vystavovať interné alebo chránené informácie na internete.
 - Inštalovať neschválený softvér z internetu.

KOMUNIKAČNÉ SLUŽBY A SOCIÁLNE SIETE

- Používajte **len povolené komunikačné služby** a aplikácie (napr. MS Teams, Outlook, Lync v rámci organizácie).
- Pri používaní sociálnych sietí (Facebook, LinkedIn atď.) si **dobre nastavte súkromie profilu**.
- **Rozmýšľajte, čo zdieľate**. Aj bežná fotografia z práce môže nechtiac odhaliť dôverné informácie.
- **Nezdieľajte firemné interné informácie** cez súkromné účty alebo neoficiálne kanály.
- Je zakázané zverejňovať súkromné údaje, ktoré majú súvis s pracovnými povinnosťami (napr. termíny pracovných ciest).

ZÁSADY BEZPEČNÉHO POUŽÍVANIA PRENOSNÝCH ZARIADENÍ

- Ste **zodpovední** za ochranu prideleného zariadenia (notebook, tablet) a dát na ňom pred krádežou a zneužitím.
- **Nikdy nenechávajte zariadenie bez dozoru** na verejných miestach (kaviareň, auto).
- Na zariadeniach používajte **automatické blokovanie obrazovky** s heslom, PINom alebo biometriou.
- Dáta na prenosných médiách (USB kľúč), ktoré obsahujú klasifikované informácie, **musia byť šifrované**.
- **Nepripájajte pracovné zariadenia na neznáme nabíjacie stanice** (napr. v obchodných centrách). Použite vlastnú nabíjačku alebo power banku.

ZÁLOHOVANIE ÚDAJOV

- **Prečo je dôležité?** Ochrana pred ransomvérom, zlyhaním techniky a ľudskou chybou (neúmyselné vymazanie).
- Zamestnanec je povinný zálohovať svoje pracovné súbory **minimálne raz mesačne**.
- Na zálohovanie primárne slúži **zdieľaný sieťový disk**.
- **Nikdy neukladajte jedinú kópiu** dôležitých súborov len na lokálny disk počítača (napr. na Plochu).
- Zálohy obsahujúce chránené údaje musia byť na záznamovom médiu **šifrované**.

SOCIÁLNE INŽINIERSTVO - DEFINÍCIA

- Je to stratégia manipulácie a zavádzania ľudí s cieľom, aby **sprístupnili citlivé informácie** alebo vykonali kroky ohrozujúce bezpečnosť.
- Spolieha sa na **psychológiu a ľudské správanie**, nie na technické zručnosti útočníka.
- **Cieľ**: Získať heslá, osobné údaje, nainštalovať malvér alebo presvedčiť obeť, aby urobila niečo v mene útočníka.
- Je to jeden z **najefektívnejších** nástrojov na získavanie informácií.

TECHNIKY SOCIÁLNEHO INŽINIERSTVA

- **Phishing:** Najznámejšia technika; podvodný e-mail s cieľom získať citlivé údaje.
- **Vishing & Smishing:** Hlasový phishing (telefonát) a SMS phishing (SMS správa).
- **Zosobnenie (Impersonation):** Útočník sa vydáva za dôveryhodnú osobu (napr. riaditeľa) a žiada o vykonanie podvodnej transakcie.
- **Baiting:** Útočník nastraží infikované fyzické médium (napr. USB kľúč) na mieste, kde ho obeť nájde.

ČO JE PHISHING?

- Cílený útok využívajúci sociálne inžinierstvo (zneužitie dôvery, manipulácia).
- Cieľom je získať citlivé informácie (heslá, čísla kariet) odoslaním falošného e-mailu, ktorý navádza na kliknutie na podvodný odkaz alebo otvorenie škodlivej prílohy.
- Útočníci často využívajú **pocit naliehavosti** ("urobte to rýchlo, inak...") a časovanie (napr. piatok poobede).
- **Upozornenie:** Bežná antivírusová ochrana **nevie detegovať phishing** a účinne pred ním chrániť.

AKO ROZPOZNAŤ PHISHING? VAROVNÉ SIGNÁLY

- **Zvláštna adresa odosielateľa:** E-mail prišiel z verejnej služby (@gmail, @yahoo) alebo doména je podozrivo zmenená (napr. www.google.com).
 - **Všeobecné oslovenie:** "Vážený zákazník," namiesto vášho mena.
 - **Gramatické chyby a zlý preklad:** Text vyzerá ako strojovo preložený.
 - **Pocit naliehavosti a vyhrážky:** Správa vyžaduje okamžitú akciu.
 - **Podozrivý odkaz alebo príloha:** Link vedie na neznámu stránku alebo správa obsahuje neočakávanú prílohu (.zip, .rar).
 - **Neobvyklá požiadavka:** Žiadosť o zadanie hesla alebo schválenie nečakanej platby.
-

