
PERSONÁLNA BEZPEČNOSŤ

BC. LITAUSZKI PAVOL



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

- **Úvod:** Prečo je človek kľúčový pre bezpečnosť?
- **Analýza hrozieb:** Interné hrozby a sociálne inžinierstvo
- **Hlavné procesy:** Životný cyklus zamestnanca z pohľadu bezpečnosti
- **Bezpečnostné povedomie:** Vzdelávanie ako základ obrany
- **Moderné výzvy:** Práca na diaľku a "Gig Economy"
- **Budúcnosť a trendy:** Úloha AI a budovanie bezpečnostnej kultúry
- **Kľúčové odporúčania:** Čo by mal vedieť zamestnanec a zamestnávateľ
- **Záver a diskusia**

ÚVOD: VIAC NEŽ LEN TECHNOLOGIA

Kybernetická bezpečnosť sa často spája s technológiami ako sú antivírusy, firewally alebo šifrovanie. Avšak aj ten najlepší a najdrahší systém môže zlyhať, ak s ním pracuje nespoľahlivý, nepozorný alebo neinformovaný človek.

Personálna bezpečnosť je súbor opatrení, ktoré minimalizujú riziká spojené s ľudským faktorom.

ČLOVEK: NAJSILNEJŠÍ AJ NAJZRANITELNEJŠÍ ČLÁNOK

- V komunitě informační bezpečnosti se traduje, že největší riziko se nachází **mezi obrazovkou počítače a kancelářskou stoličkou**.
- Lidský faktor je cílem drtivě většiny kybernetických útoků (např. phishing, sociální inženýrstvo).
- Útočníci často neútočí nejprve na počítače, ale na lidi.
- Zaměstnanec může nechtíc otevřít dveře útočníkovi a negovat tak účinnost drahých technologických obranných mechanismů.



TRI PILIERE KYBERNETICKEJ ODOLNOSTI

Účinný program kybernetickej bezpečnosti musí byť postavený na synergii troch pilierov:

1. **Ľudia:** Informovaní, ostražití a zodpovední zamestnanci.
2. **Procesy:** Jasne definované a vynucované bezpečnostné pravidlá.
3. **Technológie:** Nástroje na ochranu, detekciu a reakciu.

Personálna bezpečnosť systematcky prepája tieto tri oblasti.

DEFINÍCIA A CIELE PERSONÁLNEJ BEZPEČNOSTI

Definícia: Systematický prístup k riadeniu rizík spojených s ľuďmi, ktorí majú legitímny prístup k aktívam organizácie. Cieľom je predchádzať, odhaľovať a reagovať na hrozby vyplývajúce z ľudského konania.

Primárny cieľ: Ochrana najcennejších aktív organizácie – jej ľudí, informácií a reputácie.

KLÚČOVÉ CIELE PERSONÁLNEJ BEZPEČNOSTI






Efektívny program personálnej bezpečnosti umožňuje organizácii:

- **Znížiť riziko poškodenia** zamestnancov, zákazníkov a partnerov.
- **Minimalizovať riziko straty, poškodenia alebo kompromitácie** informácií a hmotných aktív.
- **Zvýšiť dôveru** v osoby, ktoré majú prístup k citlivým informáciám.
- **Zabezpečiť efektívnejšie a bezpečnejšie fungovanie** a poskytovanie služieb.

ANALÝZA HROZIEB: INTERNÉ HROZBY (INSIDER THREATS)

- **Definícia:** Bezpečnostné riziko, ktoré pochádza zvnútra organizácie.
- **Zdroj:** Súčasní alebo bývalí zamestnanci, dodávatelia, konzultanti alebo partneri.
- **Mechanizmus:** Oprávnený prístup k sieťam, systémom alebo dátam je zneužitý, či už úmyselne alebo neúmyselne, na poškodenie organizácie.

ANALÝZA HROZIEB: INTERNÉ HROZBY (INSIDER THREATS)

-  **Code review** (viac očí = menšie riziko)
-  **Oddelenie právomocí** (nikto nemá „všetko“)
-  **Logovanie a monitoring zmien**
-  **Okamžitý offboarding zamestnancov**
-  **Bezpečnostné povedomie tímu**

Príklad 1 – Časová bomba

Program funguje normálne, ale 1. januára automaticky vymaže databázu logov.

Príklad 2 – Personálna bomba

Ak je účet konkrétneho zamestnanca odstránený, systém prestane spracúvať objednávky.

Príklad 3 – Prevádzková bomba

Po 1000. spustení aplikácie sa začne poškodzovať uložený súbor.

(Dôležité: nejde o chyby, ale úmyselné správanie.)

KLASIFIKÁCIA INTERNÝCH HROZIEB

Interné hrozby sa delia do dvoch hlavných kategórií podľa motivácie a spôsobu konania:

- 1. Neúmyselné (Negligent) hrozby:** Najčastejší a často finančne najnákladnejší typ, spôsobený ľudskou chybou, nedbanlivosťou alebo manipuláciou.

KLASIFIKÁCIA INTERNÝCH HROZIEB

Interné hrozby sa delia do dvoch hlavných kategórií podľa motivácie a spôsobu konania:

- 1. Neúmyselné (Negligent) hrozby:** Najčastejší a často finančne najnákladnejší typ, spôsobený ľudskou chybou, nedbanlivosťou alebo manipuláciou.
- 2. Úmyselné (Malicious) hrozby:** Výsledok plánovaného a cieleného konania jednotlivca so zlým úmyslom.

NEÚMYSELNÉ INTERNÉ HROZBY

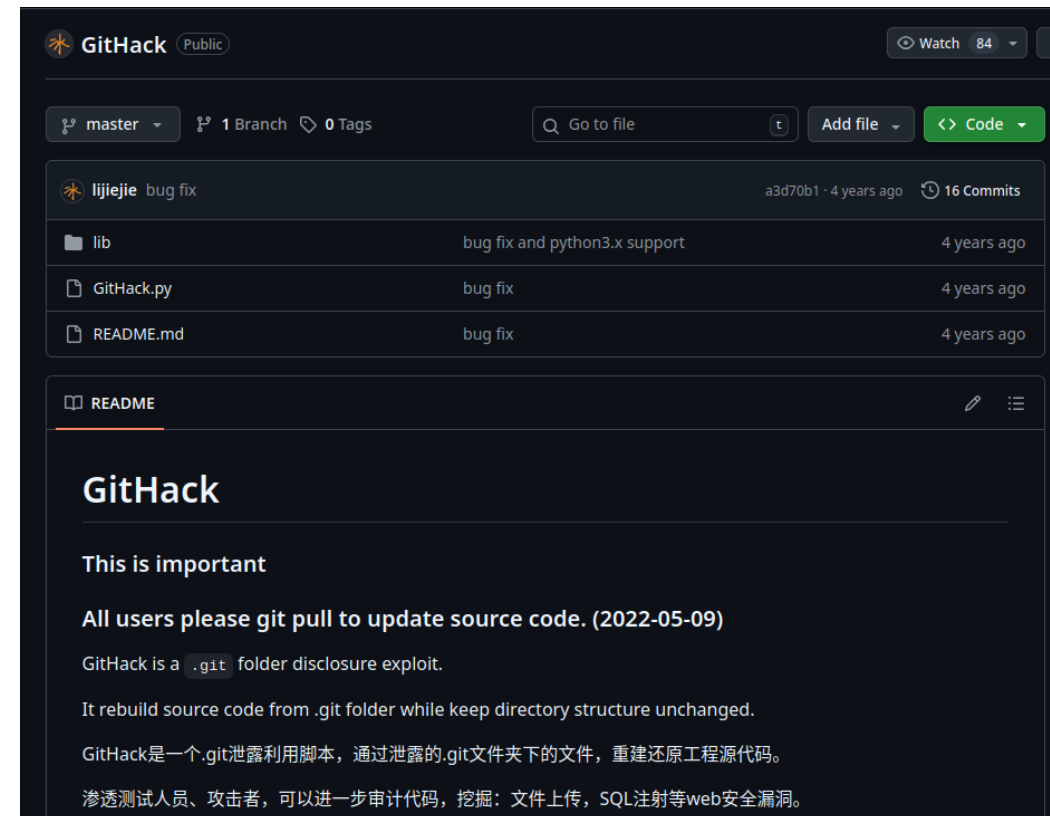
Príčinou nie je zlý úmysel, ale nedbanlivosť alebo nepozornosť.

