Awareness raising campaign for SMEs

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

VODIČ ZA INFORMACIJSKU SIGURNOST

namijenjen mikro, malim i srednjim poduzetnicima

Croatian Personal Data Protection Agency
azop
Agencija za zaštitu osobnih podataka

An Coimisiún um Chosaint Sonraí
Data Protection Commission

VUB
VRIJE UNIVERSITEIT BRUSSEL

VODIČ

ZA INFORMACIJSKU SIGURNOST

NAMIJENJEN MIKRO, MALIM I SREDNJIM PODUZETNICIMA

Sadržaj

1. Što su osobni podaci i koje su zakonske obveze zaštite osobnih podataka..... 2
2. Podizanje svijesti o važnosti zaštite podataka 3
3. Određivanje/propisivanje ovlasti tko ima pravo pristupa osobnim podacima (pravilnici o pristupu podacima, izjava o povjerljivosti ili dio ugovora) 3
4. Prikupljanje/obrada osobnih podataka samo u onoj mjeri koja je nužna za svrhu u koju se podaci obrađuju (za kvalitetno obavljanje posla) 4
5. Rok čuvanja osobnih podataka 5
6. Vođenje evidencije pristupa osobnim podacima 6
7. Korištenje lozinke za pristup opremi, računalnim programima i datotekama..... 6
8. Zaštita računala, programa i elektroničke pošte (e-mail) od neovlaštenog pristupa 8
9. Zaštita računalnih datoteka od neovlaštenog pristupa 8
10. Zaštita prijenosnih uređaja (prijenosnih računala (eng. laptop ili notebook), pametnih telefona i tablet računala (eng. smartphone i tablet) od neovlaštenog pristupa..... 9
11. Nadogradnja operativnog sustava i računalnih programa..... 10
12. Postavljanje antivirusnog programa i politika sigurnog korištenja Interneta 10
13. Postavljanje vatrozida (firewalla) 11
14. Zaštita Internet usmjerivača (eng. Internet Router) od neovlaštenog pristupa 11
15. Zaštita pristupa mrežnoj infrastrukturi 13
16. Zaštita pristupa podacima udaljenih lokacija od neovlaštenog pristupa..... 13
17. Kriptiranje podataka i prijenosnih uređaja 14
18. Razmjena podataka putem elektroničke pošte 14
19. Zaštita podataka pohranjenih u papirnatom obliku 15
20. Oprema koja se više ne koristi 15
21. Pristup opremi i programima putem kartica s čipom 16
22. Sigurnosne kopije podataka (Backup) 17
23. Fizička zaštita od nedozvoljenog pristupa..... 19
24. Kako uspostaviti informacijsku sigurnost u poslovnom subjektu? 19
25. Samoprocjena razine postavljene zaštite 20

1. Što su osobni podaci i koje su zakonske obveze zaštite osobnih podataka

Opća uredba o zaštiti podataka definira da su osobni podaci svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ("ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. Dakle, svi podaci pomoću kojih se može identificirati pojedinac/osoba, bilo kao samostalni podaci (izravno) ili povezani s drugim podacima (neizravno), predstavljaju osobne podatke.

Nadalje, Opća uredba o zaštiti podataka definira i posebnu kategoriju osobnih podataka, a to su podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu, genetski podaci, biometrijski podaci u svrhu jedinstvene identifikacije pojedinca, podaci koji se odnose na zdravlje ili podaci o spolnom životu ili seksualnoj orijentaciji pojedinca. Takvi podaci se ne smiju obrađivati osim ako je uz postojanje pravnog temelja iz članka 6. stavka 1. Opće uredbe o zaštiti podataka ispunjeno jedno od sljedećeg:

- ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha;
- obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava poslovnog subjekta ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti;
- obrada je nužna za zaštitu životno važnih interesa ispitanika;
- obrada se provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zaklade, udruženja ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem te pod uvjetom da se obrada odnosi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s njom u vezi s njezinim svrhama i da osobni podaci nisu priopćeni nikome izvan tog tijela bez privole ispitanika;
- obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;
- obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu;
- obrada je nužna za potrebe značajnog javnog interesa koje je razmjerno željenom cilju te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika;
- obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama;
- obrada je nužna u svrhu javnog interesa u području javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanje visokih standarda kvalitete i sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda ispitanika, posebno čuvanje profesionalne tajne;
- obrada je nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe koje je razmjerno cilju koji se nastoji postići te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

Također, Opća uredba o zaštiti podataka propisuje da su svi poslovni subjekti obvezni poduzeti odgovarajuće organizacijske i tehničke mjere kako bi se ti podaci zaštitili, ovisno o količini i vrsti osobnih podataka, njihovom kontekstu, svrsi zbog koje se prikupljaju/obrađuju, kao i mogućim rizicima za njihov gubitak ili zlouporabu. (članak 24., 25. i 35. Opće uredbe o zaštiti podataka).

2. Podizanje svijesti o važnosti zaštite podataka

S razlogom se odmah na početku ovog vodiča obrađuje tema podizanja svijesti o važnosti informacijske sigurnosti. Ljudski faktor je najbitniji u postupku provođenja informacijske sigurnosti i zaštite podataka i ako kod svih zaposlenika (od direktora do pomoćnog osoblja) nije postignuta svijest o važnosti informacijske sigurnosti i odgovornosti svakog pojedinca o zaštiti podataka sve ostale preporuke i propisane mjere zaštite neće imati puno značaja.

Ukoliko samo jedan zaposlenik nije toga svjestan i zanemaruje mjere informacijske sigurnosti i zaštite podataka, ugrožava cjelokupan sustav poslovnog subjekta u kojem radi i izlaže ga potencijalnoj krađi, zlouporabi i gubitku osobnih i drugih poslovnih podataka koji se prikupljaju i obrađuju tijekom poslovanja. Ovisno o kategorijama "izgubljenih" podataka i njihovoj količini, posljedice mogu biti vrlo pogubne za poslovni subjekt, a posljedično i za samog neodgovornog zaposlenika.

Od iznimne važnosti je da svi zaposlenici, bez obzira na kojoj se poslovnoj razni nalaze ("od direktora do pomoćnog osoblja"), budu svjesni:

- koje sve osobne podatke koriste i obrađuju u svom svakodnevnom radu
- kojim kategorijama osobnih podataka ti podaci pripadaju,
- gdje se ti podaci nalaze,
- koji su potencijalni rizici od krađe, zlouporabe i gubitka tih podataka,
- na koji način te podatke mogu zaštititi,
- kako se to negativno može reflektirati na poslovni subjekt u kojem rade, a u krajnjoj mjeri i na njih same,
- da je potrebno svakodnevno se pridržavati preporučenih i propisanih mjera zaštite radi smanjenja potencijalnih rizika od neovlaštenog pristupa i zlouporabe na najmanju moguću mjeru.

Stoga je vrlo bitno da svaki zaposlenik bude upoznat sa preporukama i propisanim pravilnicima odnosno politikama informacijske sigurnosti poslovnog subjekta u kojem radi te da se u svom radu pridržava propisanih mjera.

3. Određivanje/propisivanje ovlasti tko ima pravo pristupa osobnim podacima (pravilnici o pristupu podacima, izjava o povjerljivosti ili dio ugovora)

Ovisno o poslovnom subjektu, tj. broju zaposlenika i poslovnim procesima koje zaposlenici rade, odnosno njihovim radnim mjestima, nije preporučljivo da zaposlenici znaju osobne (i druge) podatke koji se u poslovnom subjektu prikupljaju i obrađuju, a nisu vezani za poslovne procese njihovog radnog mjesta.

Kao mjera zaštite osobnih podataka od neovlaštenog pristupa unutar poslovnog subjekta potrebno je odrediti koja radna mjesta, sukladno poslovnim procesima koje

obavljaju, imaju pravo pristupa i kojem opsegu osobnih (i drugih) podataka koji su nužni za kvalitetno obavljanje njihovog posla.

Ovisno o veličini poslovnog subjekta i raspoloživim resursima to se može urediti putem internih pravilnika o sistematizaciji radnih mjesta i opisu poslova, biti sastavni dio ugovora o radu ili regulirano putem Izjava o povjerljivosti.

Primjer 1.

Poslovni subjekt se bavi prodajom dijelova za vozila i ima sjedište, skladište i prodavaonica na udaljenim lokacijama. Jedna od poslovnih politika u poslovnom subjektu je da se na zahtjev kupca omogući da mu se željeni dio dostavi na kućnu adresu ukoliko nekog dijela trenutno nema u trgovini, ili ukoliko je dio većih dimenzija. Isporuka dijelova kupcima obavlja se iz skladišta poslovnog subjekta.

