EFAA za MSP – Kontrolni seznam za kibernetsko varnost

Praktičen, primerno obsežen pregled za računovodske in svetovalne prakse MSP/SMP ter njihove stranke.

Zakaj je to pomembno

Izvajalci računovodskih in svetovalnih storitev hranijo nekatere najobčutljivejše informacije svojih strank - davčne podatke, podatke o plačah, računovodske izkaze in identifikacijske podatke - zato so privlačna tarča za izsiljevalsko programsko opremo, goljufije z računi in plačili ter kompromitacijo poslovne elektronske pošte. En sam incident lahko zmoti roke za oddajo, povzroči kršitev zaupnosti strank in omaje zaupanje, od katerega je praksa odvisna.

Kibernetska varnost je zato poslovno vprašanje in vprašanje poklicne odgovornosti, ne le tehnično vprašanje, vse bolj pa se prepleta tudi z obveznostmi po GDPR in NIS2.

Ta kontrolni seznam vam pomaga pregledati ključne zaščitne ukrepe pri načrtovanju in izvajanju dela ter se z lastniki, zaposlenimi in strankami pogovoriti o osnovnih ukrepih. Namenoma je pripravljen na visoki ravni in prilagojen velikosti podjetja - obravnavajte ga dosledno, ne površno.

Kako ga uporabljati

Skupaj z lastnikom / partnerji ter ključnimi zaposlenimi preglejte šest področij in označite ☐ pri vsakem zaščitnem ukrepu, ki je dejansko vzpostavljen. Stolpci XS / S / M prikazujejo pričakovano raven za zelo majhna, majhna in srednja velika podjetja.

- ● zaščitni ukrep mora biti vzpostavljen in, kjer je relevantno, tudi zapisan.
- ○ sprejemljiva je enostavnejša, neformalna različica - z rastjo podjetja jo je treba nadgraditi.

Postavke, označene z ●, so neizogibno osnovna raven za vsako podjetje, ne glede na njegovo velikost. Kontrolni seznam ponovno izvedite vsaj enkrat letno in po vsaki večji spremembi, kot so nova poslovna aplikacija, selitev pisarne, ključna zaposlitev ali odhod zaposlenega.

Prilagoditev glede na velikost prakse

Velikost prakse	**Tipično število zaposlenih**	**Kaj pomeni »dobro«**
Zelo majhna (XS)	Samostojni izvajalec do približno 5 oseb	Pogosto brez lastne IT-službe. Varnost temelji predvsem na uglednih ponudnikih oblačnih storitev, posodobljenih napravah, MFA in dobrih navadah. Politike naj bodo kratke in praktične.
Majhna (S)	Približno 6–20 oseb	Določite kontaktno osebo za kibernetsko varnost, zapišite ključne politike ter formalizirajte varnostne kopije, preglede dostopov in osnovne korake ob incidentu.

Srednja (M)	Približno 20–50+ oseb, lahko tudi več pisarn	Pričakujejo se dokumentirani kontrolni ukrepi in politike, periodični pregledi dostopov, varnostnih kopij in ključnih varnostnih nastavitev, dokazi o izvedenih usposabljanjih in osnovnih preverjanjih ter testiranje, kjer je relevantno. Razmislite o uskladitvi s priznano osnovo, npr. nacionalno shemo osnovne varnosti ali lažjo obliko ISO 27001.

1 Upravljanje in ozaveščenost

✓	**Zaščitni ukrep** Za srednje velika podjetja ne smejo le obstajati; redno jih je treba pregledovati, odgovornosti morajo biti jasno dodeljene, izvedba usposabljanja pa evidentirana.	**XS**	**S**	**M**
☐	Vodstvo kibernetsko tveganje obravnava kot poslovno tveganje, ne le kot IT-vprašanje, in določena je odgovorna oseba za osnovno spremljanje kibernetske varnosti.	●	●	●
☐	Zaposleni so vsaj enkrat letno deležni osnovnega usposabljanja o phishing prevarah, socialnem inženiringu ter varni uporabi e-pošte, oblačnih orodij in mobilnih naprav.	●	●	●
☐	Obstaja preprosta pisna politika o sprejemljivi uporabi e-pošte, interneta, osebnih naprav in oblačnih storitev, vključno s hrambo podatkov strank.	○	●	●
☐	Podjetje ve, katerega zunanjega IT oz. kibernetskega strokovnjaka bi poklicalo ob resnem incidentu.	●	●	●

2 Dostop, identiteta in gesla

✓	**Zaščitni ukrep** Za M naj pregledi dostopov potekajo po dokumentiranem ciklu, administratorski računi naj bodo ločeno nadzorovani, spremembe ob prihodu, premestitvi ali odhodu zaposlenih pa dokazljive.	**XS**	**S**	**M**
☐	Za vse sisteme, ki vsebujejo podatke strank ali finančne podatke, se uporabljajo edinstveni uporabniški računi; skupnim generičnim prijavam se izogibamo.	●	●	●
☐	Zahtevana so močna gesla ali geselni stavki z najmanj 12 znaki, ki se ne uporabljajo ponovno v različnih sistemih; spodbuja se uporaba upravljalnika gesel.	●	●	●
☐	Večfaktorska avtentikacija (MFA) je omogočena povsod, kjer je mogoče: e-pošta, oblačno računovodstvo, oddaljeni dostop in administratorski računi.	●	●	●
☐	Dostop sledi načelu »potreba po seznanitvi«, se periodično pregleduje, dostopi nekdanjih zaposlenih pa se nemudoma odstranijo.	○	●	●