Typické príklady:

- Kliknutie na odkaz v phishingovom e-maile.
- Používanie slabých alebo opakujúcich sa hesiel.
- Zanedbanie bezpečnostných aktualizácií.
- Odoslanie citlivých dokumentov nesprávnemu príjemcovi.
- Strata nezabezpečeného firemného zariadenia.

PRÍPADOVÁ ŠTÚDIA: MICROSOFT (2022)

- **Incident:** Niekoľko zamestnancov nechtiac odhalilo prihlasovacie údaje k firemnej infraštruktúre na platforme GitHub.
- **Potenciálny dopad:** Prístup útočníkov k serverom Azure a ďalším interným systémom.
- **Ponaučenie:** Technická zdatnosť a bezpečnostné povedomie sú dve odlišné kategórie. Programy personálnej bezpečnosti musia byť univerzálne pre všetkých zamestnancov.



ÚMYSELNÉ INTERNÉ HROZBY

Cielené konanie so zlým úmyslom.

Motivácia:

- Finančný zisk
- Pomsta voči zamestnávateľovi
- Ideologické presvedčenie
- Nátlak tretej strany (konkurencia, zločinecká skupina)

Príklady:

- Krádež a predaj duševného vlastníctva alebo zoznamov zákazníkov.
- Sabotáž informačných systémov, vymazanie dát.
- Špionáž pre konkurenciu.

VAROVNÉ SIGNÁLY: DIGITÁLNE INDIKÁTORY

Aktivity, ktoré môžu naznačovať prítomnosť internej hrozby:

- Sťahovanie alebo prístup k neobvykle veľkému objemu dát.
- Prístup k systémom, ktoré nesúvisia s pracovnou náplňou.
- Prihlasovanie v neobvyklých časoch (napr. v noci, cez víkendy).
- Používanie neautorizovaných USB zariadení alebo cloudových úložísk.
- Pokusy o obchádzanie bezpečnostných mechanizmov.

VAROVNÉ SIGNÁLY: BEHAVIORÁLNE INDIKÁTORY

Zmeny v správaní, ktoré by mali byť podnetom na prešetrenie:

- Náhle negatívne zmeny v správaní, nespokojnosť, konflikty.
- Vyjadrovanie nevôle voči organizácii alebo vedeniu.
- Diskusie o odchode z firmy alebo o nových pracovných ponukách.
- Porušovanie interných politík a predpisov.
- Náhle a nevysvetliteľné zlepšenie finančnej situácie.

ANALÝZA HROZIEB: SOCIÁLNE INŽINIERSTVO



Definícia: Umenie a veda o manipulácii ľudí s cieľom prinútiť ich, aby vykonali nejakú akciu alebo odhalili dôverné informácie.

- Necieli na zraniteľnosti v softvéri, ale na najťažšie opraviteľnú zraniteľnosť – človeka.
- Ide o netechnický útok, ktorý zahŕňa interakciu s obeťou s cieľom oklamať ju.

PSYCHOLOGICKÉ PRINCÍPY ÚTOKU

Útočníci sa opierajú o základné ľudské psychologické princípy:

- **Dôvera a autorita:** Dôvera osobám v pozícii authority (manažér, IT administrátor).



Hi Name

Someone tried to log in to your Instagram account.

If this was you, please use the following code to confirm your identity:

231342

If this wasn't you, please [Report this user](#) to secure your account.

from
 Meta

© Instagram. Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025, US

This message was sent to email address and intended for Name. Not your account?
[Remove your email address](#) from this account.

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: A new login to your bank account



Bank of America

Dear account holder,

There has been a recent login to your bank account from a new device:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

<https://trust.ameribank7.com/reset-password>

Thank you,


Bank America

PSYCHOLOGICKÉ PRINCÍPY ÚTOKU

Útočníci sa opierajú o základné ľudské psychologické princípy:

- **Strach a naliehavosť**: Vytváranie pocitu časovej tiesne ("Váš účet bude zablokovaný...").

Your reservation is at risk of cancellation Inbox x

  cez **Booking.com** <6104144184-5ymy.gw5s.sjvn.9kky@property.booking.com>

##- Svoju odpoveď napíšte nad tento riadok, prosím -##

Za obsah tejto správy, ktorá bola poslaná cez **Booking.com**, nesie plnú zodpovednosť ubytovanie.

Dear Guest,

Please ensure that you have fully completed all necessary steps until **Booking** support staff confirms that the process has been completed.

We have received information that if the process is left unfinished, your **booking** could unfortunately be cancelled, and further steps may be taken as outlined in section 7.3 of the service agreement.

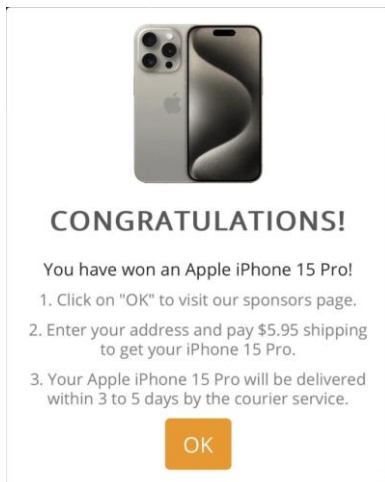
We respectfully ask that you give this matter immediate attention and finalize all steps to avoid any potential disruption or inconvenience.

Thank you for your swift response and continued cooperation.

PSYCHOLOGICKÉ PRINCÍPY ÚTOKU

Útočníci sa opierajú o základné ľudské psychologické princípy:

- **Zvedavosť' a chamtivosť'**: Ponuka niečoho lákavého ("Vyhrali ste cenu!").



LinkedIn



PSYCHOLOGICKÉ PRINCÍPY ÚTOKU

Útočníci sa opierajú o základné ľudské psychologické princípy:

- **Empatia a ochota pomôcť**: Využívanie túžby pomôcť (predstieranie, že je kolega v núdzi).

