**Analýza kybernetickej bezpečnosti spoločnosti Boprodejna**

Vytvoril Mikhail Shishov pre kurz ZKB, LS 2024/2025

**Základna informácia**

**Náplň činnosti:** Prodejna automobilů ve velkém městě.

**Sídlo:** Jedna budova v menším městě.

**Počet zaměstnanců:**

* 1 - vedení společnosti
* 6 - provozní pracovníci, prodejci
* 2 - účetní
* 2 - pobočky, administrativa

**Hardware:**

* 10x notebookov
* 1x tiskárna
* 1x sdílené úložiště pro ukládání a sdílení souborů
* 1x webový a poštovní server (cloudový)
* 5x access points pro WiFi síť v centrále
* 2x switch pro drátovou síť
* 1x router zajišťující konektivitu k Internetu

**Software:**

* Specializovaný prodejní a reklamační SW
* OS a balík kancelářských programů pro všechna zařízení

**Vymyšlená informacia navyše:**

* Firma sa nachádza v Zline, má jednú predajňu
* Má obrat 250 milionov Kč ročne
* Školenie zamestnancov ohľadom kybernetickej bezpečnosti neprebiehalo nikdy, ale je základne školenie o fyzickej bezpečnosti budov a prostriedkov firmy
* Společnost se kybernetickou bezpečností nezabývá vůbec - takže nie je chráněná voči akýmkoľvek hrozbám.

**Úvod**

Spoločnosť Boprodejna je malá firma, ktorá sa zaoberá predajom nových automobilov značky Mazda. Firma sídli v Zlíne, má tam predajňu v budove mimo centra. V spoločnosti pracuje celkovo 11 zamestnancov - konkrétne 6 predajcov, 2 účtovníčky a 3 pracovníci v oblasti administratívy a vedenia firmy. Firma dosahuje ročný obrat približne 250 miliónov Kč.

Doteraz sa v spoločnosti nekládol systematický dôraz na oblasť kybernetickej bezpečnosti. Tento fakt predstavuje obrovské riziko pre plynulosť a bezpečnosť obchodných procesov, ako aj dôvernosť a integritu uchovávaných dát.

**Technické vybavenie a aktuálny stav**

Spoločnosť v súčasnosti disponuje nasledovným technickým vybavením:

* 10 firemných notebookov používaných predajcami, účtovníkmi a administratívou
* 1 multifunkčná tlačiareň
* centrálne zdieľané dátové úložisko
* cloudový server pre firemný web a emailovú komunikáciu
* základna sieťová infraštruktúra: router, dva sieťové switche a päť Wi-Fi prístupových bodov

Zamestnanci spoločnosti nikdy neabsolvovali školenie zamerané na kybernetickú bezpečnosť. Zariadenia sú používané bez centrálnej správy alebo politiky aktualizácií, a pravidlá používania technológií nie sú formálne definované pomocou smernic.

Škaly evaluacii pravdepodobnosti hrozieb a zavažnosti nasledkov

| **Hodnota** | **Pravdepodobnosť hrozby** |
| --- | --- |
| 1 | Nepravdepodobná, nevyskytuje takmer nikdy |
| 2 | Môže vyskytnuť občas |
| 3 | Pravdepodobná |
| 4 | Vysoká pravdepodobnosť, takmer určite sa stáne |
| 5 | Trvalá, každodenná |

| **Hodnota** | **Závažnosť hrozby** |
| --- | --- |
| 1 | Zanedbatelná |
| 2 | Málo významná |
| 3 | Významná |
| 4 | Vážná |
| 5 | Kritická, môže vyvolať nevratne škody |

Vypočet

Na hodnotenie rizík je použitý model, pozostávajúci z troch hlavných faktorov.

**Hodnota aktíva (A)**

Stanovuje sa podľa dôležitosti daného aktíva pre fungovanie firmy, kde:

1 - nízka hodnota (napr. tlačiareň)

5 - kritická hodnota (napr. databáza)

**Pravdepodobnosť výskytu hrozby (T)**

Vyjadruje pravdepodobnosť, s akou sa daná hrozba môže reálne vyskytnúť, kde 1 - veľmi nepravdepodobná, a 5 - veľmi pravdepodobná.