3 Naprave, popravki in zaščita pred zlonamerno programsko opremo

	Zaščitni ukrep Za M vodite osnovni seznam naprav in programske opreme, spremljajte bolj tvegane popravke ali ranljivosti ter zagotovite dokazila, da so bile ključne posodobitve izvedene.	**XS**	**S**	**M**
☐	Vsi prenosniki, namizni računalniki in strežniki, ki se uporabljajo za poklicno delo, imajo podprte operacijske sisteme in prejemajo samodejne varnostne posodobitve.	●	●	●
☐	Na vseh končnih napravah je nameščena posodobljena protivirusna oziroma protizlonamerna zaščita, kjer je izvedljivo tudi na mobilnih napravah.	●	●	●
☐	Lokalni požarni zidovi so omogočeni, pisarniški Wi-Fi je zavarovan, privzeta gesla usmerjevalnikov oziroma administratorska gesla pa so spremenjena.	●	●	●
☐	Nameščena je samo licencirana in zaupanja vredna programska oprema iz uradnih trgovin z aplikacijami ali s spletnih strani ponudnikov.	●	●	●

4 Varstvo podatkov, oblak in varnostne kopije

	Zaščitni ukrep Za M naj bodo ureditve v zvezi z oblakom in dobavitelji dokumentirane in pregledovane, odgovornosti glede hrambe jasne, testiranje obnovitve pa strukturirano in evidentirano.	**XS**	**S**	**M**
☐	Podjetje vodi pregled ključnih informacijskih sredstev: datoteke strank, delovna gradiva, plače, davčne datoteke in arhivi e-pošte.	●	●	●
☐	Zaupni podatki strank so šifrirani; prenosniki in prenosni nosilci uporabljajo šifriranje celotnega diska.	●	●	●
☐	Uporaba oblačnih storitev je dokumentirana, jasno pa je tudi, kdo je odgovoren za varnostne nastavitve v okviru deljene odgovornosti.	○	●	●

5 E-pošta, ribarjenje in delo na daljavo

	Zaščitni ukrep Za M naj bodo pravila oddaljenega dostopa strožje urejena, uporaba zasebnih naprav za službene namene naj bo omejena ali pogojena, bolj tvegani vzorci dostopa pa naj se pregledajo, kjer je izvedljivo.	**XS**	**S**	**M**
☐	Zaposleni so usposobljeni za prepoznavanje sumljivih e-poštnih sporočil, prilog, povezav in zahtevkov za spremembo plačil ter vedo, kako jih prijaviti.	●	●	●
☐	Vzpostavljeni so osnovni varnostni ukrepi za e-pošto: filtriranje neželene pošte, pregledovanje prilog in blokiranje očitno nevarnih vrst datotek.	●	●	●
☐	Oddaljeni dostop, kot so VPN, oddaljeno namizje in oblačni portali, uporablja večfaktorsko avtentikacijo (MFA) in je omejen na odobrene naprave.	●	●	●

☐	Pravila urejajo uporabo osebnih naprav za delo (BYOD): minimalne varnostne nastavitve in mesta, kjer se lahko hranijo podatki strank.	○	●	●

6 Odziv na incidente in neprekinjeno poslovanje

✓	**Zaščitni ukrep** Za M vodite dnevnik incidentov, evidentirajte nadaljnje ukrepe, dodelite vloge pri odzivu in občasno izvedite pregled postopka ali simulacijsko vajo.	**XS**	**S**	**M**
☐	Obstaja preprost pisni kontrolni seznam za odziv na incidente: koga obvestiti, kako izolirati sisteme ter kdaj obvestiti stranke in pristojne organe.	○	●	●
☐	Opredeljeni so kritični procesi, kot so obračun plač, obračuni DDV, zakonsko poročanje in revizijsko delo na terenu, skupaj z vsaj osnovnim načrtom neprekinjenega poslovanja.	○	●	●
☐	Ključni kontaktni podatki, kot so odločevalci, IT-podpora, svetovalci in zavarovalnice, so shranjeni brez povezave in redno posodobljeni.	●	●	●
☐	Pomembni incidenti se naknadno pregledajo in vodijo do konkretnih nadaljnjih ukrepov, kot so dodatna usposabljanja ter izboljšave procesov ali kontrol.	○	●	●

Hitra samoocena

- ● Označeni so vsi bistveni ukrepi in večina ostalih - osnova je dobra; redno jo posodabljajte in testirajte.
- ● Večina bistvenih ukrepov je vzpostavljena, nekaj vrzeli ostaja - najprej prednostno uredite neoznačene postavke ●.
- ● Manjka več bistvenih ukrepov - obravnavajte jih prednostno; začnite z MFA, varnostnimi kopijami, posodobitvami in usposabljanjem zaposlenih.

Opomba: Ta kontrolni seznam je pripomoček na visoki ravni in ne nadomešča podrobnih smernic NIS2/GDPR ali nacionalnih smernic za kibernetsko varnost. Prilagodite ga svojemu podjetju in svojim strankam.

Pripomočka za člane ZRS, sept. 2024 **(dostopno z geslom):**

- **Pregled napotkov za IT varnost >>**
- **Protokol v primeru kibernetskega napada >>**