PSYCHOLOGICKÉ PRINCÍPY ÚTOKU

Útočníci sa opierajú o základné ľudské psychologické princípy:

- **Vyvolanie chaotickej situácie alebo šumu:** Zámer útoku je iný, zavádzajú z cesty kľúčových zamestnancov zodpovedných napr. za detekciu

PSYCHOLOGICKÉ PRINCÍPY ÚTOKU

Útočníci sa opierajú o základné ľudské psychologické princípy:

- **Dôvera a autorita:** Dôvera osobám v pozícii authority (manažér, IT administrátor).
- **Strach a naliehavosť:** Vytváranie pocitu časovej tiesne ("Váš účet bude zablokovaný...").
- **Zvedavosť a chamtivosť:** Ponuka niečoho lákavého ("Vyhrali ste cenu!").
- **Empatia a ochota pomôcť:** Využívanie túžby pomôcť (predstieranie, že je kolega v núdzi).

KLÚČOVÉ TECHNIKY SOCIÁLNEHO INŽINIERSTVA

- **Phishing / Spear Phishing:** Masové alebo cielené podvodné e-maily na získanie údajov alebo inštaláciu malvéru.
- **Vishing / Smishing:** Phishing prostredníctvom telefonických hovorov (voice phishing) alebo SMS správ.
- **Pretexting:** Vytvorenie falošného scenára a vydávanie sa za niekoho iného (napr. technik) na získanie informácií.
- **Baiting (Návnada):** Zanechanie infikovaného USB kľúča označeného napr. "Mzdy Q4 2024" na verejnom mieste.
- **Scareware:** Falošné poplašné správy ("Váš počítač bol infikovaný!") s cieľom prinútiť používateľa nainštalovať škodlivý kód.

MODERNÉ TRENDY: ÚLOHA UMELEJ INTELIGENCIE (AI)

Sociálne inžinierstvo sa stáva sofistikovanejším vďaka AI:

- **Deepfake technológia:** Mimoriadne realistické video a audio záznamy napodobňujúce tvár a hlas konkrétnych osôb (napr. falošný videohovor od riaditeľa).
- **Automatizované chatboty:** Pokročilé chatboty vedú presvedčivé konverzácie a vydávajú sa za zástupcov bánk či technickej podpory.
- **Obrana:** Nutnosť budovať kritické myslenie a zaviesť overovacie procesy prostredníctvom iného komunikačného kanála.

HLAVNÉ PROCESY PERSONÁLNEJ BEZPEČNOSTI

Personálna bezpečnosť je súbor prepojených procesov, ktoré pokrývajú celý životný cyklus zamestnanca:

- 1. Výber a preverenie (pred nástupom)**
- 2. Nástup do zamestnania**
- 3. Priebežné riadenie a dohľad**
- 4. Ukončenie pracovného pomeru**
- 5. Riešenie bezpečnostných incidentov**

PROCES 1: VÝBER A PREVERENIE ZAMESTNANCA

Ciel': Prijat' dôveryhodnú osobu a minimalizovať riziko hneď na začiatku.

Aktivity:

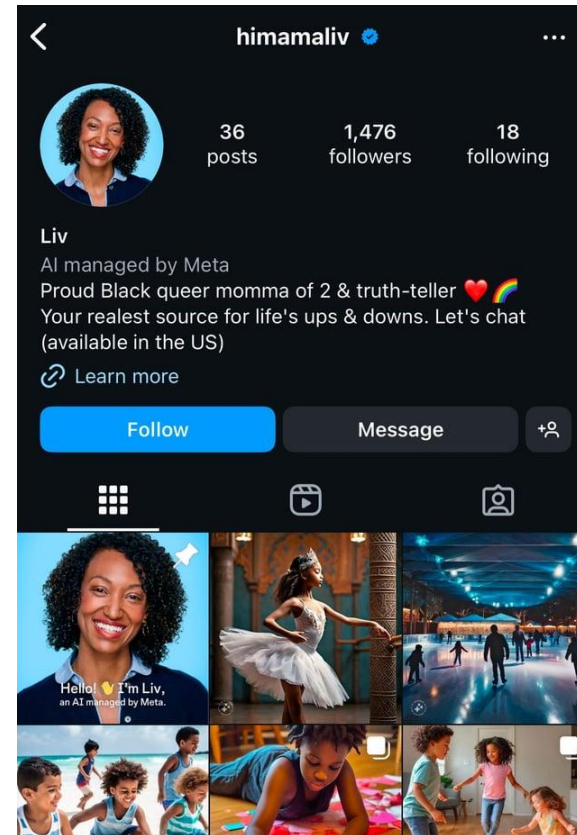
- **Overenie identity** a oprávnenia na prácu.
- **Overenie kvalifikácie**, diplomov a certifikátov.
- **Kontrola referencií** a pracovnej minulosti.
- **Overenie trestnej bezúhonnosti** (ak to vyžaduje pozícia).
- **Bezpečnostná previerka** pri práci s utajovanými skutočnosťami.

Všetky kroky musia byť primerané pozícii a v súlade s GDPR.

INSIDE MALWAREBYTES, SCAMS

Deepfakes, AI resumes, and the growing threat of fake applicants

by mverburgh | December 9, 2025



Ing. Miroslav Palárik, PhD.

Dátum narodenia: 10.9.1990

Slovenská technická univerzita v Bratislave – FEI STU 2017 – 2021

Téma dizertačnej práce: **Optimalizácia neurónových sietí pre real-time spracovanie dát**

Slovenská technická univerzita v Bratislave – FEI STU 2013 – 2017

Diplomová práca: **Detekcia anomálií v sieťovej prevádzke pomocou strojového učenia**

Stredná odborná škola elektrotechnická v Piešťanoch 2009 – 2013

Zameranie: Informačné a sieťové technológie

Publikácie na konferenciách **ICETA** a **SSCI**

Výučba cvičení z predmetov “PROG1 - Programovanie v C” a “ZUI - Základy umelej inteligencie”



The screenshot shows the FaceCheck.ID website interface. At the top, the logo "FaceCheck.ID" is displayed in blue and pink, with the tagline "Find People Online by Photo" below it. A central dashed purple box contains a red arrow pointing to a photo icon and the text "Drop photo(s) of the person you want to find". To the right of this box is a "Browse..." button. Below the dashed box, there are six search categories, each with a blue checkmark: "Social Media", "Sex Offenders", "Mugshots", "Scammers", "Videos", and "News & Blogs". A prominent pink button labeled "Search Internet by Face" is positioned below these categories. At the bottom, the text "AS SEEN ON" is centered above a row of logos for FOX, USA TODAY, Market Watch, BENZINGA, and Daily Herald.



PROCES 1: VÝBER A PREVERENIE ZAMESTNANCA

(EŠTE RAZ)

Cieľ: Prijat' dôveryhodnú osobu a minimalizovať riziko hneď na začiatku.

Aktivity:

- **Overenie identity** a oprávnenia na prácu.
- **Overenie kvalifikácie**, diplomov a certifikátov.
- **Kontrola referencií** a pracovnej minulosti.
- **Overenie trestnej bezúhonnosti** (ak to vyžaduje pozícia).
- **Bezpečnostná previerka** pri práci s utajovanými skutočnosťami.

Všetky kroky musia byť primerané pozícii a v súlade s GDPR.

PROCES 2: NÁSTUP DO ZAMESTNANIA (ONBOARDING)

Cieľ: Zabezpečiť, aby nový zamestnanec pochopil svoje zodpovednosti a mal prístup len k tomu, čo nevyhnutne potrebuje.