Kupac je u prodavaonici iskazao želju za dostavom dijelova za vozilo na kućnu adresu te prodavač od kupca prikuplja i obrađuje ime i prezime kupca, njegovu adresu i broj telefona kako bi mogli dostaviti dijelove i obavijestiti ga da je proces dostave u tijeku. Zaposlenik kadrovskih poslova za kvalitetno obavljanje svojih poslova nema potrebe biti upoznat s tim osobnim podacima kupca koje za kvalitetno obavljanje svojih poslovnih procesa prikuplja i obrađuje prodavač u prodavaonici. S druge strane, zaposlenik u skladištu treba biti upoznat s tim osobnim podacima kupca koje je prikupio i obradio prodavač kako bi sukladno poslovnom procesu dostave mogao obaviti dostavu dijelova kupcu.

U sjedištu je zaposlen zaposlenik koji se bavi kadrovskim poslovima poslovnog subjekta (obradom podataka zaposlenika za sklapanje ugovora, prijava na HZMO…). Zbog zakonskih obveza i radi prirode poslovnog procesa zaposlenik koji se bavi kadrovskim poslovima među inim prikuplja i podatke o adresi stanovanja zaposlenika poslovnog subjekta, članovima obitelji, zdravstvenom stanju zaposlenika itd. Zaposlenik u skladištu ili zaposlenik u prodavaonici za kvalitetno obavljanje svog posla nema potrebe biti upoznat s osobnim kadrovskim podacima drugih zaposlenika koje prikuplja i obrađuje zaposlenik kadrovskih poslova.

Primjer 2.

Frizerski salon se sastoji od vlasnika salona i dvoje zaposlenika. Vlasnik salona među inim obavlja i kadrovske poslove, a i zajedno sa zaposlenicima pruža frizerske usluge svojim korisnicima. Zbog zakonskih obveza i radi prirode poslovnog procesa kadrovskih poslova, vlasnik prikuplja i podatke o adresi stanovanja zaposlenika, članovima obitelji, zdravstvenom stanju zaposlenika, itd. Zaposlenici salona za kvalitetno obavljanje svog posla nemaju potrebe biti upoznati s kadrovskim osobnim podacima drugih zaposlenika koje prikuplja i obrađuje vlasnik salona. S druge strane vlasnik salona zajedno s zaposlenicima ima potrebu biti upoznat s osobnim podacima korisnika koji se prikupljaju i obrađuju o njima kako bi mogli kvalitetno pružati frizerske usluge.

4. Prikupljanje/obrada osobnih podataka samo u onoj mjeri koja je nužna za svrhu u koju se podaci obrađuju (za kvalitetno obavljanje posla)

Kao jedna od mjera informacijske sigurnosti, a isto to propisuje i Opća uredba o zaštiti podataka, je i prikupljanje osobnih podataka koji su primjereni, relevantni i ograničeni

na ono što je nužno u odnosu na svrhe u koje se obrađuju ("smanjenje količine podataka").

Dakle, potrebno je prikupljati samo onaj opseg osobnih podataka nužan za kvalitetno obavljanje pojedinog poslovnog procesa.

Na taj način se prevenira da u slučaju eventualne krađe osobnih podataka opseg tih podataka bude sveden na najmanji mogući minimum.

Primjer 1.

Frizerski salon od svojih korisnika prikuplja ime, prezime i broj telefona kako bi mogao kontaktirati korisnika o eventualnoj promjeni termina pružanja usluge. Nema potrebe da se u frizerskom salonu obrađuju datum rođenja korisnika usluge, OIB korisnika, preslika osobne iskaznice, itd. Ovi podaci nisu nužni kako bi frizerski salon korisniku pružio frizerske usluge.

Primjer 2.

Poslovni subjekt koji se bavi prodajom dijelova za vozila u svom poslovanju se koristi računalima i računalnim programima. Podatke o kupcu (fizičkoj osobi) koji želi dostavu dijelova na kućnu adresu unose u računalni program. Kako bi jednoznačno označili kupca u programu prodavač od kupca traži OIB kao jedinstvenu identifikacijsku oznaku građana Republike Hrvatske. Poslovni subjekt za prikupljanje i obradu OIB-a nema pravni temelj i zakonsku svrhu i za jedinstveno označavanje kupca treba iznaći drugi, sebi svojstven način jednoznačnog označavanja kupca.

5. Rok čuvanja osobnih podataka

Još jedna mjera informacijske sigurnosti, a koja je također propisana i Općom uredbom o zaštiti podataka je da se osobni podaci čuvaju samo onoliko dugo koliko je potrebno u svrhe radi kojih se ti osobni podaci obrađuju.

Cilj uspostavljanja ove mjere sa stajališta informacijske sigurnosti je, isto kao i kod prethodne mjere, da se u slučaju eventualne krađe osobnih podataka, odnosno neovlaštene ili nezakonite obrade opseg tih podataka svede na najmanji mogući minimum.

Dakle, svaki poslovni subjekt neprestano treba voditi računa da iz svojih sustava obrade osobnih podataka ukloni one osobne podatke za koje je prestala svrha njihove obrade i zakonska obveza njihovog čuvanja.

Primjer 1.

Frizerski salon i poslovni subjekt koji se bavi prodajom dijelova će kadrovske osobne podatke o svojim zaposlenicima obrađivati i čuvati onoliko dugo koliko je svrha njihove obrade i koliko to nalažu radno pravni zakonski propisi.

Primjer 2.

Frizerski salon je od korisnika prikupio ime, prezime i broj telefona kako bi mogao kontaktirati korisnika o eventualnoj promjeni termina pružanja usluge. Došao je dan dogovorenog termina, korisniku je pružena frizerska usluga i frizerski salon više nema potrebu i dalje čuvati te podatke o korisniku.

Primjer 3.

Kupac je u prodavaonici poslovnog subjekta koja se bavi prodajom dijelova za vozila iskazao želju za dostavom dijelova za vozilo na kućnu adresu te su od kupca prikupljeni i unijeti u računalni program za izradu dostavnice ime i prezime kupca, njegova adresa i broj telefona kako bi mu se mogli dostaviti dijelovi i obavijestiti ga da je proces dostave u tijeku. Dijelovi su dostavljeni kupcu te je kupac na dostavnici nedvojbeno potvrdio kako je preuzeo kupljene dijelove za vozilo. Nakon toga poslovni subjekt nema više potrebu čuvati gore navedene podatke o kupcu u računalnom programu za izradu dostavnice.

6. Vođenje evidencije pristupa osobnim podacima

Kao još jedna mjera zaštite od neovlaštenog pristupa osobnim podacima koristi se mjera vođenja evidencije pristupa osobnim podacima.

Poslovni programi bi trebali imati (bilo bi uputno) automatizirani sustav zapisa za evidentiranje pristupa osobnim podacima (tzv. logove) u kojima se evidentiraju podaci o korisnicima koji su pristupali poslovnom programu, vremenu kada su pristupali programu i podacima u programu te što su s tim podacima radili (unosili nove podatke, ažurirali postojeće, brisali podatke, vršili uvid u podatke, pohranjivali podatke izvan programa, ispisivali podatke,…).

Ukoliko niste upoznati s činjenicom da li poslovni programi koje koristite imaju takav sustav za evidentiranje pristupa konzultirajte se s proizvođačem programa. Ukoliko program nema takav sustav evidencije pristupa potrebno ga je nadograditi s tom mogućnošću.

Datoteke načelno nemaju mogućnost automatiziranog sustava zapisa za evidentiranje pristupa kao što je prethodno opisano. Stoga je za datoteke potrebno evidenciju pristupa voditi na neki drugi način, na primjer, korištenjem posebne datoteke u koju će se voditi evidencija pristupa (podatak o datoteci kojoj se pristupalo, tko je pristupao, kada je pristupao, što je radio s podacima…).

Operativni sustavi na računalima (Windows, Linux, macOS…) u sebi imaju ugrađenu evidenciju pristupa (tzv. logove) u kojima u osnovi vode evidenciju prijave i odjave korisnika u računalo, odnosno operativni sustav. Stoga se njihove evidencije pristupa ne mogu smatrati evidencijama pristupa osobnim podacima, ali mogu pomoći za identificiranje kada je i koliko dugo određeni korisnik pristupao tom računalu.

7. Korištenje lozinke za pristup opremi, računalnim programima i datotekama

Lozinka se koristi kao mjera zaštite od neovlaštenog pristupa opremi, računalnim programima, elektroničkoj pošti i datotekama s podacima.

Snažna sigurnosna lozinka sadrži:

- 16 ili više znakova, što više to bolje,
- velika slova (ABCDEFGH…),
- mala slova (abcdefgh…),
- brojke (123456…),
- simbole (@#$%{ } [ ] ( ) / \ ' " , ; : . < >…).