PRÍKLAD PHISHINGOVÉHO E-MAILU

Interný audit: Vykonávaný samotnou organizáciou alebo v jej mene

Varovné signály v tomto príklade:

- **Odosielateľ:** Adresa ALI@code.edu.az je podozrivá a nesúvisí so Slovenskou poštou.
 - **Naliehavosť:** "Zásielka čaká na doručenie", "Potvrďte platbu".
 - **Odkaz:** Tlačidlo "Potvrďte tu" pravdepodobne vedie na falošnú stránku, ktorej cieľom je ukradnúť platobné údaje.
 - **Malá suma:** Nízka suma (0,50 €) má znížiť ostražitosť obete.
-

ČO ROBIŤ PRI PODOZRENÍ NA PHISHING?

1. **NEKLIKAJTE** na odkazy a **NEOTVÁRAJTE** prílohy.
2. **NEREAGUJTE** na správu.
3. **NEZADÁVAJTE** žiadne prihlasovacie údaje.
4. **NAHLÁSTE** podozrivý e-mail útvaru zodpovednému za riešenie bezpečnostných incidentov (IT oddelenie), aby mohli zdroj zablokovať.
5. Ak si nie ste istí, **overte si požiadavku** iným kanálom (napr. telefonicky), ale nepoužívajte kontaktné údaje z podozrivého e-mailu.

RIZIKÁ PHISHINGU

V práci:

- Krádež peňazí z firemného účtu
- Únik osobných údajov zamestnancov alebo zákazníkov
- Infikovanie firemnej siete škodlivým kódom (napr. ransomvérom)
- Zablokovanie prístupu k informačným systémom a dátam
- Poškodenie mena a reputácie organizácie

Doma:

- Krádež peňazí z bankového účtu
- Krádež identity a účtov na sociálnych sieťach
- Strata citlivých súkromných údajov (fotografie, dokumenty)

SÚHRN: ZÁSADA ČISTÉHO STOLA A ČISTEJ OBRAZOVKY

- **Zásada čistého stola:** Pri odchode z pracoviska (obed, koniec zmeny) odložte všetky dokumenty s citlivými informáciami do uzamykateľnej skrine.
- **Zásada čistej obrazovky:** Pri každom opustení pracoviska uzamknite obrazovku počítača (**Win+L**).
- **Zásada ochrany hesla:** Heslo si nezapisujte na papieriky a nelepte na monitor.

SÚHRN: KLÚČOVÉ BEZPEČNOSTNÉ NÁVYKY (1/2)

- Používajte **silné a jedinečné heslá** pre rôzne systémy.
- **Nepripájajte nedôveryhodné médiá** (cudzie/nájsené USB, CD) do pracovného PC.
- **Nepoužívajte verejné Wi-Fi** siete bez zabezpečenia (VPN).
- Citlivé informácie pri prenose **šifrujte** (napr. zaheslovaním prílohy).
- **Neinštalujte** si na pracovný počítač vlastný, neschválený softvér.

SÚHRN: KLÚČOVÉ BEZPEČNOSTNÉ NÁVYKY (2/2)

- **Zásada "Need to Know"**: Zdieľajte informácie a udeľujte prístupy len v nevyhnutnom rozsahu pre plnenie úloh.
- **Dôkladne si všímajte e-maily**: Kontrolujte odosielateľa, gramatiku a podozrivé požiadavky.
- **Neotvárajte** podozrivé prílohy a **neklikajte** na podozrivé odkazy.
- **Nevynášajte** dokumenty (ani v listinnej podobe) z určeného miesta, ak to nie je nevyhnutné.
- **Neukladajte** klasifikované informácie na iné médium alebo počítač, ako je určené.

ZÁVER: VAŠA ROLA V KYBERNETICKEJ BEZPEČNOSTI

- Kybernetická bezpečnosť **nie je len úlohou IT oddelenia.**
- Každý zamestnanec je kľúčovým prvkom obrany.
- Vaša **obozretnosť a dodržiavanie pravidiel** sú najlepšou ochranou proti sociálnemu inžinierstvu a mnohým ďalším hrozbám.
- Zostaňte informovaní a neustále sa vzdelávajte.

DÔLEŽITÉ KONTAKTY A POSTUP PRI INCIDENTE

V prípade akéhokoľvek podozrenia na bezpečnostný incident (napr. podozrivý e-mail, strata zariadenia, detekcia vírusu):

- **Bezodkladne informujte a kontaktujte:**
 - **Manažéra kybernetickej bezpečnosti**
 - **Útvar zodpovedný za riešenie bezpečnostných incidentov**
 - **IT podporu**

Vaša rýchla reakcia môže zabrániť vážnym škodám!

ĎAKUJEM ZA POZORNOST