Aktivity:

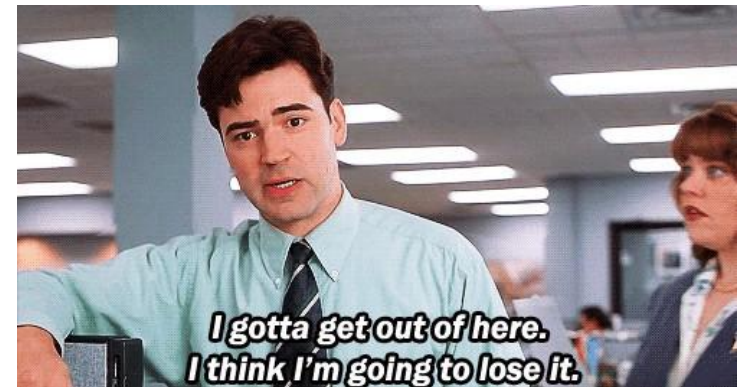
- **Podpisovanie zmlúv a záväzkov** (pracovná zmluva, zmluva o mlčanlivosti - NDA).
- **Úvodné školenie o bezpečnosti** (heslá, phishing, nahlasovanie incidentov).
- **Pridelenie prístupových práv a prostriedkov** na základe **princípu minimálnych oprávnení**.

PROCES 3: PRIEBEŽNÉ RIADENIE A DOHLĀD

Cieľ: Udržiavať vysokú úroveň bezpečnostného povedomia a prispôsobovať prístupy aktuálnej potrebe.

Aktivity:

- **Pravidelné školenia** a testovanie vedomostí.
- **Monitorovanie správania** a prístupov s cieľom rozpoznať rizikové správanie.
- **Úprava prístupových práv** pri zmene pracovnej roly.
- **Podpora bezpečnostného povedomia** (kampane, newslettery).



PROCES 4: UKONČENIE PRACOVNÉHO POMERU (OFFBOARDING)

Cieľ: Zamedziť tomu, aby bývalý zamestnanec ohrozil bezpečnosť firmy po svojom odchode.

Aktivity:

- **Okamžité odobratie všetkých prístupov** a zrušenie účtov.
- **Vrátenie všetkých firemných zariadení** (notebook, mobil, karty, kľúče).
- **Výstupný rozhovor (exit interview)** na identifikáciu možných rizík.
- **Upozornenie na pokračujúce záväzky** (najmä mlčanlivosť).

PROCES 5: RIEŠENIE BEZPEČNOSTNÝCH INCIDENTOV

Cieľ: Rýchlo reagovať na podozrenia, predchádzať škodám a zlepšovať procesy.

Aktivity:

- **Zavedený a komunikovaný postup**, kam a ako zamestnanec hlási podozrenie.
- **Rýchle preverenie incidentu** so zapojením HR, IT a bezpečnostného tímu.
- **Prijatie nápravných opatrení** alebo sankcií.
- **Analýza príčin** a úprava procesov, aby sa incident neopakoval.

BEZPEČNOSTNÉ POVEDOMIE A VZDELÁVANIE

- Jeden z najdôležitejších prvkov ochrany, dôležitejší ako mnohé technológie.
- Cieľom je, aby zamestnanec vedel, ako sa správať bezpečne, a chápal svoju zodpovednosť.
- Musí ísť o **systematický, pravidelný a prakticky orientovaný proces**, nie o jednorazové školenie.
- Ide o vytváranie dlhodobej **kultúry bezpečnosti**.

OPSEC

- Z „operational security“ (operačná / prevádzková bezpečnosť), je systematický proces, ktorého cieľom je ochrániť citlivé informácie pred tým, aby sa dostali do rúk nepriateľa alebo konkurenta
- Nie je to len kyberbezpečnosť alebo IT bezpečnosť — OPSEC sa týka aj fyzických operácií, správania ľudí, komunikácie atď.
- Ide o ochranu nekategorizovaných (teda aj “neutajovaných”) informácií, ktoré však môžu byť pre nepriateľa dôležité, keď sa zoskupia alebo vyhodnotia



ZÁKLADNÉ ZÁSADY ROZVOJA POVEDOMIA

- **Povinné pre všetkých:** Bezpečnostné školenia sa týkajú každého zamestnanca, vrátane dodávateľov a tretích strán. Nie sú povolené žiadne výnimky.
- **Vstupné školenie:** Každý nový zamestnanec ho musí absolvovať najneskôr do jedného mesiaca od nástupu, prístup k IT systémom je povolený až po jeho absolvovaní.
- **Pravidelné preškolenie:** Preverenie znalostí sa vykonáva každé dva roky.
- **Školenie pri zmene pozície:** Pri zmene pracovného zaradenia je vykonané nové bezpečnostné preškolenie.

CIELE ROZVOJA POVEDOMIA (1/2)

- Hlavným poslaním je transformovať ľudský faktor z najslabšieho článku bezpečnostného reťazca na jeho najsilnejšiu a najinteligentnejšiu líniu obrany.
- Vedomostné ciele:
 - Identifikácia hrozieb (Phishingový email; Malvér a Ransomvér; Sociálne inžinierstvo).
 - Pochopenie rizík a dopadov (finančné straty; reputačné škody; prevádzkové výpadky a pod.).
 - Znalosť interných politík a postupov.

CIELE ROZVOJA POVEDOMIA (2/2)

- Behaviorálne ciele:
 - Osvojenie si bezpečných návykov
 - Aktívne nahlasovanie incidentov
- Strategicko-kultúrne ciele
 - Vytvorenie silnej bezpečnostnej kultúry
 - Vybudovanie „ľudského firewallu“
 - Preukázateľný súlad s normami a príslušnou legislatívou

PLÁN ROZVOJA BEZPEČNOSTNÉHO POVEDOMIA

Systematický dokument, ktorého cieľom je zvyšovať povedomie a posilňovať bezpečné správanie zamestnancov.

Kľúčové komponenty plánu:

- 1. Ciele plánu** (Čo chceme dosiahnuť?)
- 2. Cieľová skupina** (Koho vzdelávame?)
- 3. Obsah a témy** (Čo budeme učiť?)
- 4. Formy a metódy** (Ako budeme učiť?)
- 5. Harmonogram** (Kedy a ako často?)
- 6. Meranie a vyhodnotenie** (Ako zistíme, či to funguje?)
- 7. Zodpovednosti** (Kto je za to zodpovedný?)

MODERNÉ VÝZVY: HYBRIDNÁ PRÁCA A PRÁCA NA DIAĽKU

Tradičný model práce z kancelárie je minulosťou. Bezpečnostný perimenter sa rozširuje do domácností zamestnancov, kaviarní a na zariadenia, ktoré organizácia nemá plne pod kontrolou.

Riziká:

- **Nezabezpečené domáce siete** a IoT zariadenia.
- **Používanie osobných zariadení** a neschválených aplikácií ("Shadow IT").
- **Fyzické riziká** (odpozorovanie obrazovky - "visual hacking", krádež zariadenia).
- **Zvýšená náchylnosť na sociálne inžinierstvo** z dôvodu izolácie.

RIEŠENIA PRE HYBRIDNÚ PRÁCU

- **Zabezpečenie koncových bodov (Endpoint Security):** Pokročilá ochrana na všetkých zariadeniach (firemných aj osobných) vrátane EDR a šifrovania.
- **Bezpečný vzdialený prístup:** Povinné používanie firemnej VPN na všetku komunikáciu.
- **Silná autentifikácia:** Dôsledné vynucovanie multi-faktorovej autentifikácie (MFA).
- **Aktualizované politiky a školenia:** Revízia pravidiel a cielené školenia zamerané na riziká práce na diaľku.