**Zraniteľnosť aktíva (V)**

Označuje úroveň náchylnosti aktíva k poškodeniu alebo zneužitiu v dôsledku hrozby, kde 1 - dobre chránené, a 5 - úplne nezabezpečené.

**Výpočet miery rizika (R)**

Miera rizika sa vypočíta ako súčin troch vyššie uvedených faktorov:

**R = T \* A \* V**

Výsledné hodnoty sú premietnuté do matice rizík, ktorá slúži ako nástroj vizualizácie kritických oblastí. Všetký vypočty sú podľa [článku](https://bpm-tema.blogspot.com/2007/11/ppadov-studie-analzy-rizik-informan.html).

Aktiva

| **Typ** | **Aktivita** | **Hodnota (5 je najdôležitejšie)** |
| --- | --- | --- |
| Informácia | Databázy | 5 |
| Backup | 3 |
| Hardware | 10 notebookov | 4 |
| Tlačiareň | 1 |
| 2 switche | 4 |
| Access points pre Wi-Fi | 3 |
| Router | 5 |
| Software | Microsoft Office, Outlook | 4 |
| OS na notebookoch - predpokladajme, že Windows 10 | 5 |
| Cloud storage | 3 |
| CRM s databázou zákazníkov a zaujemcov - predpokladajme, že Salesforce | 5 |
| Webová stránka na Wordpress | 2 |
| Programy pre predaj a reklamáciu | 4 |
| Služby | Pripojenie jednotlivých budov k internetu | 3 |
| Externý webovy server (hosting) | 2 |
| Funkčný predaj a reklamácia na pobočkách | 5 |

Hrozby

| **Hrozba** | **Popis hrozby** | **Pravdepodobnosť hrozby** |
| --- | --- | --- |
| Úniknuté alebo ztratené dáta | Vysoké riziko úniku databáz (DB zákazníkov v CRM a SQL DB pre webovú stránku), pretože sú prístupné bez dvojfaktorovej autentifikácii, prístup k CRM majú takmer všetký zamstnanci | 5 |
| Zalohovanie neprebieha pravidelne, nie je automatizované - existuje riziko ztraty dát | 4 |
| Webová stránka firmy je na Wordpress, umiestená na obyčajnom hostingu - riziko prolomení stránky spoločnosti alebo vyrazného zpomalení, útoky DDoS | 3 |
| Ztráta dát, súborov, ktoré sa nachádzajú v cloude | 1 |
| Wi-Fi sieť bez hesla - možné zneužitie | 2 |
| Zlyhanie HW | Zlyhanie hardwaru vo viac ako jednom notebooku, ztráta pobočkou možnosti normalne pracovať kvôli tomu | 1 |
| Zlyhanie tlačiarne alebo neopravnený prístup pre nadmernú tlač osobných dokumentov zamestnancov | 1 |
| Zlyhanie switchu, jedného z AP alebo routeru, ztráta možnosti pracovať kvôli tomu | 1 |
| Zlyhanie SW | Napadnutie cez email - napr. phishing, prosba stiahnuť súbor (PDF, obrázok atd.) s malwarom, spoofing mailov zamestnancov | 4 |
| Zlyhanie OS v následku napadnutia cez email alebo kvôli inštalacii piratského softwaru - nie sú aktualizácii Win 10 | 2 |
| Nefunkčnosť programov kvôli chybnej aktualizácii na stráne vyvojara | 1 |
| Fyzická nebezpečnosť | Pokus o krádež aut alebo peňazi v hotovosti | 2 |
| Poškodenie auta zákaznikom počas prehliadky auta | 2 |
| Prírodné katastrofy - pôvodeň, zemetrasenie | 1 |

