ZÁKLADY KYBERNETICKÉ BEZPEČNOSTI V PRAXI

(osnova jednodenního školení – 4 hodin + diskuze)

Cílová skupina: zaměstnanci veřejné správy, firemní pracovníci, uživatelé IT systémů bez hluboké technické znalosti

Forma: kombinace přednášky a praktického nácviku (4 h teorie + diskuze)

Cíl kurzu: Zvýšit povědomí o kybernetických hrozbách, správném chování a povinnostech podle NIS2, včetně praktických doporučení pro práci z domova a používání vlastních zařízení.

---

1. Úvod do kybernetické bezpečnosti

- Co je kybernetická bezpečnost a proč se týká každého
- Reálné příklady útoků na firmy a úřady
- Role uživatele v systému ochrany

2. Legislativa a rámec NIS2

- Směrnice NIS2 a její dopad na zaměstnance
- Novelizovaný zákon o kybernetické bezpečnosti (hlavní změny)
- Povinnosti zaměstnanců vs. odpovědnost organizace
- Hlášení incidentů a bezpečnostní role

3. Nejčastější hrozby a zranitelnosti

- Phishing, ransomware, sociální inženýrství
- Úniky dat a nedbalost
- Fyzická bezpečnost a přístup k zařízením

4. Zásady bezpečného chování v digitálním prostředí

- Pravidla pro tvorbu a správu hesel
- Dvoufaktorové ověřování (MFA)
- Rozpoznání podezřelých emailů, odkazů a příloh
- Bezpečnost na internetu a sociálních sítích

5. BYOD – Bring Your Own Device

- Výhody a rizika BYOD z pohledu zaměstnance i organizace
- Politika BYOD a co musí zaměstnanec vědět
- Ochrana dat a zařízení, oddělení osobních a firemních údajů
- Práce s firemními daty na vlastních telefonech/noteboocích

6. Bezpečný home office

- Bezpečné připojení (VPN, šifrování)
- Pravidla pro sdílený přístup a zařízení v domácnosti
- Rizika při práci ve veřejných sítích

- Ochrana před odposlechem, ztrátou zařízení, keyloggery

7. Praktické ukázky a simulace

- Rozpoznání podvodných e-mailů (phishing test)
- Cvičný incident: Jak nahlásit bezpečnostní událost
- Zabezpečení mobilního zařízení (nastavení PIN, biometrie, šifrování)
- Vyzkoušení 2FA, práce s bezpečnostními klíči

8. Bezpečné nastavení domácí Wi-Fi a práce z domova

- Kontrola a zabezpečení domácí sítě
- Oddělené sítě pro hosty, aktualizace routeru
- Vytvoření pravidel pro domácí digitální hygienu

9. Cvičení – BYOD modelová situace

- Simulace: připojení vlastního zařízení do firemní sítě
- Kontrola bezpečnostních zásad, školení zaměstnanců
- Hodnocení rizik a správné chování v konkrétním scénáři

10. Shrnutí a zpětná vazba

- Kvíz/review klíčových bodů kurzu
- Diskuze: Jak mohu přispět k vyšší kybernetické bezpečnosti?
- Předání doporučení a podpůrných materiálů (checklisty, infografiky)

Výstupní materiály pro účastníky

- Základní příručka „Digitální hygiena zaměstnance“
- Poster: „10 zásad bezpečné práce z domova“
- BYOD checklist
- Vzor postupu pro hlášení incidentu
- Mini-kvíz pro opakování

DIGITERRA

Digitální hygiena zaměstnance

Základní příručka pro bezpečné každodenní používání IT v práci i doma

V souladu s NIS2 a zákonem o kybernetické bezpečnosti

---

1. Co je digitální hygiena?

Digitální hygiena je soubor návyků a pravidel, která chrání vaše zařízení, účty i citlivé informace před zneužitím. Stejně jako si myjeme ruce, i v digitálním světě potřebujeme pravidelně „čistit“ a chránit svá data.