Kod kreiranja lozinke treba izbjegavati:

- riječi iz rječnika, a pogotovo na engleskom jeziku (aeroplane, laptop, RedSox, automobil, bicikl, računalo,…),
- često korištene i opće poznate lozinke (password, default, admin, guest, …,),
- naše osobne podatke ili podatke naših bližnjih (ime i/ili prezime, datum rođenja, vjenčanja, zaposlenja, adresa stanovanja, imena djece, bliže rodbine, kućnog ljubimca, ime firme…(primjerice, IvanaHorvat, Petar 14.02.1988., 14.02.1988., Ilica 111, 10000 Zagreb…)
- korisničko ime (ivana.horvat, ihorvat,…),
- niz istih slova, brojki ili znakova (aaaaa, aaaa1111, aa11++, ..)
- ponavljanje istih riječi (markomarko, avionavion,…)
- nizove slova i/ili brojki na tipkovnici (qwertz, 123456, 1q2w3e4r5t, …)
- općepoznati identifikacijski podatak (npr. OIB, broj zdravstvenog osiguranja (MBO), broj službene iskaznice, registarska oznaka vozila, adresa radnog mjesta, kat i broj ureda…) (, ZG-2324-BC, Selska 136,…)
- slabo kreirane lozinke ili slabo pretvorene fraze (password123, lozinka356, john1234, ivana12345, p@ssw0rd, l0z1nk@).

Za kreiranje snažnih lozinki na Internetu postoje generatori lozinki koji ih kreiraju na temelju zadanih postavki od čega se sve treba sastojati lozinka (primjer generirane lozinke: UZCQf]&}q{f4c+ct).

Tako generirane lozinke (nasumičan niz slova, brojki i simbola) je teško upamtiti. Stoga možete pribjeći triku da za generiranje lozinke odaberete nekakvu frazu ili citat. Zatim dodate simbole, a neka slova zamijenite brojkama ili simbolima (npr. iz fraze "Voćka poslije kiše" može nastati lozinka %V0ćk@=p0sl1j3=k1š3). Takvu lozinku je puno lakše zapamtiti nego nasumični niz slova, brojki i simbola.

Snažne lozinke nije potrebno periodično mijenjati, kako su do sad bile sigurnosne preporuke. Istraživanja su pokazala da zbog učestalog mijenjanja lozinki i potrebe kreiranja jedinstvene lozinke za pristup svakoj opremi i svakom programu, korisnici počinju primjenjivati manje sigurne lozinke, odnosno iste lozinke za više uređaja i programa. Snažnu lozinku je potrebno promijeniti na uređaju ili u programu u slučaju sumnje kako je ista kompromitirana od strane neovlaštenog korisnika i omogućuje neovlašten pristup.

Vrlo važno je napomenuti kako je potrebno voditi računa da se lozinke ne pohranjuju, odnosno zapisuju na lako dostupnim mjestima (npr. na papirićima zalijepljenim na opremu ili spremljenim ispod opreme, u rokovnicima ili bilježnicama koji se nalaze na radnim površinama…).Lozinke je potrebno pohraniti u adekvatno osiguran uredski namještaj ili neko drugo mjesto kojem samo ovlašteni zaposlenik ima pristup (npr. zaposlenik papir na kojem se nalazi njegovo korisničko ime i lozinka za pristup računalu drži u zaključanoj ladici uredskog stola od koje samo on ima ključ).

Ukoliko poslovni subjekt u poslovanju koristi više programa i zaposlenici koriste veći broj korisničkih imena i lozinki, rad si mogu olakšati korištenjem tzv. alata za upravljanje lozinkama (eng. password manager) kako ne bi morali pamtiti ili zapisivati sve te lozinke.

8. Zaštita računala, programa i elektroničke pošte (e-mail) od neovlaštenog pristupa

Kao mjera zaštite od neovlaštenog pristupa računalu, računalnim programima i elektroničkoj pošti koriste se korisničko ime i lozinka/zaporka (eng. user name i password).

Svaki zaposlenik treba imati jedinstveno korisničko ime i lozinku radi zaštite od neovlaštenog pristupa za:

- računalo na kojem radi (stolno ili prijenosno),
- poslovne programe koje koristi u poslovne svrhe,
- adrese elektroničke pošte (e-mail) koje koristi u poslovne svrhe.

Svoja korisnička imena i lozinke zaposlenici ne bi trebali otkrivati ostalim zaposlenicima. Ukoliko je to iz iznimnih i opravdanih razloga potrebno (npr. zaposlenik je na dužem bolovanju pa je potrebno pristupiti njegovom računalu, poslovnim programima i/ili adresi elektroničke pošte), nakon što su ti razlozi prošli zaposlenik bi trebao odmah zamijeniti stare lozinke novim.

Preporučljivo je, u slučaju izbivanja s radnog mjesta na kom se nalazi računalo ili dužeg vremena nekorištenja napraviti odjavu iz sustava (tzv. logout), odnosno postaviti automatsko zaključavanje zaslona nakon određenog vremena nekorištenja računala

Poslovna računala prvenstveno treba gledati kao alat za rad te ih stoga koristiti isključivo u poslovnu, a ne i u privatnu svrhu. Na njima bi trebali biti instalirani samo poslovni programi nužni za redovno obavljanje posla i pohranjeni samo poslovni podaci. Instaliranjem dodatnih programa koji se ne koriste za poslovanje, a pogotovo programa iz neprovjerenih izvora (eng. untrusted sources) i nesigurnih proizvođača (eng. untrusted developers) povećava se rizik od neovlaštenog pristupa računalu. Ukoliko dođe do neovlaštenog pristupa računalu, a na njemu su pohranjeni privatni osobni podaci (npr. fotografije, preslike osobnih dokumenata…) i njima se može neovlašteno pristupiti i zlorabiti ih.

9. Zaštita računalnih datoteka od neovlaštenog pristupa

Računalne datoteke (npr. Word dokumenti, Excel tablice,…) za razliku od računala, računalnih programa i elektroničke pošte kao mogućnost zaštite od neovlaštenog pristupa imaju samo zaštitu putem lozinke.

Stoga je za računalne datoteke od iznimne važnosti odrediti prava pristupa datotekama za radna mjesta, koja ovisno o poslovnim procesima prikupljaju i obrađuju podatke u tim datotekama.

Datoteke je potrebno zaštititi putem snažne lozinke, a lozinku za otključavanje datoteke trebaju znati samo zaposlenici koji za to imaju dodijeljene ovlasti. Preporučljivo bi bilo voditi evidenciju tko je pristupao datoteci, kada, u koju svrhu i što je radio u njoj.

10. Zaštita prijenosnih uređaja (prijenosnih računala-eng. laptop ili notebook, pametnih telefona i tablet računala-eng. smartphone i tablet) od neovlaštenog pristupa

Prijenosna računala se kao i stolna računala od neovlaštenog pristupa štite korisničkim imenom i lozinkom.

Pametni telefoni i tablet računala imaju različite vrste zaštite od neovlaštenog pristupa (tzv. zaključavanje zaslona) ovisno o operativnom sustavu koji se na njima nalazi (Android, iOS, Mobile Windows…) i opcija koje je proizvođač uređaja ugradio u njih.

Tako se pametni telefoni i tablet računala od neovlaštenog pristupa mogu zaštititi putem:

- PIN-a (niz 4 ili više znamenki koje korisnik odabere),
- Uzorka (polje s 3x3 točke koje korisnik međusobno spaja kako želi),
- Lozinke/zaporke
- Otiska prsta,
- Prepoznavanja lica korisnika,
- Očitavanja (skeniranja) šarenice oka,
- Očitavanja i lica i šarenica oka.

Zaštita od neovlaštenog pristupa putem PIN-a i uzorka pripada jednostavnijim načinima zaštite te ukoliko je moguće preporučljivije je koristiti lozinku kao mjeru zaštite od neovlaštenog pristupa. Ukoliko se koristi neka od ove tri vrste zaštite potrebno ih je periodično mijenjati.

Kako su svi prijenosni uređaji zbog svoje karakteristike da se mogu koristiti bilo gdje podložniji gubitku ili krađi preporučljivo je uvesti i dodatne mjere zaštite kako bi se zaštitili podaci od neovlaštenog pristupa.

Ukoliko prijenosno računalo ili operativni sustav koji je postavljen (instaliran) na prijenosnom računalu imaju opciju kriptiranja diska računala, preporučljivo je uključiti navedenu opciju. Na taj način, ukoliko se računalo izgubi ili bude ukradeno podaci na disku čak i nakon njegovog vađenja iz računala i priključivanja na neko drugo računalo neće biti čitljivi te se neće moći zlorabiti

Na pametnim telefonima i tablet računalima, ukoliko postoji ta opcija, preporučljivo je uključiti opciju brisanja sadržaja uređaja nakon određenog broja neuspjelih pokušaja otključavanja zaslona.