Matica zraniteľnosti, a vysledok nasleduje v matici rizik

| **Popis hrozby** | **Popis aktiva** | **Databázy (CRM + SQL)** | **Backup** | **NTB** | **Tlačiareň** | **Switche** | **AP** | **Router** | **Office, Outlook** | **Windows 10** | **Cloud** | **Webová stránka** | **Predaj a reklamácia, programy** | **Pripojenie k internetu** | **Webový server** | **Predaj a reklamácia, funkčnosť** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Hodnota aktiva** | 5 | 3 | 4 | 1 | 4 | 3 | 5 | 4 | 5 | 3 | 2 | 4 | 3 | 2 | 5 |
| **Popis hrozby** | **P hrozby** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Vysoké riziko úniku databáz (DB zákazníkov v CRM a SQL DB pre webovú stránku), pretože sú prístupné bez dvojfaktorovej autentifikácii, prístup k CRM majú takmer všetký zamstnanci | 5 | 5 | 3 |  |  |  |  |  |  |  |  |  |  |  |  | 5 |
| Zalohovanie neprebieha pravidelne, nie je automatizované - existuje riziko ztraty dát | 4 |  | 5 |  |  |  |  |  |  |  | 2 | 3 |  |  |  |  |
| Webová stránka firmy je na Wordpress, umiestená na obyčajnom hostingu - riziko prolomení stránky spoločnosti alebo vyrazného zpomalení, útoky DDoS | 3 |  |  |  |  |  |  |  |  |  |  | 3 |  |  |  |  |
| Ztráta dát, súborov, ktoré sa nachádzajú v cloude | 1 |  |  |  |  |  |  |  |  |  | 5 |  |  |  |  |  |
| Wi-Fi sieť bez hesla - možné zneužitie | 2 |  |  |  |  | 1 | 1 | 1 |  |  |  |  |  | 2 |  |  |
| Zlyhanie hardwaru vo viac ako jednom notebooku, ztráta pobočkou možnosti normalne pracovať kvôli tomu | 1 |  |  | 5 |  |  |  |  |  |  |  |  |  |  |  |  |
| Zlyhanie tlačiarne alebo neopravnený prístup pre nadmernú tlač osobných dokumentov zamestnancov | 1 |  |  |  | 5 |  |  |  |  |  |  |  |  |  |  |  |
| Zlyhanie switchu, jedného z AP alebo routeru, ztráta možnosti pracovať kvôli tomu | 1 |  |  |  |  | 4 | 2 | 5 |  |  |  |  |  | 5 |  |  |
| Napadnutie cez email - napr. phishing, prosba stiahnuť súbor (PDF, obrázok atd.) s malwarom, spoofing mailov zamestnancov | 4 | 5 | 5 |  |  |  |  |  |  | 5 |  | 5 | 5 |  |  |  |
| Zlyhanie OS v následku napadnutia cez email alebo kvôli inštalacii piratského softwaru - nie sú aktualizácii Win 10 | 2 |  |  |  |  |  |  |  |  | 5 |  |  |  |  |  |  |
| Nefunkčnosť programov kvôli chybnej aktualizácii na stráne vyvojara | 1 | 3 |  |  |  |  |  |  | 3 | 3 |  |  |  |  |  |  |
| Pokus o krádež aut alebo peňazi v hotovosti | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 3 |
| Poškodenie auta zákaznikom počas prehliadky auta | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 5 |