---

2. 10 zásad digitální hygieny zaměstnance

1️⃣ Používejte silná a jedinečná hesla

- Každý účet = jiné heslo
- Používejte správce hesel (např. Bitwarden, KeePass, 1Password)
- Nikdy si hesla nezapisujte na papír v blízkosti PC

2️⃣ Aktivujte dvoufázové ověření (2FA)

- Ideálně pomocí mobilní aplikace nebo hardwarového klíče
- Nejen pro e-mail, ale i pro přístup do firemních systémů

3️⃣ Aktualizujte systém a aplikace

- Zapněte automatické aktualizace
- Aktualizujte také antivir, prohlížeče a doplňky

4️⃣ Zamykání zařízení při odchodu

- Vždy uzamkněte obrazovku, i při krátkém odchodu od počítače
- Na mobilních zařízeních nastavte PIN, gesto nebo biometrické ověření

5️⃣ Pozor na phishing a podvody

- Neklikejte na odkazy v podezřelých e-mailech
- Nezadávejte přihlašovací údaje na neznámé nebo podezřelé weby
- Hlaste podezřelé zprávy IT oddělení

6️⃣ Oddělujte pracovní a osobní zařízení

- Nepoužívejte firemní notebook pro soukromé účely a naopak
- Pokud používáte vlastní zařízení (BYOD), respektujte bezpečnostní pravidla

7️⃣ Bezpečné připojení

- Při práci mimo kancelář vždy používejte VPN
- Vyhněte se veřejným Wi-Fi sítím bez ochrany

8️⃣ Zálohujte důležitá data

- Firemní data zálohujte na určené firemní úložiště, ne na osobní disk
- Pravidelně kontrolujte přístup k zálohám

9️⃣ Ověřujte si aplikace a přílohy

- Nestahujte aplikace z neznámých zdrojů
- Neotvírejte přílohy z neznámých e-mailů, ani pokud „vypadají důvěryhodně“

🔟 Hlášení incidentů

- V případě podezření na únik dat, napadení zařízení nebo neobvyklé chování **okamžitě kontaktujte IT nebo bezpečnostní tým**

---

3. BYOD a home office – zvláštní pozornost

Používáte vlastní zařízení pro práci?

- Instalujte doporučený bezpečnostní software
- Šifrujte disk a nastavte silné zabezpečení přístupu
- Nepůjčujte zařízení dětem nebo členům rodiny

Pracujete z domova?

- Používejte VPN a aktuální antivir
- Pracujte v odděleném prostoru, pokud možno bez přístupu ostatních
- Nepoužívejte firemní účty v osobním prohlížeči

---

4. Co dělat v případě bezpečnostního incidentu?

1. **Neklikejte dál, nepokračujte v práci.**
2. **Odpojte zařízení od internetu (Wi-Fi, kabel).**
3. **Kontaktujte IT / bezpečnostního správce.**
4. **Popište situaci – co se stalo, co jste udělali, co se zobrazilo.**

BONUS: Rychlý checklist (pro tisk)

✅ Zamknul/a jsem si zařízení při odchodu?

✅ Pracuji z bezpečné sítě a s aktualizovaným softwarem?

✅ Nezadal/a jsem citlivé údaje na podezřelé stránce?

✅ Všechna hesla mám uložená bezpečně?

✅ Hlásím incidenty a podezření bez odkladu?

DIGITERRA

10 zásad bezpečné práce z domova

Pracujte odkudkoli – ale bezpečně!

✅ 1. Používejte zabezpečené připojení (VPN)

Připojujte se ke všem firemním systémům přes firemní VPN – šifruje komunikaci a chrání přístupová data.

✅ 2. Aktualizujte zařízení i software

Udržujte operační systém, aplikace i antivirový program vždy aktuální. Zastaralý software je snadný cíl.

✅ 3. Zabezpečte domácí Wi-Fi síť

Změňte výchozí heslo k routeru, nastavte silné šifrování (WPA3/WPA2) a vypněte přístup pro neznámá zařízení.

✅ 4. Zamykání zařízení při každém odchodu

I doma platí: když odcházíte od počítače, stiskněte *Win+L* nebo použijte zámek obrazovky.

✅ 5. Oddělujte osobní a pracovní aktivity

Na firemním zařízení neinstalujte osobní software ani neprohlížejte neznámé weby.