Ukoliko se radi dodatnog prostora za pohranu podataka u pametnim telefonima i tablet računalima koriste memorijske kartice (SD kartice), te ukoliko uređaji imaju tu opciju, preporučljivo je kriptiranje memorijskih kartica. Ukoliko uređaji nemaju tu opciju, preporučljivo je ne koristiti memorijske kartice za pohranu podataka.

Kontakt podatke (imenike) u pametnim telefonima (i ako tablet računala koriste mobilne SIM kartice) potrebno je pohranjivati na uređaje, a ne na mobilne SIM kartice.

Isto kao i poslovna stolna računala i poslovne prijenosne uređaje prvenstveno treba gledati kao alat za rad te ih koristiti isključivo u poslovnu, a ne i u privatnu svrhu. Na njima bi trebali biti instalirani samo poslovni programi nužni za redovno obavljanje posla i pohranjeni samo poslovni podaci. Instaliranjem dodatnih programa koji se ne koriste za poslovanje, a pogotovo na pametnim telefonima i tablet računalima (npr.

igrice, programi za društvene mreže, sportski programi…) povećava se rizik od neovlaštenog pristupa tim uređajima. Ukoliko dođe do neovlaštenog pristupa mobilnom uređaju, a na njemu su pohranjeni privatni osobni podaci (npr. fotografije, preslike osobnih dokumenata, privatni imenici…) i njima se može neovlašteno pristupiti i zlorabiti ih.

11. Nadogradnja operativnog sustava i računalnih programa

Redovna nadogradnja operativnog sustava računala i mobilnih uređaja (za računala Windows, Linux, macOS…, za mobilne uređaje iOS, Android, Windows Mobile...) i široko rasprostranjenih računalnih programa (programi iz MS Office paketa, uredskih paketa za druge operativne sustave, programa za sažimanje, programa za izradu sigurnosne kopije (backup)…) od velike je važnosti za informacijsku sigurnost i zaštitu podataka.

Proizvođači redovitim izdavanjem nadogradnji za svoje programske proizvode (operativne sustave i računalne programe) "krpaju" uočene sigurnosne propuste te time kroz njih onemogućuju neovlašten pristup tzv. hakerima, a samim tim i mogućnost krađe osobnih podataka, odnosno njihove neovlaštene ili nezakonite obrade.

Stoga je bitno redovito nadograđivati programske proizvode koji se nalaze na svim poslovnim računalima.

Također je bitno redovito provjeravati da li proizvođač i dalje pruža korisničku podršku (podršku nadogradnje) za programske proizvode koje poslovni subjekt koristi u svom poslovanju. Ukoliko proizvođač prestaje sa pružanjem takve podrške potrebno je preći na novije verzije programskih proizvoda ili kod drugog proizvođača.

Razlog tome je što ukoliko proizvođač za određenu seriju proizvoda (npr. Microsoft ukine korisničku podršku za Windows XP ili Office XP), a i nakon posljednje nadogradnje u proizvodu postoje sigurnosni propusti, korištenje takvih proizvoda predstavlja sigurnosni rizik i ostavlja mogućnost neovlaštenog pristupa hakerima, a samim tim mogućnost krađe osobnih podataka, odnosno njihove neovlaštene ili nezakonite obrade, neovlaštenog preuzimanja kontrole nad računalnim poslovnim sustavom pa čak i mogućnost uništavanja cjelokupnog sustava.

12. Postavljanje antivirusnog programa i politika sigurnog korištenja Interneta

Svako računalo ili pametni mobilni uređaj (smarthpone) na sebi bi trebao imati instaliran i pokrenut antivirusni program. Njihova primarna funkcija je otkrivanje i uklanjanje malicioznih programa (tzv. virusa) na računalu ili mobilnom uređaju koji ovisno od namjene mogu omogućiti neovlašten pristup računalu i računalnom sustavu, krađu podataka, odnosno njihovu neovlaštenu ili nezakonitu obradu, kriptiranje, odnosno zaključavanje podataka na računalu čime oni postaju neupotrebljivi, itd.

Zbog konstantnog razvoja novih vrsta virusa, kako bi antivirusni programi bili maksimalno učinkoviti potrebna je njihova redovita nadogradnja.

Ovdje je potrebno napomenuti, s obzirom da se konstantno razvijaju nove verzije virusa, postoji mogućnost da antivirusni program kojeg koristite još ne sadrži uzorak virusa u svom katalogu za detekciju računalnih virusa te se računalo ipak može zaraziti s virusom. Stoga je osim korištenja antivirusnog programa, bitno kod zaposlenika

podići svijest o sigurnom korištenju elektroničke pošte i sadržaja na Internetu i provoditi politiku sigurnog korištenja Interneta. Osnovna pravila sigurnog korištenja Interneta su:

- prilikom korištenja Interneta posjećivati samo stranice koje su neophodne za obavljanje posla, odnosno službene Internet stranice nekog društva ili institucije,
- ne otvarati elektroničku poštu nepoznatih pošiljatelja i sumnjivog sadržaja (npr. ako je elektroničku poštu poslao Peter Lee s adrese mickey.mouse@mikrosoft.cn već sama adresa pošte je neuvjerljiva i takvu poštu treba obrisati. Ukoliko se sadržaj elektroničke pošte čini kao službeno obraćanje npr. banke i u kom se radi provjere podataka ili ažuriranja sustava od primatelja traži da otvori poveznicu iz sadržaja i na toj Internet stranici unese korisničko ime i lozinku takva pošta nije službena jer niti jedna institucija neće tražiti od korisnika provjeru korisničkih podataka na takav način i poruku treba obrisati.)

13. Postavljanje vatrozida (firewalla)

Vatrozid (eng. firewall) je mrežni sigurnosni sustav čija je namjena zaštita uređaja koji se spajaju na Internet u našem okruženju od neovlaštenog pristupa tim uređajima s Interneta (tzv. hakerskog napada) i zaštitu ostalih sudionika na Internetu od neovlaštenih radnji iz našeg okruženja (hakerski napadi, neželjena elektronička pošta tzv. spam…).

Vatrozid može biti u obliku računalnog programa (tzv. softverski) te je postavljen (instaliran) na pojedino računalo i ima ulogu zaštite tog računala. Također može biti i kao uređaj (tzv. hardverski) i tada mu je namjena zaštita svih uređaja koji su spojeni na njega.

Za podešavanje vatrozida potrebno je poznavanje mrežnih protokola i mrežnih portova te je, ukoliko poslovni subjekt nema zaposlenika koji posjeduje navedeno znanje, za naprednija podešavanja potrebna suradnja adekvatnog vanjskog suradnika.

Neki operativni sustavi u sebi već sadrže vatrozid s unaprijed definiranim postavkama koje u zadovoljavajućoj mjeri štite prosječnog korisnika (korisnik koji se u osnovnoj mjeri koristi Internetom).

Moderni Internet usmjerivači u sebi sadrže vatrozid i obično imaju već predefinirane postavke vatrozida koje i manje informatički obrazovanim korisnicima omogućuju postavke jednostavnije verzije vatrozida kao i dodatna, sofisticiranija podešavanja sigurnosnih postavki za korisnike koji posjeduju višu razinu informatičkog obrazovanja.

14. Zaštita Internet usmjerivača (eng. Internet Router) od neovlaštenog pristupa

Internet usmjerivač je uređaj koji omogućuje spajanje računala i ostale opreme na Internet i dobili ste ga od svog pružatelja Internet usluge (eng. Internet provider) kao opremu za pristup Internetu. Kako je Internet usmjerivač uređaj koji je izravno priključen na Internet i spona je između opreme koju koristite u poslovanju i Interneta, od iznimne je važnosti postaviti kvalitetnu zaštitu od neovlaštenog pristupa. Koraci za kvalitetnu zaštitu Internet usmjerivača nisu teški, a kako ih napraviti na modelu i marki koju Vi koristite opisano je u uputama koje ste dobili uz njega. Ukoliko i dalje niste

sigurni kako to učiniti možete potražiti pomoć službe za korisnike Vašeg pružatelja Internet usluga.

Pružatelji Internet usluga dostavljaju Internet usmjerivače s unaprijed određenim (predefiniranim) korisničkim imenom i lozinkom za administriranje, odnosno podešavanje postavki Internet usmjerivača. Ovisno o marki i modelu Internet usmjerivača ti podaci su općepoznati i ukoliko se ne promjene omogućuju hakerima jednostavan pristup administriranju Internet usmjerivača, a nakon toga i ulazak u poslovni sustav putem Interneta za daljnja zlonamjerna djelovanja. Stoga je vrlo bitno promijeniti predefinirano korisničko ime i lozinku za administriranje jedinstvenim korisničkim imenom i lozinkom koji su poznati samo zaposlenicima ovlaštenim za administriranje Internet usmjerivača.