| **Popis hrozby** | **Popis aktiva** | **Databáza (CRM + SQL)** | **Backup** | **NTB** | **Tlačiareň** | **Switche** | **AP** | **Router** | **Office, Outlook** | **Windows 10** | **Cloud** | **Webová stránka** | **Predaj a reklamácia, programy** | **Pripojenie k internetu** | **Webový server** | **Predaj a reklamácia, funkčnosť** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Hodnota aktiva** | 5 | 3 | 4 | 1 | 4 | 3 | 5 | 4 | 5 | 3 | 2 | 4 | 3 | 2 | 5 |
| **Popis hrozby** | **P hrozby** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Vysoké riziko úniku databáz (DB zákazníkov v CRM a SQL DB pre webovú stránku), pretože sú prístupné bez dvojfaktorovej autentifikácii, prístup k CRM majú takmer všetký zamstnanci | 5 | 5 \* 5 \* 5 = 125 | 3 \* 3 \* 5 = 45 |  |  |  |  |  |  |  |  |  |  |  |  | 5 \* 5 \* 5 = 125 |
| Zalohovanie neprebieha pravidelne, nie je automatizované - existuje riziko ztraty dát | 4 |  | 5 \* 3 \* 4 = 60 |  |  |  |  |  |  |  | 2 \* 3 \* 4 = 24 | 3 \* 2 \* 4 = 24 |  |  |  |  |
| Webová stránka firmy je na Wordpress, umiestená na obyčajnom hostingu - riziko prolomení stránky spoločnosti alebo vyrazného zpomalení, útoky DDoS | 3 |  |  |  |  |  |  |  |  |  |  | 3 \* 2 \* 3 = 18 |  |  |  |  |
| Ztráta dát, súborov, ktoré sa nachádzajú v cloude | 1 |  |  |  |  |  |  |  |  |  | 5 \* 3 \* 1 = 15 |  |  |  |  |  |
| Wi-Fi sieť bez hesla - možné zneužitie | 2 |  |  |  |  | 2 \* 4 \* 1 = 8 | 3 \* 2 \* 1 = 6 | 5 \* 2 \* 1 = 10 |  |  |  |  |  | 2 \* 3 \* 2 = 12 |  |  |
| Zlyhanie hardwaru vo viac ako jednom notebooku, ztráta pobočkou možnosti normalne pracovať kvôli tomu | 1 |  |  | 5 \* 4 \* 1 = 20 |  |  |  |  |  |  |  |  |  |  |  |  |
| Zlyhanie tlačiarne alebo neopravnený prístup pre nadmernú tlač osobných dokumentov zamestnancov | 1 |  |  |  | 5 \* 1 \* 1 = 5 |  |  |  |  |  |  |  |  |  |  |  |
| Zlyhanie switchu, jedného z AP alebo routeru, ztráta možnosti pracovať kvôli tomu | 1 |  |  |  |  | 4 \* 4 \* 1 = 16 | 2 \* 3 \* 1 = 6 | 5 \* 5 \* 1 = 25 |  |  |  |  |  | 5 \* 3 \* 1 = 15 |  |  |
| Napadnutie cez email - napr. phishing, prosba stiahnuť súbor (PDF, obrázok atd.) s malwarom, spoofing mailov zamestnancov | 4 | 5 \* 5 \* 4 = 100 | 5 \* 3 \* 4 = 60 |  |  |  |  |  |  | 5 \* 5 \* 4 = 100 |  | 5 \* 2 \* 4 = 40 | 5 \* 4 \* 4 = 80 |  |  |  |
| Zlyhanie OS v následku napadnutia cez email alebo kvôli inštalacii piratského softwaru - nie sú aktualizácii Win 10 | 2 |  |  |  |  |  |  |  |  | 5 \* 5 \* 2 = 50 |  |  |  |  |  |  |
| Nefunkčnosť programov kvôli chybnej aktualizácii na stráne vyvojara | 1 | 3 \* 5 \* 1 = 15 |  |  |  |  |  |  | 3 \* 4 \* 1 = 12 | 3 \* 5 \* 1 = 15 |  |  |  |  |  |  |
| Pokus o krádež aut alebo peňazi v hotovosti | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 3 \* 5 \* 2 = 30 |
| Poškodenie auta zákaznikom počas prehliadky auta | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 5 \* 5 \* 2 = 50 |

Návrh bezpečnostných opatrení a ekonomika

| **Opatrenie** | **Náklady, odhad** | **Efektívita** | **Komentár** |
| --- | --- | --- | --- |
| Nastavenie regulárnheho zalohovania | takmer žiadné,  pár hodín práci, 1000-3000 Kč | Vysoká | Pomocou bezplatných programov alebo funkcii v už nainštalovanom SW |
| Pravidelné testovanie obnovy záloh | žiadné | Nízka | Kontrola toho, že dáta sa ukaladjú správne, bez chyb, že všetko potrebné je v cloudu. Môže prebiehať raz za 180 dní |
| Školenie zamestnancov | 5-15 000 Kč, ročne | Vysoká | Ročne školenie, ktoré pomôže bojovať proti ľudským chybam. Môžú byť aj kurzy |
| Zavedenie dvojfaktorovej autentifikácie | žiadné | Stredná | Istota v tom, že prístup nebude zneužitý neopravnenou osobou. Autentifikácia sa nastavuje cez Google Autenticator, Microsoft alebo podobne služby |
| Obmedzenie prístupu k CRM podľa rolí | takmer žiadné,  pár hodín práci | Vysoká | Bežný zamestnanec musí mať menej opravnení a menej údajov zákazníkov |
| Použitie Cloudflare a Google Recaptcha | takmer žiadné,  pár hodín práci vyvojara | Stredná | Zlepšená bezpečnosť stránky, zaroveň aj zvyšuje rychlosť, na webu je menej botov a nevhodných zpráv |
| Zabezpečenie Wi-Fi siete | takmer žiadné | Stredná | Obmedzený prístup k Wi-FI, nastavenie hesla |
| Zavedenie aktualizácií OS a softvéru, inštalacia Windows 11 | zaleží na SW, takže žiadné až 20 000 Kč | Nízka | Lepšia bezpečnosť v aktualizáciach |
| Ochrana HW pred výpadkom | 50 000 Kč | Stredná | Zdroj nepřerušovaného napájania (UPS), aby internetové služby bežali bez poruch. Náhradne notebooky |
| Kamerový systém, zálohovanie záznamov, poistenie od nejakej poišťovni | 50 000 Kč - 200 000 Kč | Vysoká | Vyrazné zlepšenie bezpečnosti. Monitorovánie priestorov, zálohovanie videa |