✅ 6. Buďte opatrní při práci ve sdíleném prostředí

Zajistěte, aby obrazovka nebyla na očích ostatním členům domácnosti. Používejte ochranu obrazovky nebo sluchátka.

✅ 7. Zacházejte s citlivými daty jako v kanceláři

Netiskněte důvěrné dokumenty bez zabezpečeného úložiště, nepřenášejte data nešifrovaně a nic nesdílejte přes osobní účty.

✅ 8. Pozor na phishing a falešné zprávy

Kyberzločinci cílí na vzdálené pracovníky. Nepodléhejte tlakům v e-mailech – ověřujte si identity odesílatelů.

✅ 9. Pravidelně zálohujte důležitá data

Zálohujte na firemní cloud nebo zabezpečený externí disk, nikoli na domácí úložiště bez šifrování.

✅ 10. Vědět, co dělat při incidentu

Zaznamenejte si kontakt na IT podporu. Podezřelé chování systému = ihned odpojit od sítě a nahlásit.

Pamatujte:

Vaše domácí pracoviště je prodloužením firemní kanceláře.

Co byste si nedovolili v práci, nedělejte ani doma.

DIGITERRA

BYOD – bezpečnostní checklist pro zaměstnance

Ověřte si, že vaše zařízení je připravené pro bezpečnou práci

1. Zabezpečení zařízení

☐ Zařízení je chráněno silným heslem, PINem nebo biometrikou

☐ Obrazovka se automaticky uzamkne po nečinnosti (max. 5 minut)

☐ V zařízení je zapnuto **šifrování disku** (např. BitLocker, FileVault, Android/iOS default)

☐ Zařízení je chráněno antivirem / bezpečnostní aplikací

☐ Je povoleno **vzdálené vymazání** (pro případ ztráty/krádeže)

2. Aktualizace a software

☐ Operační systém je **aktuální** – automatické aktualizace jsou zapnuté

☐ Pracovní aplikace (e-mail, VPN, kancelářský software) jsou pravidelně aktualizované

☐ V zařízení nejsou instalovány neověřené nebo nelegální aplikace

☐ Používám **oddělený pracovní profil nebo kontejner** (např. Android Work Profile, MDM řešení)

☐ Firemní data nejsou ukládána na osobní cloudové účty (Google Drive, Dropbox apod.)

3. Připojení a přístup

☐ K firemní síti se připojuji **výhradně přes zabezpečené VPN**

☐ Připojuji se jen z důvěryhodných a zabezpečených Wi-Fi sítí

☐ Mám aktivované **dvoufaktorové ověření (2FA)** pro přístup do všech důležitých systémů

☐ Nepoužívám sdílené účty nebo hesla – přístupy jsou **individuální a chráněné**

4. Soukromí a osobní život

☐ Pracovní účet je oddělený od osobního (např. v e-mailovém klientu)

☐ Zařízení **nepoužívají jiné osoby** (ani členové rodiny) pro práci s firemními daty

☐ Pracovní data nezálohuji na osobní flash disky, externí disky nebo osobní cloud

☐ Při ztrátě nebo podezření na zneužití zařízení vím, **koho kontaktovat a jak nahlásit incident**

5. Povědomí a odpovědnost

☐ Znám pravidla BYOD ve své organizaci a podepsal/a jsem souhlas s jejich dodržováním

☐ Absolvoval/a jsem základní školení kybernetické bezpečnosti

☐ Vím, že i při používání vlastního zařízení musím chránit firemní data jako na pracovním PC

Shrnutí:

Používám-li vlastní zařízení k práci, jsem zodpovědný/á za jeho zabezpečení.
Firma má právo vyžadovat určité nastavení a pravidla – a já mám právo vědět, co se od mého zařízení očekává.

Vzor postupu pro hlášení bezpečnostního incidentu

Pro zaměstnance veřejných institucí a firem

Co je bezpečnostní incident?

Bezpečnostní incident je jakákoli událost, která může **ohrozit důvěrnost, integritu nebo dostupnost** dat, systémů nebo služeb. Např.

