# Samoprocjena razine postavljene zaštite

Upitnik za samoprocjenu se popunjava na način da se prvo utvrdi glavno područje na koje se odnose zaštitne mjere i da li ga poslovni subjekt primjenjuje u svom poslovanju, a onda objektivno za svaku mjeru stavlja oznaka (npr. X) u stupac ovisno o tome da li je navedena mjera uspostavljena, nije ili nije primjenjiva (npr. u poslovanju poslovnog subjekta se ne koristi navedeni uređaj) (stupac n/a). Cilj je za sve mjere imati oznaku u stupcu da, odnosno ako nije primjenjivo u stupcu n/a.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ako se u poslovanju koristi Internet** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li je na Internet usmjerivaču promijenjeno predefinirano korisničko ime i lozinku za administriranje jedinstvenim korisničkim imenom i lozinkom koji su poznati samo zaposlenicima ovlaštenim za administriranje Internet usmjerivača? |  |  |  |
| Da li je Internet usmjerivač nadograđen na posljednju službenu verziju koju je izdao proizvođač Internet usmjerivača? |  |  |  |
| Da li je za bežični pristup kreirana jedinstvena snažna lozinka korištenjem WPA2 sigurnosnog protokola? |  |  |  |
| Da li je na Internt usmjerivaču isključena spajanje na usmjerivaču putem opcije WPS? |  |  |  |
| Da li je isključen udaljeni pristup Internet usmjerivaču s Interneta (tzv. pristup izvana)? |  |  |  |
| Da li je na Internet usmjerivaču isključena opcija Universal Plug and Play (UpnP)? |  |  |  |
| Da li je na Internet usmjerivaču uključena opcija ograničavanja pristupa Internet usmjerivaču putem filtriranja MAC adrese uređaja koje koristite u poslovanju? |  |  |  |
| Da li je Internet usmjerivač postavljen u odgovarajući uredski namještaj (npr. računalne ormare) i/ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa? |  |  |  |
| Da li je postavljen vatrozid? |  |  |  |
| Da li je uspostavljena politika sigurnog korištenja Interneta? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ako se u poslovanju koriste računala** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li svaki ovlašteni zaposlenik koji koristi računalo ima jedinstveno korisničko ime i lozinku za pristup računalu? |  |  |  |
| Da li je operativni sustav na računalima ažuriran na posljednju službenu verziju proizvođača? |  |  |  |
| Da li proizvođač i dalje pruža korisničku podršku (podršku nadogradnje) za sve operativne sustave na računalima koji se koriste u organizaciji? |  |  |  |
| Da li je na svim računalima instaliran antivirusni program? |  |  |  |
| Da li je antivirusni program nadograđen na posljednju verziju programa i kataloga za detekciju računalnih virusa? |  |  |  |
| Da li je na računalima postavljeno automatsko zaključavanje zaslona nakon određenog vremena nekorištenja računala? |  |  |  |
| Da li su računalni serveri postavljeni u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa? |  |  |  |
| Da li su diskovni sustavi koji služe za pohranu podataka postavljeni u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa? |  |  |  |
| Da li su vanjski diskovi postavljeni u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa? |  |  |  |
| Da li su računala, pisači, kopirke,… koji se koriste u interaktivnom radu s korisnicima usluga organizacije fizički odijeljena od korisnika usluga ili im je u najmanju ruku otežan pristup opremi i uvid u podatke? |  |  |  |
| Da li su diskovi prijenosnih računala ili dio diska u kojem se pohranjuju podaci kriptirani? |  |  |  |
| Da li su USB stikovi ili dio USB stikova u kojem se pohranjuju podaci kriptirani? |  |  |  |
| Da li su prijenosni diskovi ili dio prijenosnog diska u kojem se pohranjuju podaci kriptirani? |  |  |  |
| Da li su memorijske kartice ili dio memorijske kartice u kojem se pohranjuju podaci kriptirani? |  |  |  |
| Da li su kada se ne koriste svi prijenosni mediji i prijenosni uređaji pohranjeni u odgovarajući uredski namještaj (npr. ladice, ormare, …) i prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa? |  |  |  |
| Da li su sa opreme koja se više neće koristiti u poslovne svrhe uklonjeni podaci na adekvatan način? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ako se u poslovanju koriste računalni programi i/ili datoteke za pohranu podataka** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li svaki ovlašteni zaposlenik koji koristi program ima jedinstveno korisničko ime i lozinku za pristup programu? |  |  |  |
| Da li su programi ažurirani na posljednju službenu verziju proizvođača? |  |  |  |