Odhadované mzdy

* Predajcovia: 6 \* 35 000 Kč -> 210 000 Kč
* Účtovníčky: 2 \* 40 000 Kč -> 80 000 Kč
* Administratíva a vedenie: 3 \* 45 000 Kč -> 135 000 Kč
* Hrubé mzdy spolu: 425 000 Kč mesačne a 5 100 000 Kč ročne

**Odhadované odvody a dane**

* Sociálne a zdravotné odvody (~34%): ~1 734 000 Kč ročne
* Daň z príjmu právnických osôb: ~19% zo zisku (predpokladaná daň pri zisku 10 mil. Kč = 1,9 mil. Kč)

**Odhadované prevádzkové náklady**

* Prenájom priestorov: cca 100 000 Kč/mesiac -> 1 200 000 Kč/rok
* Ine (energie, voda, kúrenie a klimatizácia atd.): cca 700 000 Kč/rok

**Náklady na kybernetickú bezpečnosť (z navrhovaných opatrení)**

* Celkové náklady na bezpečnosť v tomto roku: cca 260 000 Kč
* Podiel na ročnom obrate: cca 0,1%
* Podiel na ročnom zisku: cca 2,6%

Z tohto vyplyvá, že firma môže si dovoliť prijatie týchto opatrení a zmien.

**Harmonogram s prioritami**

| **Deadline (začiatok práci je 15.04.2025)** | **Opatrenie** | **Priorita** | **Komentár** |
| --- | --- | --- | --- |
| 21.04.2025 | Nastavenie regulárnheho zalohovania | Vysoká | Pomocou bezplatných programov alebo funkcii v už nainštalovanom SW |
| 28.04.2025 - začiatok školenia, ktoré musí byť dokončené všetkými maximálne za mesiac | Školenie zamestnancov | Vysoká | Ročne školenie, ktoré pomôže bojovať proti ľudským chybam. Môžú byť aj kurzy |
| 30.04.2025 | Obmedzenie prístupu k CRM podľa rolí | Vysoká | Bežný zamestnanec musí mať menej opravnení a menej údajov zákazníkov |
| 12.05.2025 | Kamerový systém, zálohovanie záznamov | Vysoká | Vyrazné zlepšenie bezpečnosti. Monitorovánie priestorov, zálohovanie videa |
| 19.05.2025 | Ochrana HW pred výpadkom energii | Stredná | Nastavit zdroj nepřerušovaného napájania (UPS), aby internetové služby bežali bez poruch. Náhradne notebooky |
| 26.05.2025 | Zavedenie dvojfaktorovej autentifikácie | Stredná | Istota v tom, že prístup nebude zneužitý neopravnenou osobou. Autentifikácia sa nastavuje cez Google Autenticator, Microsoft alebo podobne služby |
| 28.05.2025 | Použitie Cloudflare a Google Recaptcha | Stredná | Zlepšená bezpečnosť stránky, zaroveň aj zvyšuje rychlosť, na webu je menej botov a nevhodných zpráv |
| 02.06.2025 | Zabezpečenie Wi-Fi siete | Stredná | Obmedzený prístup k Wi-FI, nastavenie hesla |
| 09.06.2025 | Zavedenie aktualizácií OS a softvéru, inštalacia Windows 11 | Nízka | Lepšia bezpečnosť v aktualizáciach |
| 13.06.2025 | Pravidelné testovanie obnovy záloh | Nízka | Kontrola toho, že dáta sa ukaladjú správne, bez chyb, že všetko potrebné je v cloudu. Môže prebiehať raz za 180 dní |

**Návrh smernice pre používateľov - bežných zamestnancov**

**Úvod**

Táto smernica stanovuje základné pravidlá správania sa používateľov informačných systémov spoločnosti s cieľom zabezpečiť dôvernosť, integritu a dostupnosť firemných údajov a systémov. Každý zamestnanec, ktorý má prístup k informačným a komunikačným technológiám firmy, je povinný dodržiavať túto smernicu.