Svaki Internet usmjerivač kako bi mogao ispravno funkcionirati sadrži u sebi program koji mu to omogućuje, a njegov naziv na engleskom je firmware. Proizvođači Internet usmjerivača nakon uočenih grešaka u radu firmwarea i sigurnosnih propusta u postavkama izdaju novije verzije firmwarea. Stoga ih je potrebno redovno nadograđivati na posljednju službenu verziju koju je izdao proizvođač Internet usmjerivača za model i marku koju Vi koristite.

Preporučljivo je svu opremu koju koristite u poslovanju, a koja treba pristup Internetu povezati s Internet usmjerivačem žičnim putem. Određena oprema, kao što su pametni telefoni i tablet računala, nemaju mogućnost povezivanja žičnim putem te je navedenu opremu potrebno s Internet usmjerivačem povezati bežičnim putem (tzv. Wi-Fi). Tada je u postavkama usmjerivača potrebno lozinku za bežični pristup definirati korištenjem WPA2 sigurnosnog protokola, a lozinku kreirati sukladno preporukama za snažne lozinke.

Opcija WPS je namijenjena za jednostavnije bežično spajanje uređaja na Internet usmjerivač pritiskom na gumb na usmjerivaču ili putem brojčanog PIN-a. Hakeri vrlo jednostavno mogu doći do PIN-a za bežično spajanje putem WPS-a, stoga je navedenu opciju potrebno isključiti, osim ako Vam zaista nije potrebna.

Noviji Internet usmjerivači dolaze s opcijom koja omogućuje udaljeni pristup usmjerivaču s Interneta (tzv. pristup izvana). Ukoliko nema potrebe za administratorski pristup Internet usmjerivaču izvana, iz sigurnosnih razloga je navedenu opciju preporučljivo isključiti.

Velik broj novijih Internet usmjerivača dolazi s opcijom Universal Plug and Play (UPnP) koja je namijenjena jednostavnom priključivanju modernih kućanskih uređaja (npr. televizora, igraćih konzola…) kako bi se za njihovo priključivanje na usmjerivač izbjeglo prolaženje kroz sve prozore za podešavanje postavki na uređaju. Ukoliko je ova opcija uključena omogućuje virusima administrativni pristup Internet usmjerivaču, stoga ju je potrebno isključiti.

U sigurnosnim postavkama postoji mogućnost ograničavanja pristupa Internet usmjerivaču putem filtriranja MAC adrese uređaja (računalo, mobitel, tablet računalo…). MAC adresa je oznaka dijela uređaja koja omogućuje uređaju spajanje na mobitel, a obično je prikazana u mrežnim postavkama uređaja i prikazana je u obliku 6 parova znamenki odvojenih crticom (01-23-45-67-89-ab) ili 6 parova znamenki odvojenih dvotočkom (01:23:45:67:89:ab). Upisivanjem MAC adresa uređaja koji imaju dozvoljen pristup Internet usmjerivaču onemogućuje se pristup svim drugim uređajima koji se ne nalaze na tom popisu.Potrebno je strogo voditi računa da pristup poslovnom

Internet usmjerivaču i samim tim i pristup Internetu onemogući za zaposlenike koji u svojim poslovnim procesima nemaju potrebe korištenja Interneta, kao i trećim stranama (poslovnim partnerima, kupcima, korisnicima usluga,…). Ukoliko, radi podizanja razine usluge koju nudite, želite ipak omogućiti pristup Internetu zaposlenicima i trećim stranama, provjerite da li Internet usmjerivač ima mogućnost korištenja tzv. mreže za goste. Na taj način ćete im omogućiti spajanje na Internet, a neće imati mogućnost pristupa poslovnoj mreži.

Internet usmjerivač je potrebno i fizički zaštititi od neovlaštenog pristupa. Preporučljivo je usmjerivač smjestiti u zatvoreni prostor ili uredski namještaj koji su osigurani ključem te da je fizički pristup dozvoljen samo ovlaštenim osobama u poslovnom subjektu.

15. Zaštita pristupa mrežnoj infrastrukturi

Ovisno o veličini poslovnog subjekta i količini poslovne opreme (računala, prijenosnih računala, printera, mrežnih kopirki…) te poslovnim procesima postoji potreba međusobnog povezivanja navedene opreme u lokalnu mrežu. Za povezivanje opreme koriste se mrežni preklopnici (eng. switch).

Mrežne preklopnike je potrebno i fizički zaštititi od neovlaštenog pristupa smještanjem u zatvoreni prostor, mrežne ormariće ili uredski namještaj koji su osigurani ključem te da je fizički pristup dozvoljen samo ovlaštenim osobama u poslovnom subjektu.

Ukoliko je to moguće, preporučljivo je koristiti mrežne preklopnike koji imaju mogućnost konfiguriranja. Na takvim preklopnicima moguće je postaviti dodatne sigurnosne mjere u vidu da se utori za mrežne kabele u koje nisu priključeni uređaji stave van funkcije dok se za to ne ukaže potreba. Moguće je također podesiti koji uređaji međusobno mogu biti povezani, kao i koji uređaji imaju pravo pristupa Internetu. Za podešavanje postavki na ovakvom tipu preklopnika potrebno je poznavanje mrežnih protokola i mrežnih portova te je, ukoliko poslovni subjekt nema zaposlenika koji posjeduje navedeno znanje, potrebna suradnja s adekvatnim vanjskim suradnikom.

16. Zaštita pristupa podacima udaljenih lokacija od neovlaštenog pristupa

Ukoliko poslovni subjekt ima izdvojene lokacije i međusobno ih treba povezati (umrežiti) da svi zaposlenici mogu komunicirati kao da su na jednoj lokaciji, ili zaposlenik samostalno ima potrebu raditi s udaljenog mjesta i koristiti resurse poslovnog subjekta, tada je potrebno između lokacija uspostaviti tzv. virtualnu privatnu mrežu (VPN) (eng. Virtual Private Network). Kao komunikacijski medij koristi se Internet, a kako je Internet nesiguran medij za komunikaciju, VPN omogućuje da se putem Interneta, između pristupnih točaka na Internet na različitim lokacijama (npr. Internet usmjerivača) uspostavi siguran privatni kanal za komunikaciju i da svi zaposlenici digitalno komuniciraju kao da su u jednoj lokalnoj mreži. VPN stvara privatni „tunel“, odnosno kriptiranu vezu koju ne može dekriptirati te na taj način onemogućuje neovlašten pristup podacima i opremi s Interneta.

Novije verzije Internet usmjerivača imaju u sebi opciju uspostavljanja VPN mreže, a za uspostavljanje VPN mreže s udaljenim lokacijama potrebna je malo veća razina informatičkog znanja od prosječnog koja uključuje poznavanje mrežnih protokola, mrežnih protokola za "tuneliranje" i protokola za kriptiranje veze.

17. Kriptiranje podataka i prijenosnih uređaja

Kriptiranje podataka je pretvaranje podataka pomoću šifre iz čitljivog oblika u nečitljiv (šifriran) oblik, koji je nečitljiv svima onima koji nemaju šifru (ključ) kojim se podaci mogu vratiti u čitljivi oblik.

Kriptirati se mogu:

- mediji za pohranu podataka (USB stik, disk, prijenosni disk…),
- dijelovi medija za pohranu,
- datoteke u kojima su pohranjeni podaci,
- sami podaci pohranjeni u bazama podataka.

Kriptiranje medija za pohranu ili samo dijela medija za pohranu u kom se čuvaju podaci radi se pomoću posebnih programa za kriptiranje. Kriptiranje medija funkcionira na takav način da se cijeli medij ili samo dio medija za pohranu kriptira i samo ovlaštena osoba/korisnik koji ima lozinku za dektriptiranje može otključati medij i koristiti datoteke i podatke. Na tržištu postoje i besplatne verzije programa koje dovoljno sigurno kriptiraju medije za pohranu i relativno su jednostavne za korištenje.

Preporučljivo je kriptirati medije za pohranu koji se koriste izvan službenih prostorija poslovnog subjekta (disk prijenosnog računala, prijenosni disk, USB stik, memorijska kartica,…). Obično nije potrebno kriptirati cijeli medij za pohranu već samo dio u kojem će biti pohranjeni podaci koje treba zaštititi od neovlaštenog pristupa. Na taj način i u slučaju gubitka takvog medija, kriptirani podaci neće biti upotrebljivi sve dok pronalazaču nije poznata lozinka za dekriptiranje.