- Podezřelý e-mail (phishing)
- Ztráta nebo krádež zařízení (notebook, telefon)
- Neoprávněný přístup do systému
- Šifrování dat (ransomware)
- Únik dat (osobních, zákaznických, interních)
- Neobvyklé chování zařízení nebo systémů

✅ 1. ZACHOVEJTE KLID – ale jednejte rychle

Čím dříve je incident nahlášen, tím větší je šance na minimalizaci škod.

✅ 2. OKAMŽITĚ PROVEĎTE TATO OPATŘENÍ:

Situace	Akce
Podezřelý e-mail	Neotvírejte přílohy, neklikejte na odkazy, nepřeposílejte
Podezřelé chování systému	Odpojte zařízení od sítě (Wi-Fi, kabel)
Ztráta zařízení	Pokud je možné, aktivujte vzdálené vymazání nebo lokalizaci
Viditelný útok (např. šifrování dat)	Vypněte zařízení a nezasahujte dál

---

✅ 3. NAHLAŠTE INCIDENT SPRÁVNÉ OSOBĚ / TÝMU:

- 📞 Telefon (pohotovostní linka IT): **[doplňte konkrétní číslo]**
- 📧 E-mail bezpečnostního týmu: **[incidenty@vasedomena.cz]**
- 🛠️ Interní portál pro hlášení incidentů: **[odkaz na intranet / formulář]**

✅ 4. CO PŘI HLÁŠENÍ UVÉST:

Při komunikaci s IT/bližším bezpečnostním týmem uveďte:

- **Jméno, oddělení a kontakt**
- **Čas, kdy jste si incidentu všimli**
- **Popis události** – co se stalo, na kterém zařízení
- **Kroky, které jste už provedli** (např. odpojení, vypnutí, záloha)
- **Přílohy** – printscreeny, kopie podezřelého e-mailu apod.
- **Dopad na vaši práci** (např. nemožnost přístupu, ztráta dat)

✅ 5. CO DÁL?

- Vyčkejte na pokyny od IT nebo bezpečnostního správce
- Nesdílejte informace o incidentu mimo určený okruh osob
- Nepodnikněte další vlastní „opravné kroky“, pokud nejste vyzváni

---

Pamatujte:

Incident není selhání zaměstnance, ale hrozba, kterou je třeba rychle a odpovědně řešit.
Raději **nahlásit planý poplach**, než mlčet při reálném ohrožení.

DIGITERRA

Mini-kvíz: Otestuj svou kybernetickou hygienu

Vyberte vždy jednu správnou odpověď (a, b nebo c).

1. Co je hlavním cílem phishingového útoku?

a) Vymazání souborů na disku
b) Získání citlivých údajů (např. hesel)
c) Zablokování počítače

2. Co z následujícího je příkladem silného hesla?

a) 12345678
b) mojeheslo
c) G!r7$Zk#92lQ

3. Jak byste měli zacházet s podezřelým e-mailem s přílohou?

a) Otevřít jej a zjistit, o co jde
b) Přeposlat kolegovi pro názor
c) Neotevírat, nahlásit IT oddělení

4. Co znamená zkratka BYOD?

a) Bring Your Official Device
b) Back Your Office Drive
c) Bring Your Own Device

5. Kdy je nejvhodnější používat VPN?

a) Jen když chci skrýt svou IP adresu
b) Při připojení k veřejné nebo domácí Wi-Fi síti kvůli práci
c) Při přehrávání videí

6. Jaké opatření je NEJÚČINNĚJŠÍ proti neoprávněnému přístupu k účtu?

a) Heslo s minimálně 6 znaky
b) Automatické přihlášení
c) Dvoufaktorové ověření (2FA)

7. Co uděláte, pokud vám někdo omylem pošle soubor s osobními údaji?

a) Uložíte si ho pro jistotu
b) Přepošlete dál, ať to někdo vyřeší
c) Nahlásíte incident podle interního postupu

8. Které heslo je bezpečnější?

a) Januška2024
b) VseNajednou!
c) jAnUšKa2024

✅ Klíč ke kvízu: 1 – **b**, 2 – **c**, 3 – **c**, 4 – **c**, 5 – **b**, 6 – **c**, 7 – **c**, 8 – **b**