**1. Zodpovedné používanie zariadení a služieb:**

1. Firemné informačné technológie (notebooky, tlačiarne, servery, cloudové služby) sú určené výlučne na pracovné účely. Ich používanie na súkromné účely je povolené len so súhlasom vedenia spoločnosti.
2. Zamestnanci nesmú inštalovať softvér na firemné zariadenia bez povolenia. Každý softvér musí byť schválený IT správcom a mať platnú licenciu.
3. Pripojenie externých zariadení (napr. USB, SSD atd.) je povolené len po ich kontrole a schválení správcom systému.

**2. Prístupové údaje k službam a správa hesiel:**

1. Každý zamestnanec je povinný používať silné heslo s minimálnou dĺžkou 10 znakov, ktoré obsahuje kombináciu veľkých a malých písmen, číslic a špeciálnych znakov.
2. Používateľ nesmie zdieľať svoje prístupové údaje s inými osobami ani ich ukladať v nezabezpečenom formáte (napr. na papieri).
3. Heslá je potrebné meniť pravidelne, minimálne raz za 180 dní.
4. Viacfaktorové overovanie (MFA) je povinné pre všetky služby, ktoré túto možnosť podporujú.

**3. Ochrana dát a predchádzanie incidentom:**

1. Používateľ nesmie bez povolenia sťahovať, ukladať alebo prenášať osobné, obchodné alebo finančné údaje mimo schválených úložísk.
2. Je zakázané otvárať e-mailové prílohy a odkazy od neznámych alebo podozrivých odosielateľov.
3. V prípade podozrenia na infikovanie zariadenia, únik údajov alebo iný bezpečnostný incident je používateľ povinný bezodkladne kontaktovať osobu, zodpovednú za bezpečnosť IT vo firme.

**4. Vzdelávanie a zodpovednosť:**

1. Každý zamestnanec je povinný zúčastniť sa školenia zameraného na kybernetickú bezpečnosť minimálne raz za jeden rok.
2. Dodržiavanie tejto smernice je súčasťou pracovnej disciplíny. Porušenie môže viesť k disciplinárnym opatreniam v rámci platných zákonov ČR, vrátane vypovedi z práci, alebo právnym dôsledkom.

**Návrh smernice pre administrátorov - správcov informačných systémov**

**Úvod**

Táto smernica definuje povinnosti a štandardy pre správu, údržbu a ochranu informačných systémov spoločnosti Boprodejna. Je určená pre technických pracovníkov a IT administrátorov, ktorí zodpovedajú za prevádzku, dostupnosť a bezpečnosť systémových a sieťových služieb.

**1. Správa používateľských účtov:**

1. Všetci používatelia musia mať vytvorený individuálny používateľský účet. Spoločné účty sú zakázané.
2. Po ukončení pracovného pomeru zamestnanca musí byť jeho prístup deaktivovaný bezodkladne, najneskôr do 24 hodín.
3. Administrátor musí používať oddelený účet pre bežné činnosti a administráciu.

**2. Zabezpečenie a aktualizácia systémov:**

1. Všetky zariadenia musia byť chránené aktualizovaným antivírusovým riešením a nastaveným firewallom.
2. Operačné systémy a softvér musia byť pravidelne aktualizované, najneskôr do 15 pracovných dní od vydania aktualizacií.
3. Bezdrôtová sieť (Wi-Fi) musí byť zabezpečená a chranená heslom, ktoré však môže byť zdieľano s navštevníkom.

**3. Zálohovanie a obnova dát:**

1. Zálohy kritických dát (účtovníctvo, zákaznícke údaje, interné dokumenty) sa musia vykonávať denne.
2. Zálohy musia byť uložené oddelene od primárnych systémov, buď v cloude alebo na fyzickom externom zariadení.