Datoteke u kojima su pohranjeni podaci mogu se kriptirati pomoću programa za sažimanje/arhiviranje datoteka (tzv. zipanje). Datoteke se pomoću programa za sažimanje "zapakiraju" u novu datoteku, a odabirom opcije za kriptiranje se takva datoteka zaštićuje pomoću lozinke od nedozvoljenog pristupa.

Programi u kojima se u poslovanju obrađuju podaci (npr. blagajne, program za evidenciju zaposlenika, program za plaće…) te podatke obično spremaju u baze podataka. Da bi podaci u bazama podataka bili pohranjeni u kriptiranom obliku, programi kojima se obrađuju ti podaci trebaju u sebi imati algoritme za enkripciju. Poslovni subjekt treba napraviti procjenu koji podaci su od posebne važnosti i za koje bi neovlašteni pristup i njihova zlouporaba izazvali ogromne štete. Takve podatke je preporučljivo u bazama pohranjivati u kriptiranom obliku te s proizvođačem programa dogovoriti da se program prilagodi potrebama poslovnog subjekta.

18. Razmjena podataka putem elektroničke pošte

Elektronička pošta (e-mail), a pogotovo elektronička pošta putem javnih servisa (Gmail, Hotmail, Yahoo Mail…) je vrlo nesiguran način komunikacije i razmjene podataka.

Razlog tome je što elektronička pošta od pošiljatelja do primatelja putuje u lako čitljivom obliku i prolazi kroz niz komunikacijskih točaka (Internet, internetska mrežna oprema, serveri elektroničke pošte…) nad kojima niti pošiljatelj niti primatelj nemaju kontrolu.

Stoga ukoliko je ipak potrebno razmjenjivati podatke putem elektroničke pošte treba voditi računa o sljedećem:

- u samom tekstu elektroničke pošte ne navoditi osobne podatke izvan granica poslovnih kontakt podataka, a pogotovo bilo koji osobni podatak trećih osoba (osoba koje nisu pošiljatelj ili primatelj),
- osobne podatke pohraniti u datoteku, a datoteku zaštiti snažnom lozinkom i tek tako zaštićenu datoteku poslati u privitku elektroničke pošte,
- ukoliko je potrebno slati veću količinu datoteka s osobnim podacima, prethodno ih je potrebno sažeti (u slengu – zipati) putem programa za sažimanje (zip, rar…), a tako sažetu datoteku zaštititi snažnom lozinkom i tek tako zaštićenu datoteku poslati u privitku elektroničke pošte,
- lozinku ne dostavljati primatelju putem elektroničke pošte nego nekog drugog komunikacijskog kanala (npr. putem telefona, SMS-a…),
- po mogućnosti, nakon uspješnog prijema elektroničke pošte i nakon što je primatelj pohranio datoteku na svoje računalo, pošiljatelj i primatelj brišu elektroničku poštu s datotekama u privitku.

19. Zaštita podataka pohranjenih u papirnatom obliku

I u današnje vrijeme računala i modernih tehnologija i dalje se u poslovanju primjenjuje pohrana podataka u papirnatom obliku. I za podatke u papirnatom obliku potrebno je uspostaviti odgovarajuće mjere zaštite od neovlaštenog pristupa.

Kao što je to već ranije rečeno, bez obzira da li su podaci pohranjeni u digitalnom ili papirnatom obliku, potrebno je odrediti/propisati koja radna mjesta, sukladno poslovnim procesima koje obavljaju, imaju pravo pristupa opsegu osobnih (i drugih) podataka koji su nužni za kvalitetno obavljanje njihovog posla.

Kako je papir fizički medij, za zaštitu od neovlaštenog pristupa podacima pohranjenim u papirnatom obliku koriste se fizičke mjere zaštite. Podatke u papirnatom obliku potrebno je nakon korištenja pohraniti adekvatan prostor i u adekvatan uredski namještaj (ladica, ormar, vatro nepropusni ormar…) koji su od neovlaštenog pristupa zaštićeni ključem ili na neki drugi sigurnosni način (npr. putem kartica s čipom i čitača kartica), a ne ih držati na otvorenom poslovnom prostoru (npr. na radnom stolu, na pultu …).

Nakon prestanka svrhe čuvanja podataka u papirnatom obliku takve dokumente potrebno je uništiti pomoću rezača papira.

20. Oprema koja se više ne koristi

U nekom trenutku oprema koja se koristila u poslovanju, bilo zbog kvara ili starosti, se treba rashodovati, odnosno ukoliko je oprema bila unajmljena, a istekao je ugovor najma se treba vratiti. Takva oprema (pogotovo računala i mobilna oprema) u sebi i dalje sadrži podatke. Prije nego se takva oprema zbrine u elektronički otpad ili donira ukoliko još uvijek ima neku uporabnu vrijednost, potrebno je na njoj pobrisati/uništiti podatke koji su u njoj pohranjeni u digitalnom obliku na siguran način.

Podaci u digitalnom obliku su pohranjeni na medijima za pohranu:

- disk (hard disk, ssd disk,…) u računalima, kopirnoj opremi, snimačima video nadzornog sustava…
- diska u samoj mobilnoj opremi, memorijske kartice, SIM kartice u mobilnoj opremi,
- prijenosni mediji: prijenosni disk, USB stik, memorijske kartice, CD/DVD, magnetne trake…

Sigurno uklanjanje podataka s medija može se provesti:

- Sigurnim brisanjem medija za pohranu podataka
- Fizičkim uništavanjem medija za pohranu,
- Demagnetizacijom.

Za sigurno brisanje medija za pohranu nije dovoljno napraviti obično brisanje podataka ili formatiranje medija, jer se tako obrisani, odnosno formatirani podaci mogu vrlo uspješno vratiti. Sigurno brisanje se obavlja pomoću programa koji su napravljeni upravo za tu namjenu. Medij za pohranu podataka se priključuje na računalo na kojem se nalazi program za sigurno brisanje i pokretanjem programa i odabirom medija se obavlja sigurno brisanje podataka na njemu. Proces sigurnog brisanja je vremenski duži proces i upravo zbog toga se u operativnim sustavima ne nalazi kao standardna opcija brisanja datoteka i programa jer bi se uvelike smanjila brzina i funkcionalnost svakodnevnog rada na računalu.

Sigurno brisanje u pametnim telefonima i tablet računalima obavlja se odabirom opcije vraćanja uređaja na tvorničke postavke.

Fizičko uništavanje medija za pohranu predstavlja njihovo usitnjavanje na veličinu toliko malu da se pokušajem ponovnog spajanja medija podaci sa njih ne mogu više uspješno vratiti. Npr. CD/DVD mediji, kao i podaci na papir se prije nego što će se odložiti u otpad usitnjavaju pomoću rezača CD/DVD medija odnosno papira na sitne komadiće. Diskovi, prijenosni diskovi, USB stikovi, memorijske kartice se uništavaju pomoću drobilica na sitne komadiće.

Također na tržištu postoje tvrtke koje se profesionalno bave sigurnim brisanjem medija, a koje će za svoju uslugu izdati i certifikat kako je medij sigurno obrisan.

Koji od navedenih načina sigurnog brisanja, odnosno uništavanja podataka će se primijeniti ovisi o:

- količini podataka na mediju,
- vrsti podataka koja se nalazi na mediju,
- vrsti medija na kojem su pohranjeni podaci,
- stanju u kojem se nalazi medij.

21. Pristup opremi i programima putem kartica s čipom

Postoji mogućnost da se pristup računalu i programima od neovlaštenog pristupa zaštiti pomoću kartica s čipom (tzv. pametnih kartica). Takve kartice poslovni subjekti već koriste prilikom npr. pristupa programima za prijavu i odjavu zaposlenika u sustav obaveznog zdravstvenog osiguranja.

Na isti način poslovni subjekt može imati svoje pametne kartice s pomoću kojih će ograničavati pristup računalu, opremi i programima.

Na ovaj način se pomoću kartice definira tko ima pravo pristupa određenom računalu, opremi i programu i nije potrebno kreirati i pamtiti lozinke za pristup. Iako ovakav pristup olakšava rad i ovdje treba voditi računa o zaštitnim mjerama. Preporučljivo je propisati pravila upravljanja i dodjele kartica ovlaštenim zaposlenicima te dodjele ovlaštenja za pristup po pojedinoj kartici. Svakako je potrebno voditi evidenciju kojoj kartici su dodijeljene koje ovlasti, kao i koja kartica je dodijeljena kojem zaposleniku. Zaposlenici trebaju voditi računa da svoje kartice ne daju na korištenje drugim zaposlenicima, a pogotovo ne trećim osobama.