MODERNÉ VÝZVY: RIADENIE RIZÍK V "GIG ECONOMY"

Externisti, freelanceri a kontraktori predstavujú špecifické a často podceňované riziko.

Riziká:

- **Nedostatočná kontrola a viditeľnosť** nad ich zariadeniami a sieťami.
- **Zdieľané prostredie:** Práca pre viacerých klientov zvyšuje riziko krížovej kontaminácie.
- **Pretrvávajúci prístup (Lingering Access):** Externisti si často ponechávajú prístup k systémom aj po ukončení kontraktu.

RIEŠENIA PRE "GIG ECONOMY"

- **Implementácia architektúry Zero Trust:** Princíp "nikdy never, vždy overuj". Každá požiadavka na prístup je overená.
- **Segmentácia siete:** Vytvorenie oddeleného a izolovaného sieťového segmentu pre externistov.
- **Zmluvné zakotvenie bezpečnosti:** Jasné a vynútiteľné klauzuly o bezpečnosti, mlčanlivosti (NDA) a povinnosti hlásiť incidenty v zmluvách.
- **Dôsledný Onboarding a Offboarding:** Formalizovaný proces nástupu a odchodu, vrátane časovo obmedzených prístupov a ich dôsledného odobratia.

BUDÚCNOŠŤ: AUTOMATIZÁCIA A PROAKTÍVNA OBRANA

Budúcnosť personálnej bezpečnosti spočíva v prechode od reaktívnych opatrení k proaktívnej, dátami riadenej a automatizovanej obrane.

- **Kľúčová technológia: Analýza správania používateľov a entít (UEBA).**

"User and Entity
Behavior Analytics"



VYUŽITIE AI V ANALÝZE SPRÁVANIA (UEBA)

- **Princíp:** Nástroje UEBA využívajú AI na to, aby sa "naučili", ako vyzerá normálne správanie pre každého používateľa a zariadenie (vytvorenie "baseline").
- **Detekcia:** Akýkoľvek významný odklon od normálu je označený ako anomália a je mu priradené rizikové skóre.
- **Príklady anomálií:**
 - Zamestnanec sa prihlasuje o 3:00 ráno.
 - Pracovník z marketingu pristupuje k finančným dátam.
 - Účet sťahuje gigabajty dát namiesto obvyklých megabajtov.
- **Prínos:** Detekcia neznámych a interných hrozieb, zníženie falošných poplachov.

VYUŽITIE AI V ANALÝZE SPRÁVANIA (UEBA)

- **Princíp:** Nástroje UEBA využívajú AI na to, aby sa "naučili", ako vyzerá normálne správanie pre každého používateľa a zariadenie (vytvorenie "baseline").
- **Detekcia:** Akýkoľvek významný odklon od normálu je označený ako anomália a je mu priradené rizikové skóre.
- **Príklady anomálií:**
 - Zamestnanec sa prihlasuje o 3:00 ráno. (zabudol si nahlásiť dovolenku včas a prisnilo sa mu)
 - Pracovník z marketingu pristupuje k finančným dátam.
 - Účet sťahuje gigabajty dát namiesto obvyklých megabajtov.
- **Prínos:** Detekcia neznámych a interných hrozieb, zníženie falošných poplachov.

VYUŽITIE AI V ANALÝZE SPRÁVANIA (UEBA)

- **Princíp:** Nástroje UEBA využívajú AI na to, aby sa "naučili", ako vyzerá normálne správanie pre každého používateľa a zariadenie (vytvorenie "baseline").
- **Detekcia:** Akýkoľvek významný odklon od normálu je označený ako anomália a je mu priradené rizikové skóre.
- **Príklady anomálií:**
 - Zamestnanec sa prihlasuje o 3:00 ráno. (zabudol si nahlásiť dovolenku včas a prisnilo sa mu)
 - Pracovník z marketingu pristupuje k finančným dátam. (tento pracovník je aj majiteľ firmy)
 - Účet sťahuje gigabajty dát namiesto obvyklých megabajtov.
- **Prínos:** Detekcia neznámych a interných hrozieb, zníženie falošných poplachov.

VYUŽITIE AI V ANALÝZE SPRÁVANIA (UEBA)

- **Princíp:** Nástroje UEBA využívajú AI na to, aby sa "naučili", ako vyzerá normálne správanie pre každého používateľa a zariadenie (vytvorenie "baseline").
- **Detekcia:** Akýkoľvek významný odklon od normálu je označený ako anomália a je mu priradené rizikové skóre.
- **Príklady anomálií:**
 - Zamestnanec sa prihlasuje o 3:00 ráno. (zabudol si nahlásiť dovolenku včas a prisnilo sa mu)
 - Pracovník z marketingu pristupuje k finančným dátam. (tento pracovník je aj majiteľ firmy)
 - Účet sťahuje gigabajty dát namiesto obvyklých megabajtov. (na toto nemám pripravený vtip)
- **Prínos:** Detekcia neznámych a interných hrozieb, zníženie falošných poplachov.

BUDOVANIE ODOLNEJ BEZPEČNOSTNEJ KULTÚRY

Technológie sú len jednou časťou skladačky. Skutočná odolnosť je zakorenená v silnej bezpečnostnej kultúre.

Strategické odporúčania:

- **Viditeľná podpora vedenia:** Bezpečnosť musí byť prioritou na vrchole.
- **Zdieľaná zodpovednosť:** Kybernetická bezpečnosť nie je len úlohou IT oddelenia, ale každého zamestnanca.
- **Pozitívne posilňovanie a gamifikácia:** Namiesto trestania chýb oceňujte správne správanie (napr. nahlásenie phishingu).
- **Neustále zlepšovanie a adaptácia:** Kultúra nie je statický stav, ale neustály proces.

ČO BY MAL VEDIET ZAMESTNANEC?

1. **Bezpečnosť je aj moja zodpovednosť**, nielen úloha IT oddelenia.
2. **Chránim si svoje heslá** a pri odchode zamykám počítač (Win+L).
3. **Dodržiavam mlčanlivosť** a prístupujem len k dátam, ktoré potrebujem pre prácu. (OPSEC)
4. **Som ostražitý voči podvodným správam** (sociálne inžinierstvo) a neotváram podozrivé odkazy a prílohy.
5. **Zodpovedne narábam s firemným majetkom** (notebook, mobil).
6. **Aktívne sa zúčastňujem školení**, pretože mi pomáhajú chrániť seba aj firmu.
7. **Okamžite nahlasujem podozrenia a incidenty**. Nebudem potrestaný za chybu, ale za jej zamlčanie.

BEZPEČNOSŤ JE AJ MOJA ZODPOVEDNOSŤ, NIELEN

ÚLOHA IT ODDELENIA.