| Da li proizvođač i dalje pruža korisničku podršku (podršku nadogradnje) za sve programe koji se koriste u organizaciji? |  |  |  |
| Da li je pristup bazama podataka koje koriste programi zaštićen jedinstvenim korisničkim imenom i lozinkom za svakog za to ovlaštenog zaposlenika/korisnika |  |  |  |
| Da li programi imati automatizirani sustav zapisa za evidentiranje pristupa (tzv. logove)? |  |  |  |
| Da li je svaka datoteka u kojoj se pohranjuju podaci osigurana snažnom lozinkom? |  |  |  |
| Da li su s lozinkom upoznati samo ovlašteni zaposlenici? |  |  |  |
| Da li je za svaku datoteku u kojoj se pohranjuju podaci uspostavljena adekvatna evidencija pristupa podacima? |  |  |  |
| Da li se rade sigurnosne kopije podataka (backup) na adekvatan način? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ako se u poslovanju koristi elektronička pošta za razmjenu podataka** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li se ne navode osobni podaci izvan granica poslovnih kontakt podataka, a pogotovo bilo koji osobni podatak trećih osoba (osoba koje nisu pošiljatelj ili primatelj) |  |  |  |
| Da li su datoteke u kojima su pohranjeni osobni podaci prije slanja zaštićene snažnom lozinkom? |  |  |  |
| Da li su sažete datoteke (zipane) u kojima se nalaze druge datoteke koje sadrže osobne podatke prije slanja zaštićene snažnom lozinkom? |  |  |  |
| Da li se lozinka za pristup poslanim datotekama dostavlja primatelju putem drugog komunikacijskog kanala? |  |  |  |
| Da li je nakon uspješnog prijema elektroničke pošte i pohrane datoteka na računalo primatelja takva elektronička pošta obrisana i kod pošiljatelja i kod primatelja? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ako se u poslovanju koriste pametni telefoni i/ili tablet računala** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li je na pametnim telefonima i tablet računalima uključeno sigurno zaključavanje zaslona? |  |  |  |
| Da li je na pametnim telefonima i tablet računalima uključena opcija brisanja sadržaja uređaja nakon određenog broja neuspjelih pokušaja otključavanja zaslona? |  |  |  |
| Da li su na pametnim telefonima i tablet računalima instalirani samo programi nužni za poslovanje? |  |  |  |
| Da li su poslovni programi zaštićeni jedinstvenim korisničkim imenom i/ili lozinkom? |  |  |  |
| Da li se kontakt podaci (imenici) pohranjuju u pametne telefone i tablet računala, a ne na SIM kartice? |  |  |  |
| Da li je na pametnim telefonima i tablet računalima pohranjeni samo poslovni podaci, a ne i osobni podaci korisnika uređaja? |  |  |  |
| Da li su memorijske kartice (SD kartice) kriptirane? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ako se u poslovanju koristi mrežna infrastruktura i/ili udaljeni pristup** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li su mrežni preklopnici (switch) postavljeni u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa? |  |  |  |
| Da li su utori na mrežnom preklopniku koji se ne koriste stavljeni van funkcije (isključeni) dok se za to ne ukaže potreba? |  |  |  |
| Da li je podešeno koji uređaji mogu međusobno biti povezani (umreženi)? |  |  |  |
| Da li je podešeno koji uređaji imaju pravo pristupa Internetu? |  |  |  |
| Da li je za povezivanje izdvojenih lokacija, odnosno udaljeni pristup uspostavljena tzv. virtualna privatna mreža (VPN)? |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ako se u poslovanju koriste podaci pohranjeni u papirnatom obliku** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li je propisano koji zaposlenici imaju pravo pristupa tim podacima? |  |  |  |
| Da li se podaci pohranjuju u odgovarajući uredski namještaj (npr.ladice, ormare) i/ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa? |  |  |  |
| Da li se nakon prestanka svrhe čuvanja podataka u papirnatom obliku takvi dokumenti uništavaju pomoću rezača papira? |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Organizacijske zaštitne mjere** | | | |
|  | **Da** | **Ne** | **n/a** |
| Da li je kod svih zaposlenika podignuta svijest o važnosti zaštite podataka? |  |  |  |
| Da li je propisan pravilnik o informacijskoj sigurnosti? |  |  |  |
| Da li su propisane ovlasti tko ima pravo pristupa osobnim podacima? |  |  |  |
| Da li je propisano za svaki poslovni proces opseg osobnih podataka samo u onoj mjeri koja je nužna za svrhu u koju se podaci obrađuju (za kvalitetno obavljanje posla)? |  |  |  |
| Da li su za svaki poslovni proces propisani rokovi čuvanja osobnih podatka? |  |  |  |