22. Sigurnosne kopije podataka (Backup)

Postoje različiti uzroci uslijed kojih u poslovnom subjektu može doći do gubitka podataka. Npr. u računalu se može pokvariti disk, pametni telefon ili tablet računalo se može pokvariti, računalo i mobilni uređaji se mogu zaraziti virusom koji će uništiti podatke, zaposlenik namjerno ili ne namjerno može pobrisati podatke, podaci mogu biti uništeni hakerskim napadom, može doći do elementarnih nepogoda (požar, potres, poplava…). Stoga je bitno imati sigurnosne kopije podataka koji će poslovnom subjektu omogućiti nesmetano funkcioniranje i mogućnost nastavka rada i uslijed ovakvih nepredviđenih okolnosti.

Za kvalitetnu izradu sigurnosne kopije podataka potrebno je:

1. **identificirati podatke za koje se radi sigurnosna kopija**

Svaki poslovni subjekt ovisno o svom poslovanju odlučuje koji su mu podaci važni za neometano poslovanje i za koje je potrebno izraditi sigurnosnu kopiju. U osnovi, za sve podatke koje nije jednostavno, lako ili ih uopće nije moguće zamijeniti u slučaju gubitka, potrebno je raditi sigurnosne kopije.

2. **odrediti medij na koji se vrši pohrana**

Izbor medija na koji se vrši pohrana sigurnosne kopije ovisi o važnosti podataka za koje se izrađuje sigurnosna kopija, veličini sigurnosne kopije, o rokovima čuvanja sigurnosne kopije, koliko često se izrađuju sigurnosne kopije, kao i o tome, koje su mogućnosti poslovnog subjekta vezano za izradu i čuvanje sigurnosnih kopija. Mediji za pohranu mogu biti CD/DVD, USB stik, vanjski disk, magnetne trake, diskovni sustavi (eng. disk storage), sigurnosna kopija u oblaku (cloud backup)…

3. **odrediti mjesto čuvanja sigurnosnih kopija podatka**

Medije sa sigurnosnim kopijama podataka potrebno je pohraniti na sigurnu lokaciju (npr. zaključanu ladicu ili ormar, vatrootporan sef) kojoj pristup imaju samo ovlašteni zaposlenici poslovnog subjekta. Idealno bi bilo kada bi se mediji sa sigurnosnim kopijama pohranjivali na lokaciji koja je sigurna i dovoljno udaljena od originalne lokacije kako bi se u slučaju elementarne nepogode ili drugog uzroka koji je počinio štetu većih razmjera podaci mogli sigurno vratiti i ponovno uspostaviti normalno poslovanje poslovnog subjekta.

4. **odrediti rok i način čuvanja sigurnosnih kopija**

Ovisno o tome koliko često se mijenjaju podaci i koju količinu podataka je potrebno sačuvati definiraju se i periodi u kojima se radi sigurnosna kopija podataka i načini na koji se rade sigurnosne kopije podataka (da li se rade sigurnosne kopije svih podataka

ili samo izmijenjenih tj. novih podataka). Tako se sigurnosna kopija može raditi odmah nakon nastanka podatka, periodično u toku dana, dnevno, tjedno, polumjesečno, mjesečno, polugodišnje ili godišnje. Obično se u praksi periodične sigurnosne kopije podataka izrađuju za datoteke koje su nastale iz tekstualnih i tabelarnih programa, baze podataka koje koriste računalni programi, elektronička pošta… dok se sigurnosne kopije za računalne programe i operativne sustave pohranjuju nakon instalacija većih nadogradnji ili novijih verzija. Npr. dnevno se rade samo kopije datoteka u kojima se mijenjaju podaci na dnevnoj bazi, tjedno kopije navedenih datoteka, elektroničke pošte i baza podataka u kojima se podaci ne mijenjaju učestalo, a mjesečno, polugodišnje i/ili godišnje cjelokupna sigurnosna kopija čitavog računala.

5. testirati sigurnosne kopije podataka

Kako bi bili sigurni da se iz sigurnosnih kopija podataka, pohranjeni podaci mogu uspješno vratiti nazad i neometano koristiti potrebno je kopije i testirati, odnosno napraviti probno vraćanje podataka iz sigurnosnih kopija.

Preporučljivo je raditi testiranje sigurnosne kopije:

- nakon izrade prve sigurnosne kopije kako bi bili sigurni da je kopija ispravno napravljena i da se programi, baze i/ili datoteke s podacima mogu sigurno vratiti,
- nakon nabavke novog računala kako bi bili sigurni da će se sve potrebne datoteke, baze i programi moći koristiti na novom računalu,
- nakon veće nadogradnje postojećeg operativnog sustava ili prelaska na noviju verziju operativnog sustava kako bi bili sigurni da promjene u operativnom sustavu nemaju utjecaja na ispravan rad programa i neometano korištenje datoteka i baza s podacima,
- nakon nadogradnje programa ili instaliranja nove verzije programa kojim se kreiraju tekstualne, tablične i druge vrste datoteka u kojima su pohranjeni podaci, kako bi bili sigurni da se datoteke mogu ispravno otvarati i koristiti,
- periodično kako bi se provjerilo da nije došlo do oštećenja medija na kojem su pohranjene sigurnosne kopije podataka.

Ovisno o veličini poslovnog subjekta, količini podataka koji se obrađuju i složenosti poslovnih procesa ovisi i na koji način će se raditi sigurnosna kopija podataka. Tako na primjer, u frizerskom salonu u kojem se za obradu podataka koristi jedno računalo i podaci se pohranjuju u tekstualne i tablične datoteke, za izradu sigurnosne kopije se može koristiti program koji je integriran u sam operativni sustav ili neki od programa za komprimiranje (zipanje) datoteka, a kao medij za pohranu se može koristiti prijenosni disk ili USB stik odgovarajućeg kapaciteta. S druge strane u prodavaonici auto dijelova gdje se koriste različiti programi koji podatke pohranjuju u baze podataka i gdje se obrađuju velike količine podataka, možda će biti potrebno nabaviti programe namijenjene za automatiziranu izradu sigurnosnih kopija podatka, a kao medij za pohranu prijenosni disk većeg kapaciteta ili čak diskovni sustav (eng. disk storage).

Ukoliko se poslovni subjekt odluči sigurnosne kopije raditi kod vanjskog suradnika koji pruža usluge izrade i čuvanja sigurnosnih kopija u oblaku (cloud backup), potrebno je voditi računa da li pružatelj usluge pruža i jamči dovoljno visoku razinu sigurnosti za tako pohranjene podatke (da li podatke čuva u kriptiranom obliku, da li ima uspostavljenu visoku razinu zaštite od neovlaštenog pristupa podacima, da li je osigurao sigurnu (VPN) Internetsku vezu između korisnika i oblaka…).

23. Fizička zaštita od nedozvoljenog pristupa

Prilikom uspostavljanja zaštitnih mjera u poslovnom subjektu, potrebno je voditi računa i o uspostavljanju odgovarajućih fizičkih mjera zaštite od nedozvoljenog pristupa kako prostorijama unutar poslovnog subjekta tako i opremi koja se koristi u poslovnom subjektu.

Potrebno je prilikom uspostavljanja fizičkih mjera zaštite voditi računa:

- da se prostor zgrade osigura od neovlaštenog pristupa kada na adekvatan način van radnog vremena poslovnog subjekta (npr. postavljanjem protuprovalnih alarma, a ako se procjena rizika pokaže potrebnim i opravdanim i postavljanjem video nadzornog sustava),
- o ograničavanju pristupa uredskom namještaju i prostorijama u kojima se pohranjuju osobni i drugi povjerljivi podaci (npr. prostorije u kojima se nalaze računala/serveri na kojima se pohranjuju podaci, prostorije i ormari u kojima se u papirnatom obliku čuvaju podaci…),
- o ograničavanju pristupa opremi na koju se pohranjuju podaci (računalni serveri, diskovni sustavi, vanjski diskovi,…) postavljanjem u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa (npr. pomoću ključa ili pametnih kartica),
- o postavljanju ostale opreme (npr. Internet usmjerivač, mrežni preklopnici,…) u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa (npr. pomoću ključa ili pametnih kartica),
- da je uredska oprema (računala, pisači, kopirke…) koji se koriste u interaktivnom radu s korisnicima usluga poslovnog subjekta fizički odijeljena od korisnika usluga ili im je u najmanju ruku otežan pristup opremi i uvid u podatke (npr. između korisnika i radnog mjesta, odnosno opreme nalazi se pult koji priječi korisnika da pristupi opremi, pisači, kopirke i uredski namještaj u koji se odlažu podaci u papirnatom obliku su dovoljno daleko da korisnik usluga nema uvid u podatke, monitor računala je okrenut od korisnika…).

Ukoliko zaposlenici nose podatke sa sobom izvan prostorija poslovnog subjekta, također je od iznimne važnosti uspostaviti odgovarajuće sigurnosne mjere fizičke zaštite od neovlaštenog pristupa podacima.