Rozšířený test: Základy kybernetické bezpečnosti

1–5: Hesla a přihlašování

1. Jaké je nejbezpečnější heslo?
   a) admin123
   b) Letni2024
   c) mJ7!vP#92k
2. Co je dvoufaktorové ověření (2FA)?
   a) Přihlášení dvakrát po sobě
   b) Ověření hesla a další metodou (např. kód v mobilu)
   c) Heslo + jméno uživatele
3. Kdy je nutné změnit heslo?
   a) Když unikne, nebo se o to někdo pokusí
   b) Každý den
   c) Nikdy, pokud ho znám jen já
4. Kde je vhodné si ukládat hesla?
   a) Na papírek v šuplíku
   b) Do správce hesel
   c) Do poznámky na ploše
5. Co je slabé heslo?
   a) Rw#e9@1sBz!
   b) MojeFirma2024!
   c) 123456

6–10: E-maily a phishing

6. Co je phishing?
   a) Test síťového připojení
   b) Simulace zálohování dat
   c) Pokus vylákat informace pomocí podvodné zprávy
7. Co uděláte, když obdržíte e-mail s výhrůžkou a žádostí o peníze?
   a) Ihned zaplatíte
   b) Přepošlete kolegovi
   c) Nahlásíte IT / bezpečnostnímu oddělení
8. Jak může vypadat phishingový e-mail?
   a) Obsahuje gramatické chyby, tlak na rychlé jednání
   b) Má výhrůžky a falešné logo
   c) Obojí je možné
9. Odkud většinou přichází phishing?
   a) Od známé adresy
   b) Z podvržené nebo cizí domény
   c) Pouze přes SMS
10. Jak nejlépe ověřit legitimitu e-mailu?
    a) Kliknutím na odkaz
    b) Zavoláním odesílateli na známé číslo
    c) Odpovědí na zprávu

11–15: Zařízení a domácí prostředí

11. Jak zabezpečit notebook při práci mimo kancelář?
    a) Zakrýt logo
    b) Pracovat jen offline
    c) Použít VPN a zamykat obrazovku
12. Co je BYOD?
    a) Vlastní zařízení používané k práci
    b) Firemní auto
    c) Rezervovaný zasedací čas
13. Jak poznám, že někdo neoprávněně použil mé zařízení?
    a) Baterie se vybíjí rychleji
    b) Jsou přítomny neznámé procesy / aplikace
    c) Mám nový tapetu
14. Proč je důležité aktualizovat software?
    a) Kvůli novým funkcím
    b) Aby se zrychlil počítač
    c) Kvůli odstranění zranitelností
15. Co udělat při ztrátě služebního telefonu?
    a) Zavolat na něj a čekat
    b) Změnit pozadí
    c) Nahlásit a aktivovat vzdálené vymazání

16–20: Chování, zákon a incidenty

16. Který krok je správný při podezření na útok?
    a) Pokračovat v práci
    b) Odpojit zařízení od sítě a nahlásit incident
    c) Restartovat počítač a zapomenout
17. Co je bezpečnostní incident?
    a) Zapomenuté heslo
    b) Událost s potenciálním dopadem na bezpečnost
    c) Pomalý počítač
18. Kdy se používá VPN?
    a) Při sledování filmů
    b) Při připojení k firemní síti zvenčí
    c) Když je slabý signál
19. Co je povinností zaměstnance dle kybernetické politiky?
    a) Vyměnit router
    b) Nahlásit incidenty a chránit přístupy
    c) Nic, odpovídá firma
20. Proč je důležitá digitální hygiena?
    a) Zabraňuje špíně na klávesnici
    b) Zajišťuje osobní a firemní bezpečnost při práci s IT
    c) Jen kvůli pravidlům EU

🗝 **Klíč správných odpovědí:** 1–c, 2–b, 3–a, 4–b, 5–c, 6–c, 7–c, 8–c, 9–b, 10–b, 11–c, 12–a, 13–b, 14–c, 15–c, 16–b, 17–b, 18–b, 19–b, 20–b

---