**4. Šifrovanie a ochrana údajov:**

1. Notebooky a iné počitači nesmú byť prístupne bez hesla.
2. Firma musí brať do úvahy GDPR a chraniť údaje podľa platných zákonov ČR a EÚ.
3. Komunikácia medzi klientom a serverom (napr. web) musí byť zabezpečená certifikátom TLS/SSL.

**5. Monitorovanie a riešenie incidentov:**

1. IT správca je povinný zabezpečiť zber a monitorovanie systémových logov.
2. Pri podozrení na bezpečnostný incident musí bezodkladne riešiť problém.
3. O incidente musí byť spísaná správa, ktorá bude archivovaná pre prípadné vyšetrovanie alebo audit.
4. Dodržiavanie tejto smernice je súčasťou pracovnej disciplíny. Porušenie môže viesť k disciplinárnym opatreniam v rámci platných zákonov ČR, vrátane vypovedi z práci, alebo právnym dôsledkom.

**Návrh smernice o fyzickej bezpečnosti**

**Úvod**

Cieľom tejto smernice je stanoviť zásady a opatrenia na ochranu fyzického majetku spoločnosti, ako aj zamedziť neoprávnenému fyzickému prístupu k citlivým technickým zariadeniam, dátam a priestorom. Smernica dopĺňa technické opatrenia v oblasti kybernetickej bezpečnosti o fyzické aspekty ochrany.

**1. Ochrana budovy a priestorov:**

1. Prístup do administratívnej časti firmy je povolený iba zamestnancom spoločnosti a oprávneným návštevám, pričom zamestnanec musí byť prítomný počas celej doby navštevy.
2. Vstup do budov musí byť zabezpečený elektronickým alebo mechanickým uzamykaním mimo pracovnej doby.
3. Všetky vstupné dvere (prípadne aj okná) musia byť uzatvárané počas neprítomnosti zamestnancov.

**2. Ochrana technických zariadení:**

1. Sieťové prvky (router, switchy, access pointy atd.) musia byť umiestnené v uzamknutej skrini, skrinke alebo vyhradenej miestnosti bez prístupu pre verejnosť.
2. Koncové zariadenia (notebooky, tlačiarne, počitače) nesmú byť ponechávané bez dozoru na verejne prístupných miestach.
3. V prípade prenosných zariadení sa odporúča používať fyzické zámky, napríklad Kensington lock a podobne.
4. Prístup k zdieľanému úložisku, ak bude nejakým spôsobom preniesený do budov, musí byť zabezpečený v uzamknutej miestnosti alebo skrinke.
5. Akýkoľvek servis alebo výmena sieťových komponentov smie byť vykonaná iba kvalifikovaným technickým pracovníkom.

**3. Ochrana pred krádežou a neoprávneným vstupom:**

1. Majetok firmy musí byť evidovaný, aby možnosť ztráty bez všimnutia bola vylučena.
2. V prípade odcudzenia zariadenia je zamestnanec povinný bezodkladne informovať vedenie a správcu systému, zaroveň aj zablokovať prístup k zariadeniu, ak existuje možnosť.
3. Vo firme by mal byť vyvesený oznam o zákaze neautorizovaného vstupu do sieťových zariadení.

**4. Zodpovednosť a kontrola:**

1. Fyzickú bezpečnosť pravidelne preveruje vedenie firmy alebo poverený zamestnanec, minimálne raz za 180 dní.
2. Porušenie týchto pravidiel môže viesť k disciplinárnym postihom podľa vnútorného poriadku firmy.
3. Prípadné incidenty sa zaznamenávajú do vyhradeného úložiska, aby boli archivované pre prípadné vyšetrovanie alebo audit.

**Záver**

Z hľadiska nákladov predstavujú odporúčané opatrenia minimálnu záťaž na celkový rozpočet spoločnosti, no môžu zásadným spôsobom znížiť pravdepodobnosť kybernetických incidentov.

Zavedením bezpečnostných politík, technických opatrení a pravidelného školenia je možno výrazne znížiť zraniteľnosť, takže investícia do kybernetickej bezpečnosti sa oplatí, najmä v porovnaní s potenciálnymi stratami, spôsobenými výpadkom systémov alebo únikom údajov. Odporúča sa zabezpečiť implementáciu všetkých navrhnutých krokov do 6 mesiacov a následne ich pravidelne vyhodnocovať.