24. Kako uspostaviti informacijsku sigurnost u poslovnom subjektu?

Kroz ovaj vodič dane su upute gdje su moguće sigurnosne točke koje omogućuju nedozvoljen pristup osobnim podacima i podacima uopće. Također su navedene i mjere koje pomažu kako bi se informacijska sigurnost podigla na najveću moguću razinu.

Može se zaključiti kako postoje četiri područja u kojima se mogu nalaziti osobni podaci i podaci uopće i o kojima je potrebno voditi računa kod zaštite podataka:

- Oprema (Hardware) (npr. Računalo, Internet router, mrežni preklopnik (switch), bežične pristupne točke (Wifi Access Point) mobitel, pametni printeri/kopirke,…)
- Računalni programi/programi za mobilne uređaje i datoteke (Software)
- Komunikacijski kanal (digitalna žična/bežična (wifi) komunikacija između opreme, Internet,…)

- Osobni podaci pohranjeni na papirnatim dokumentima

Kako bi se u poslovnom subjektu uspostavila odgovarajuća razina informacijske sigurnosti potrebno je analizirati sve poslovne procese koji se odvijaju u poslovnom subjektu od početka do kraja.

Tijekom analize poslovnog procesa u svakom od koraka poslovnog procesa treba provjeriti:

- gdje se u procesu nalaze osobni podaci,
- postoji li pravni temelj za prikupljanje/obradu tih osobnih podataka,
- tko ima mogućnost pristupa tim podacima,
- kolika šteta bi nastala prilikom zlouporabe osobnih podataka,
- koje od mjera informacijske sigurnosti je potrebno uspostaviti da bi se postigla odgovarajuća informacijska sigurnost,
- jesu li uspostavljene odgovarajuće mjere informacijske sigurnosti.

Prilikom uvođenja novog poslovnog procesa ili izmjene koraka u postojećem poslovnom procesu također je potrebno napraviti analizu poslovnog procesa i provjeriti je li postavljena odgovarajuća razina informacijske sigurnosti. Također je preporučljivo raditi periodične provjere uspostavljenih mjera informacijske sigurnosti i štite li se na adekvatan način podaci ili su potrebna poboljšanja.

Također je potrebno propisati odgovarajuće pravilnike odnosno politike informacijske sigurnosti koji će primjereno poslovnom subjektu definirati odgovarajuće organizacijske i tehničke mjere zaštite osobnih podataka koji se u poslovnom subjektu obrađuju.

Naposljetku, vrlo je bitno educirati sve zaposlenike o važnosti zaštite osobnih podataka te ih upoznati sa opsegom osobnih podataka koje oni obrađuju tijekom svog rada, kao i sa propisanim pravilnicima odnosno politikama informacijske sigurnosti poslovnog subjekta u kojem radi.

25. Samoprocjena razine postavljene zaštite

U ovom poglavlju se nalaze upitnici koji poslovnom subjektu mogu pomoći prilikom samoprocjene uspostavljene razine zaštite informacija i podataka u poslovnom subjektu.

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**
Je li 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?			
Je li Internet usmjerivač nadograđen na posljednju službenu verziju koju je izdao proizvođač Internet usmjerivača?			
Je li za bežični pristup kreirana jedinstvena snažna lozinka korištenjem WPA2 sigurnosnog protokola?			
Je li na Internet usmjerivaču isključeno spajanje na usmjerivaču putem opcije WPS?			
Je li isključen udaljeni pristup Internet usmjerivaču s Interneta (tzv. pristup izvana)?			
Je li na Internet usmjerivaču isključena opcija Universal Plug and Play (UpnP)?			
Je li na Internet usmjerivaču uključena opcija ograničavanja pristupa Internet usmjerivaču putem filtriranja MAC adrese uređaja koje koristite u poslovanju?			
Je li Internet usmjerivač postavljen u odgovarajući uredski namještaj (npr. računalne ormare) i/ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa?			
Je li postavljen vatrozid?			
Je li uspostavljena politika sigurnog korištenja Interneta?			

Ako se u poslovanju koriste računala			
	Da	**Ne**	**n/a**
Ima li svaki ovlašteni zaposlenik koji koristi računalo jedinstveno korisničko ime i lozinku za pristup računalu?			
Je li operativni sustav na računalima ažuriran na posljednju službenu verziju proizvođača?			
Pruža li proizvođač i dalje korisničku podršku (podršku nadogradnje) za sve operativne sustave na računalima koji se koriste u organizaciji?			
Je li na svim računalima instaliran antivirusni program?			
Je li antivirusni program nadograđen na posljednju verziju programa i kataloga za detekciju računalnih virusa?			
Je li na računalima postavljeno automatsko zaključavanje zaslona nakon određenog vremena nekorištenja računala?			
Jesu li računalni serveri postavljeni u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa?			
Jesu li 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?			
Jesu li vanjski diskovi postavljeni u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa?			
Jesu li 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?			

Jesu li diskovi prijenosnih računala ili dio diska u kojem se pohranjuju podaci kriptirani?			
Jesu li USB stikovi ili dio USB stikova u kojem se pohranjuju podaci kriptirani?			
Jesu li prijenosni diskovi ili dio prijenosnog diska u kojem se pohranjuju podaci kriptirani?			
Jesu li memorijske kartice ili dio memorijske kartice u kojem se pohranjuju podaci kriptirani?			
Jesu li 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?			
Jesu li 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**
Ima li svaki ovlašteni zaposlenik koji koristi program jedinstveno korisničko ime i lozinku za pristup programu?			
Jesu li programi ažurirani na posljednju službenu verziju proizvođača?			
Pruža li proizvođač i dalje korisničku podršku (podršku nadogradnje) za sve programe koji se koriste u organizaciji?			
Je li pristup bazama podataka koje koriste programi zaštićen jedinstvenim korisničkim imenom i lozinkom za svakog za to ovlaštenog zaposlenika/korisnika?			
Imaju li programi automatizirani sustav zapisa za evidentiranje pristupa (tzv. logove)?			
Je li svaka datoteka u kojoj se pohranjuju podaci osigurana snažnom lozinkom?			
Jesu li s lozinkom upoznati samo ovlašteni zaposlenici?			
Je li za svaku datoteku u kojoj se pohranjuju podaci uspostavljena adekvatna evidencija pristupa podacima?			
Rade li se 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)			
Jesu li datoteke u kojima su pohranjeni osobni podaci prije slanja zaštićene snažnom lozinkom?			
Jesu li sažete datoteke (zipane) u kojima se nalaze druge datoteke koje sadrže osobne podatke prije slanja zaštićene snažnom lozinkom?			

Dostavlja li se lozinka za pristup poslanim datotekama primatelju putem drugog komunikacijskog kanala?			
Je li 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**
Je li na pametnim telefonima i tablet računalima uključeno sigurno zaključavanje zaslona?			
Je li na pametnim telefonima i tablet računalima uključena opcija brisanja sadržaja uređaja nakon određenog broja neuspjelih pokušaja otključavanja zaslona?			
Jesu li na pametnim telefonima i tablet računalima instalirani samo programi nužni za poslovanje?			
Jesu li poslovni programi zaštićeni jedinstvenim korisničkim imenom i/ili lozinkom?			
Pohranjuju li se kontakt podaci (imenici) u pametne telefone i tablet računala, a ne na SIM kartice?			
Jesu li na pametnim telefonima i tablet računalima pohranjeni samo poslovni podaci, a ne i osobni podaci korisnika uređaja?			
Jesu li memorijske kartice (SD kartice) kriptirane?			

Ako se u poslovanju koristi mrežna infrastruktura i/ili udaljeni pristup			
	Da	**Ne**	**n/a**
Jesu li mrežni preklopnici (switch) postavljeni u odgovarajući uredski namještaj (npr. računalne ormare) ili prostorije koji su na adekvatan način osigurani od nedozvoljenog pristupa?			
Jesu li utori na mrežnom preklopniku koji se ne koriste stavljeni van funkcije (isključeni) dok se za to ne ukaže potreba?			
Je li podešeno koji uređaji mogu međusobno biti povezani (umreženi)?			
Je li podešeno koji uređaji imaju pravo pristupa Internetu?			
Je li 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**
Je li propisano koji zaposlenici imaju pravo pristupa tim podacima?			
Pohranjuju li se podaci 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?			

Općenite zaštitne mjere			
	Da	**Ne**	**n/a**
Je li kod svih zaposlenika podignuta svijest o važnosti zaštite podataka?			
Je li propisan pravilnik o informacijskoj sigurnosti?			
Jesu li propisane ovlasti tko ima pravo pristupa osobnim podacima?			
Je li propisan 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)?			
Jesu li za svaki poslovni proces propisani rokovi čuvanja osobnih podatka?			