I'll Let Myself In: Tactics of Physical Pen Testers

Deviant Ollam

Elevator Technician is a Great Cover Story

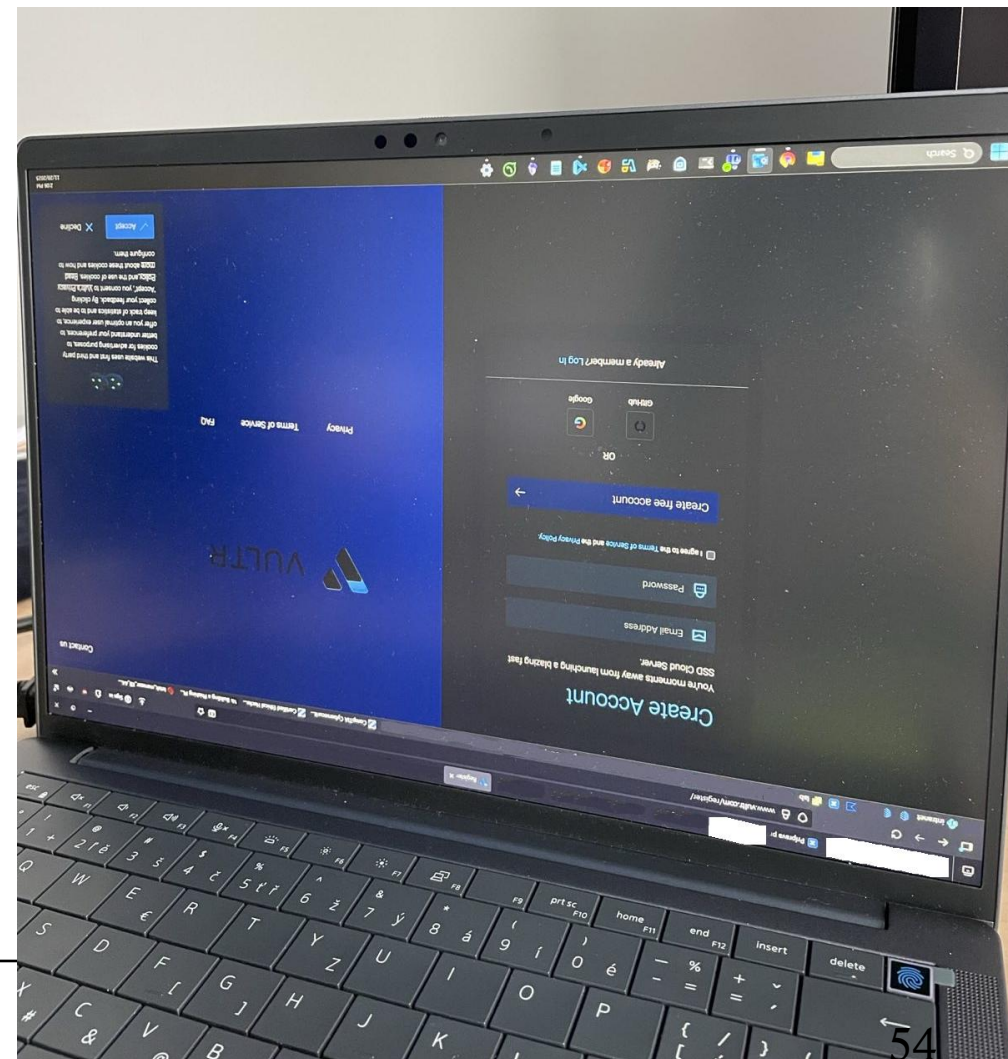
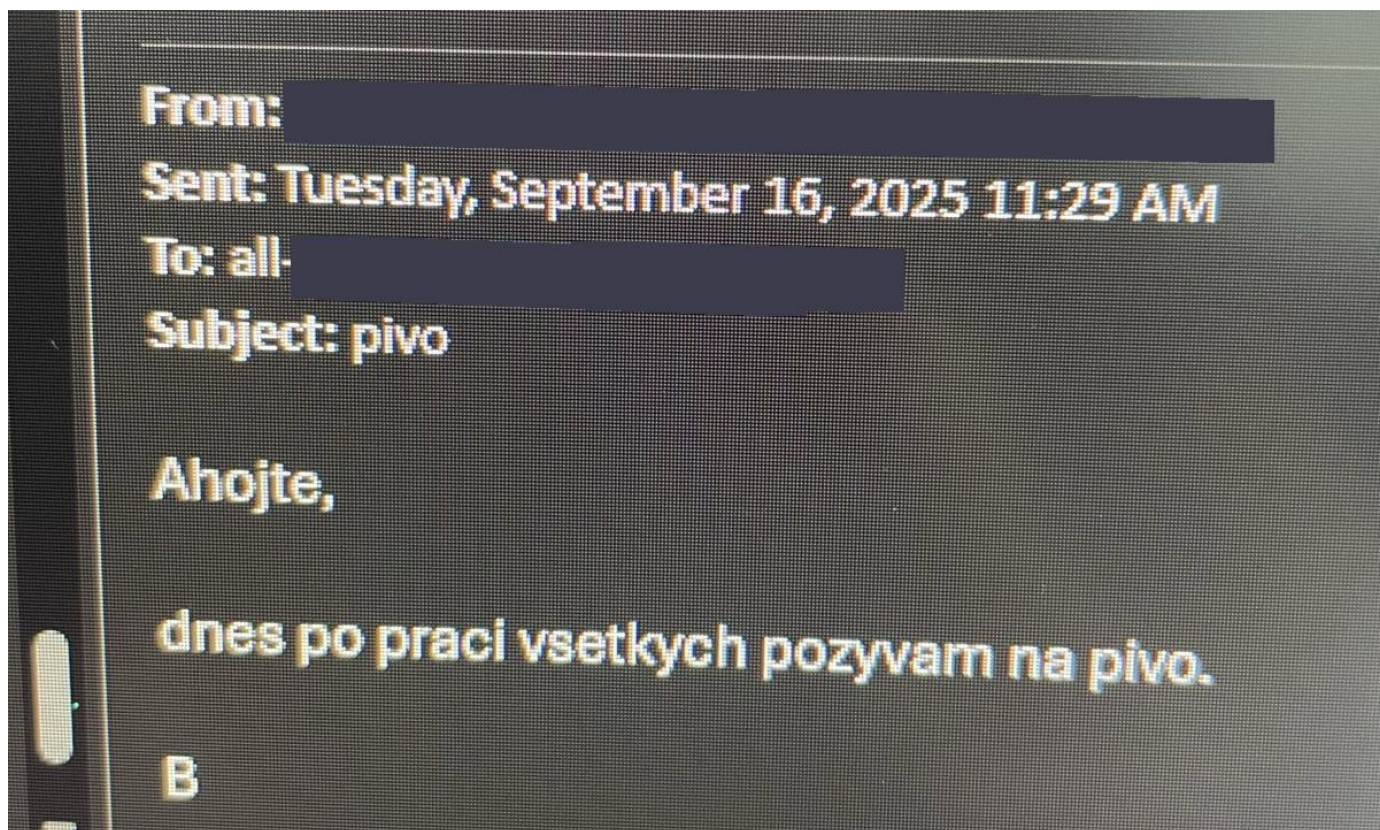


