Checklist kyberbezpečnosti pre malú firmu

Pre firmy, živnostníkov a neziskovky. Pri každom bode zaškrtnite ÁNO alebo NIE. Každé NIE je úloha na najbližší mesiac.

Firma / organizácia: _____ Dátum kontroly: _____ Vyplnil/a: _____

1. HESLÁ A PRIHLASOVANIE

#	Opatrenie	ÁNO	NIE
1	Každý zamestnanec má vlastný účet a vlastné heslo (žiadne spoločné heslo „pre všetkých“).	☐	☐
2	Heslá majú aspoň 12–14 znakov a pre každú službu sú iné.	☐	☐
3	Používame správcu hesiel; heslá nie sú na papierikoch ani v e-mailoch.	☐	☐
4	Dvojfázové overenie (2FA) je zapnuté na e-maile.	☐	☐
5	2FA je zapnuté na internet bankingu, účtovnom softvéri, sociálnych sieťach a e-shope.	☐	☐
6	Predvolené heslá (router, tlačiareň, kamera) sme zmenili.	☐	☐

2. ZÁLOHY

#	Opatrenie	ÁNO	NIE
7	Dôležité údaje (účtovníctvo, zmluvy, zákazky) sa zálohujú aspoň raz týždenne.	☐	☐
8	Máme 3 kópie údajov na 2 rôznych médiách a 1 kópiu mimo firmy (pravidlo 3-2-1).	☐	☐
9	Externý zálohovací disk je po zálohovaní odpojený.	☐	☐
10	Za posledné 3 mesiace sme vyskúšali obnoviť súbor zo zálohy.	☐	☐

3. ZARIADENIA A AKTUALIZÁCIE

#	Opatrenie	ÁNO	NIE
11	Počítače a mobily majú zapnuté automatické aktualizácie.	☐	☐
12	Prehliadače, web (napr. WordPress a pluginy) a router sa pravidelne aktualizujú.	☐	☐
13	Nepoužívame zariadenia ani systémy, ktoré už nedostávajú bezpečnostné aktualizácie.	☐	☐
14	Na každom počítači je zapnutý antivírus (napr. Microsoft Defender).	☐	☐
15	Zariadenia majú zámok obrazovky s PIN-om / heslom.	☐	☐
16	Notebooky majú šifrovaný disk (BitLocker / FileVault).	☐	☐

4. SIEŤ A WI-FI

#	Opatrenie	ÁNO	NIE
17	Firemná Wi-Fi používa šifrovanie WPA2 alebo WPA3 a silné heslo.	☐	☐
18	Zákazníci a návštevy majú samostatnú hosťovskú Wi-Fi sieť.	☐	☐
19	Na verejnej Wi-Fi sa neprihlasujeme do bankingu (používame mobilné dáta).	☐	☐

5. E-MAILY, PLATBY A PODVODY

#	Opatrenie	ÁNO	NIE
20	Zamestnanci vedia rozpoznať phishing (nátlak, podozrivý odosielateľ, cudzí odkaz, žiadosť o heslo).	☐	☐
21	Zmenu čísla účtu dodávateľa vždy overujeme telefonicky na známom čísle.	☐	☐
22	Väčšie alebo neobvyklé platby schvaľujú dvaja ľudia.	☐	☐
23	Podozrivé e-maily zamestnanci hlásia, nie mažú potichu.	☐	☐

6. PRÍSTUPY A ĽUDIA

#	Opatrenie	ÁNO	NIE

24	Máme zoznam, kto má prístup ku ktorým účtom a systémom (tabuľka nižšie).	☐	☐
25	Každý má len tie oprávnenia, ktoré potrebuje na prácu.	☐	☐
26	Pri odchode zamestnanca rušíme prístupy v posledný deň a meníme zdieľané heslá.	☐	☐
27	Zamestnanci za posledných 12 mesiacov absolvovali školenie kybernetickej bezpečnosti.	☐	☐

7. PLÁN PRE PRÍPAD ÚTOKU

#	Opatrenie	ÁNO	NIE
28	Vieme, koho volať: banka, IT podpora, SK-CERT, polícia (kontakty nižšie).	☐	☐
29	Vieme, že výkupné neplatíme a údaje obnovujeme zo zálohy.	☐	☐
30	Vieme, kto posúdi, či pri úniku osobných údajov treba do 72 hodín informovať Úrad na ochranu osobných údajov SR.	☐	☐

TABUĽKA PRÍSTUPOV

Účet / systém	Kto má prístup	2FA zapnuté?	Posledná zmena hesla
Firemný e-mail			
Internet banking			
Účtovný softvér			
Web / e-shop			
Sociálne siete			

DÔLEŽITÉ KONTAKTY PRI ÚTOKU

Banka – blokovanie karty / platby	_____
IT podpora / správca siete	_____
SK-CERT – nahlásenie incidentu	sk-cert.sk (formulár „Nahlásiť incident“)
Polícia (podvod, krádež peňazí)	158
Zodpovedná osoba za GDPR	_____

Týka sa vás zákon o kybernetickej bezpečnosti (NIS2)?

- Zákon č. 69/2018 Z. z. v znení novely č. 366/2024 Z. z. (účinná od 1. 1. 2025) sa týka najmä stredných a veľkých subjektov vo vymenovaných odvetviach (energetika, doprava, zdravotníctvo, digitálna infraštruktúra, potraviny, výroba, verejná správa a ďalšie).
- Niektoré subjekty sú povinné bez ohľadu na veľkosť (napr. poskytovatelia DNS, dôveryhodných a telekomunikačných služieb).
- Povinné subjekty sa registrujú v JISKB pri Národnom bezpečnostnom úrade do 60 dní od začatia činnosti.
- Ak si nie ste istí, overte si to na nbu.gov.sk alebo s právnikom.

Pripravila nezisková organizácia Digitálne zručnosti, n.o. – digitalnezrucnosti.sk. Školenia kybernetickej bezpečnosti pre zamestnancov: digitalnezrucnosti.sk/sluzby/vzdelavanie-zamestnancov/. Checklist nenahrádza právne poradenstvo.