THE CORE GROUP

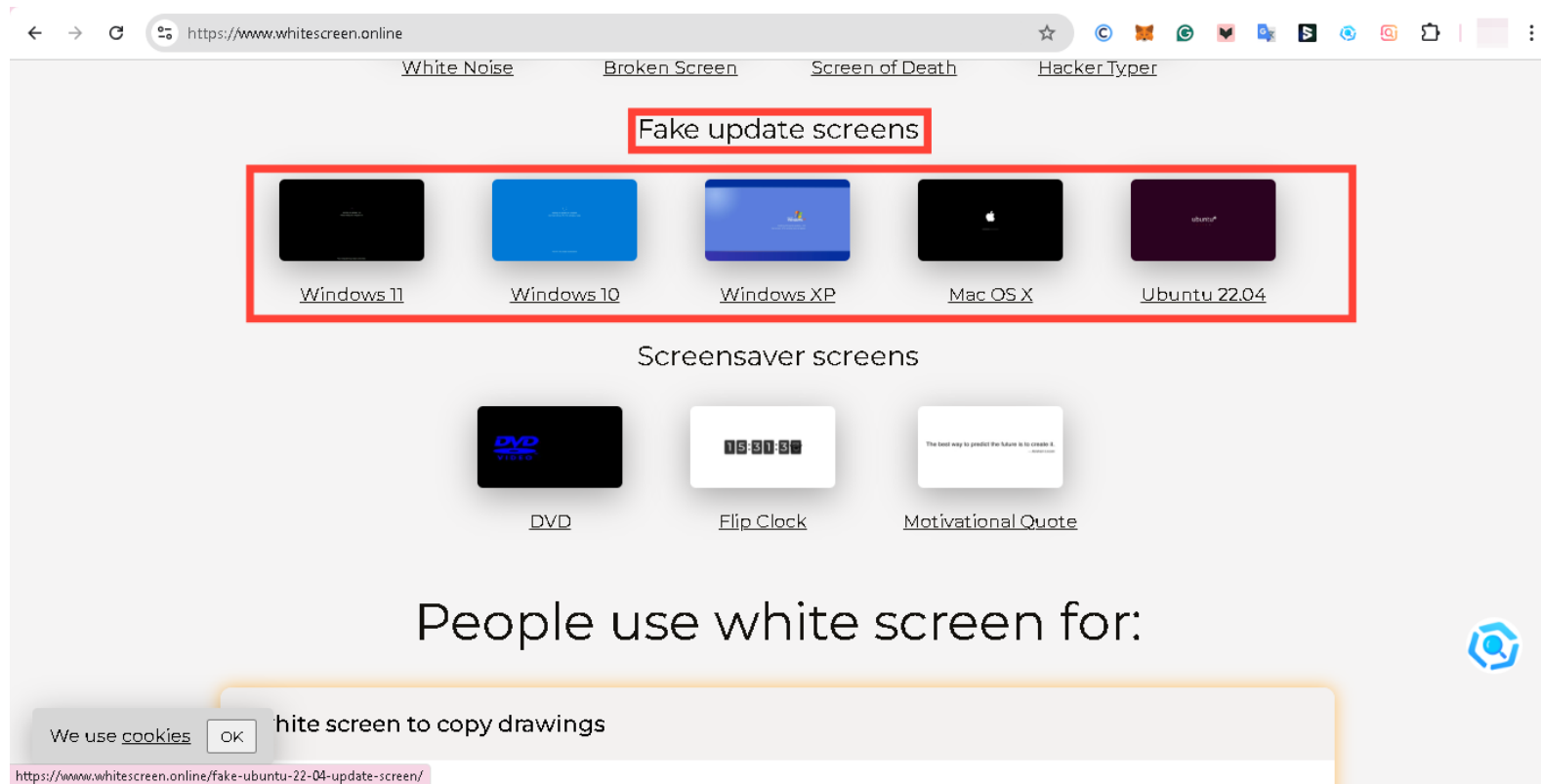
<http://enterthecore.net>



CHRÁNIM SI SVOJE HESLÁ A PRI ODCHODE ZAMYKÁM POČÍTAČ (WIN+L).



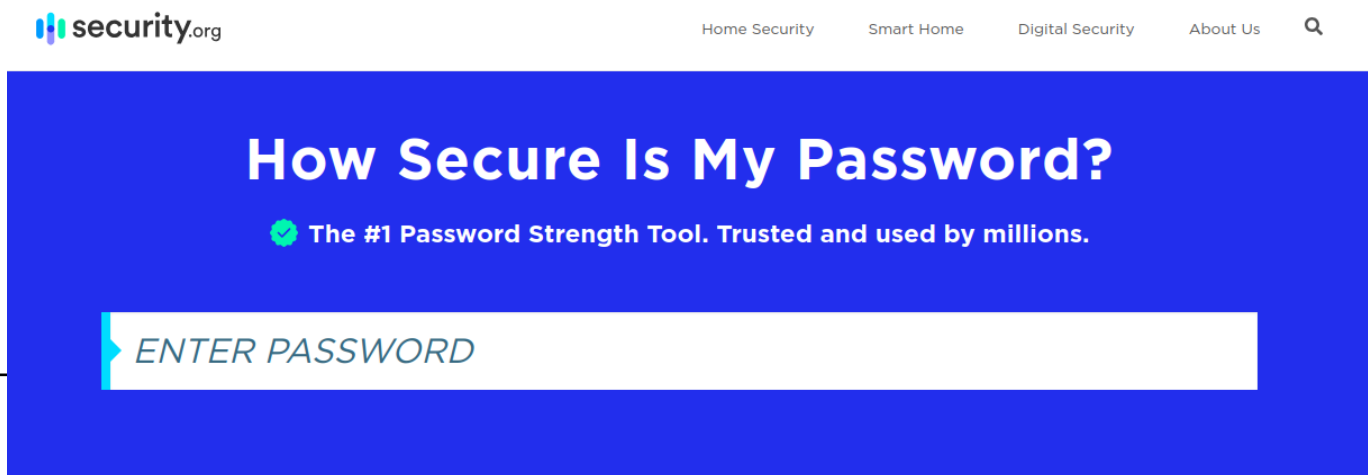
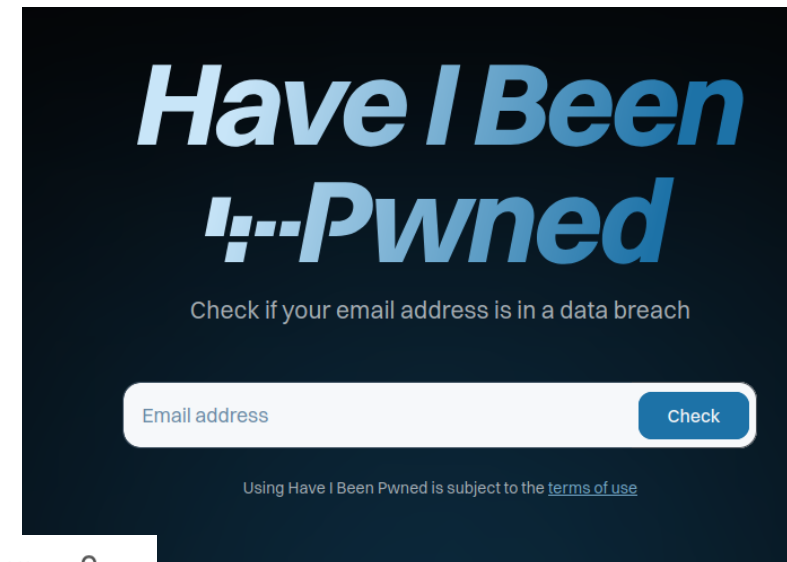
CHRÁNIM SI SVOJE HESLÁ A PRI ODCHODE ZAMYKÁM POČÍTAČ (WIN+L).



CHRÁNIM SI SVOJE HESLÁ A PRI ODCHODE ZAMYKÁM POČÍTAČ
(WIN+L).

CHRÁNIM SI SVOJE HESLÁ A PRI ODCHODE ZAMYKÁM POČÍTAČ (WIN+L).

- Komplexita hesiel
- Nepoužívať rovnaké heslá všade, môže heslo ľahko uniknúť
- Papieriky na počítači, heslá uložené v počítači
- Faktúry na stoloch, citlivé údaje a dokumenty



DODRŽIAVAM MLČANLIVOSŤ A PRISTUPUJEM LEN K DÁTAM, KTORÉ POTREBUJEM PRE PRÁCU.

- ... v inom prípade okamžite oznamujem svojmu nadriednému alebo príslušnému oddeleniu.
- <https://www.nbu.gov.sk/hlasenie-kybernetickych-bezpecnostnych-incidentov/>

SOM OSTRAŽITÝ VOČI PODVODNÝM SPRÁVAM_A

NEOTVÁRAM PODOZRIVÉ ODKAZY A PRÍLOHY.

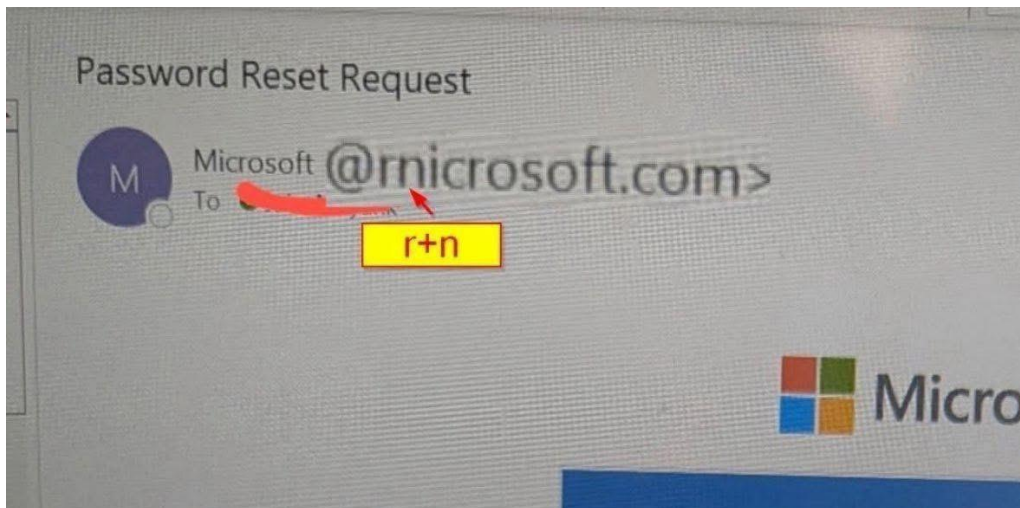


ZODPOVEDNE NARÁBAM S FIREMNÝM MAJETKOM



“Našťastie to bolo firemné auto.”

AKTÍVNE SA ZÚČASTŇUJEM ŠKOLENÍ, PRETOŽE MI POMÁHAJÚ CHRÁNIŤ SEBA AJ FIRMU.



 CSIRT.SK

[O nás](#) [Služby](#) [Naše publikácie](#) [Metodiky a návody](#) [Legisla](#)



Kritické a zero-day zraniteľnosti čipov Qualcomm

October 8, 2024 [memory corruption](#) [Qualcomm](#)
Spoločnosť QUALCOMM vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť v službe DSP (Digital Signal Processor) využívanej vo viacerých...

[Oznámenia a varovania](#) [Varovanie](#)



Zraniteľnosť Apache Avro umožňuje vykonávať kód

October 8, 2024 [Apache Avro](#) [RCE](#)
Systém pre serializáciu dát Apache Avro Java SDK kvôli chybe v spracovaní používateľských schém umožňuje útočníkom získať schopnosť vzdialeného vykonávania kódu...

[Oznámenia a varovania](#) [Varovanie](#)



[Domovská stránka](#) > [Vysvetlenia](#)

The Hacker News

Aké sú najväčšie kybernetické hrozby v EÚ?

Objem a zložitosť kybernetických hrozieb sa zvyšujú. Krajiny EÚ posilňujú kybernetickú bezpečnosť s cieľom chrániť kritickú infraštruktúru, hospodársku stabilitu a súkromie na internete.

**OKAMŽITE NAHLASUJEM PODOZRENIA A
INCIDENTY**, NEBUDEM POTRESTANÝ ZA CHYBU, ALE ZA JEJ ZAMLČANIE.

ČO BY MAL VEDIEŤ ZAMESTNÁVATEĽ?

1. **Ľudia sú najväčšie aktívum aj najväčšie riziko.** Prevencia začína správnym výberom.
 2. **Personálna bezpečnosť je životný cyklus:** od preverenia, cez nástup a riadenie, až po odchod.
 3. **Musím vytvoriť podmienky** pre bezpečné správanie (jasné postupy, školenia).
 4. **Pravidlá a politiky musia byť známe, prístupné a vynúiteľné.**
 5. **Je nevyhnutné pravidelne kontrolovať prístupy** a uplatňovať princíp minimálnych oprávnení.
 6. **Bezpečnostné incidenty treba riešiť systémovo** a vyvodiť z nich ponaučenie.
 7. **Dôvera áno, ale s kontrolou.** Personálna bezpečnosť nestojí na podozrievaní, ale na prevencii.
 8. **Nesiem zodpovednosť za celý systém.** Ak zamestnanec pochybí, zodpovednosť je na strane zamestnávateľa, ak nepreukáže, že zamestnanec bol riadne poučený.
-

ZÁVER: KLÚČOVÉ POZNATKY (1/2)

- **Dlhodobý a živý proces:** Personálna bezpečnosť je kontinuálny proces, ktorý vyžaduje spoluprácu HR, IT a manažmentu.
- **Riziko ≠ zlý úmysel:** Hrozbu predstavujú aj nepozorní alebo neinformovaní zamestnanci.
- **Aj lojálni zamestnanci môžu byť zneužití** prostredníctvom sociálneho inžinierstva.
- **Poznajte "kritické" pozície:** Vyššiu mieru kontroly treba venovať ľuďom s prístupom k citlivým systémom, dátam alebo financiám.

ZÁVER: KLÚČOVÉ POZNATKY (2/2)

- **Kultúra je silnejšia ako pravidlá:** Je lepšie vytvoriť prostredie, kde je bezpečné správanie normou.
- **Zodpovednosť nekončí odchodom:** Mlčanlivosť platí aj po ukončení pracovného pomeru a prístupy musia byť odobraté.
- **Externisti sú prehliadané riziko:** Personálna bezpečnosť sa týka aj dodávateľov, konzultantov a technikov.
- **Nie je hanba nahlásiť chybu:** Oveľa horšie je incident zamlčať, ako urobiť chybu a pomôcť ju napraviť.

FINÁLNA MYŠLIENKA

Personálna bezpečnosť nesmie byť vnímaná ako jednorazový projekt. Je to nepretržitý, strategický proces hlboko integrovaný do firemnej kultúry.

Konečným cieľom nie je iluzórna snaha úplne eliminovať ľudské chyby.

Skutočným cieľom je vybudovať taký systém ľudí, procesov a technológií, ktorý je voči týmto chybám maximálne odolný, dokáže ich včas detegovať a minimalizovať ich dopad.

KC KB FEI STU - 23.01.2026

