Awareness raising campaign for SMEs

Sigurnost podataka

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

An Coimisiún um Chosaint Sonraí Data Protection Commission

Croatian Personal Data Protection Agency azop Agencija za zaštitu osobnih podataka

VUB VRIJE UNIVERSITEIT BRUSSEL

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

Voditelji obrade podataka u privatnom i javnom sektoru prikupljaju i čuvaju sve veće količine osobnih podataka o pojedincima. Tome je uvelike pridonijelo smanjenje troškova elektroničke pohrane i obrade. Organizacije također sve više povjeravaju obradu podataka trećim stranama koje to obavljaju u njihovo ime (izvršitelji obrade). Mnoge organizacije također i dalje drže velike količine osobnih podataka u fizičkom obliku – često na mjestima izvan njihovog sjedišta. Ovo veliko povećanje količine osobnih podataka koji se obrađuju i čuvaju dovodi do sigurnosnih izazova za organizacije koje prikupljaju podatke. **Voditelji obrade moraju redovito revidirati svoje pohrane osobnih podataka i postupke koje imaju za zaštitu tih podataka. Pitanja koja bi si trebali postaviti uključuju:**

- **Znamo li koje vrste osobnih podataka posjedujemo**
  - **elektronički (uključujući manje očite podatke kao što su slike videonadzornog sustava)?**
  - **na papiru?**
- **Možemo li opravdati prikupljanje ovih informacija?**
- **Zašto ih skupljamo?**
- **Za što se koriste?**
- **Koliko dugo ih držimo?**
- **Tko ima pristup njima?**
- **Kome ćemo ih otkriti?**
- **Drže li se na sigurnom?**
- **Kako raspolažemo podacima?**
- **Ako obradu osobnih podataka prepustimo izvršitelju obrade (uključujući pružatelja usluga u cloudu), jesmo li zadovoljni da su njihovi sigurnosni postupci prikladni?**

Zakonodavni okvir

- Opća uredba o zaštiti podataka (GDPR) ne definira posebne sigurnosne mjere koje voditelj obrade podataka ili izvršitelj obrade mora poduzeti, iako Uredba o e-privatnosti detaljno navodi neke zahtjeve specifične za sektor elektroničkih komunikacijskih usluga.
- Međutim, GDPR, u člancima 25. i 32., postavlja obvezu voditeljima obrade i izvršiteljima obrade da provode tehničku i integriranu zaštitu podataka kako bi se osigurala razina sigurnosti koja odgovara riziku, uzimajući u obzir:
- stanje tehnike;
- troškove provedbe;
- prirodu, opseg, kontekst i svrhu obrade; i
- vjerojatnost i ozbiljnost rizika za prava i slobode pojedinaca.

Nadalje, predlaže se sljedeći popis odgovarajućih mjera;

- pseudonimizacija i enkripcija osobnih podataka;
- sposobnost osiguravanja trajne povjerljivosti, integriteta, dostupnosti i otpornosti sustava i usluga obrade;
- mogućnost pravodobnog obnavljanja dostupnosti i pristupa osobnim podacima u slučaju fizičkog ili tehničkog incidenta; i
- proces za redovito testiranje i ocjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguranje sigurnosti obrade.

Voditelji obrade podataka i izvršitelji obrade također su dužni osigurati da njihovo osoblje i druge osobe na radnom mjestu budu upoznate sa sigurnosnim mjerama i da ih se pridržavaju. Zakonska obveza zaštite osobnih podataka odnosi se na svakog voditelja obrade podataka i izvršitelja obrade, bez obzira na njihovu veličinu. U ovim smjernicama identificirani su određeni problemi koje bi voditelji obrade i izvršitelji obrade trebali uzeti u obzir pri razvoju svojih *sigurnosnih politika.*

Prikupljanje podataka i politika zadržavanja podataka

Najučinkovitije sredstvo za ublažavanje rizika od gubitka ili krađe osobnih podataka nije zadržavanje podataka. Zadržavanje podataka uvijek treba procijeniti u odnosu na poslovne potrebe i svesti na najmanju moguću mjeru, bilo ne prikupljanjem nepotrebnih podataka ili brisanjem podataka čim potreba za njima prođe. Primjer su organizacije koje ručno prikupljaju podatke o kreditnoj kartici, uključujući datum isteka i CVV broj, te pohranjuju takve informacije nakon obrade transakcije.

Voditelj obrade uvijek treba znati koje podatke ima, gdje se čuvaju i kako teku kroz organizaciju. Bez ovog nadzora, učinkovita je zaštita osobnih podataka unutar organizacije težak zadatak.

Kontrola pristupa

Voditelj obrade podataka ima dužnost ograničiti pristup osobnim podacima. Veća ograničenja pristupa ili kontrole trebale bi se primijeniti na osjetljivije podatke. Voditelj obrade podataka mora biti svjestan različitih korisnika koji pristupaju njihovim sustavima/zapisima. Različite vrste korisnika mogu uključivati:

- osoblje na različitim razinama;

- treće strane / izvršitelji obrade

- kupci

- poslovni partneri

Moraju se uzeti u obzir različiti zahtjevi svake od ovih vrsta korisnika, a njihove privilegije pristupa osobnim podacima trebaju u potpunosti odražavati te zahtjeve.

Prirodu pristupa dopuštenog pojedinom korisniku treba redovito postavljati i provjeravati. **Pojedinačni članovi osoblja trebali bi imati pristup samo podacima koji su im potrebni za obavljanje njihovih dužnosti**. U svim organizacijama s pristupom osobnim podacima potrebni su posebni postupci kako bi se povećao ili ograničio prethodni pristup kada se promijeni uloga korisnika, spriječila upotreba dijeljenih vjerodajnica (više pojedinaca koji koriste jedno korisničko ime i lozinku) i kako bi se otkrila upotreba zadanih lozinki. To mora biti podržano redovitim pregledima stvarnog pristupa kako bi se osiguralo da je sav ovlašteni pristup osobnim podacima strogo nužan i opravdan za obavljanje funkcije.

Posebnu pozornost treba posvetiti implementaciji računa IT administratora s neograničenim pristupom osobnim podacima. Trebale bi postojati politike u pogledu provjere i nadzora

članova osoblja kojima su ti računi dodijeljeni. Član osoblja s takvim odgovornostima trebao bi imati odvojene korisničke i administratorske račune.

Trebale bi postojati stroge kontrole mogućnosti preuzimanja osobnih podataka iz sustava organizacije. Takvo preuzimanje može se blokirati tehničkim sredstvima (onemogućavanje pogona itd.). Mnoge su organizacije donijele odluku da blokiraju pristup USB priključcima nakon što su ispitale rizike vezane za ostavljanje takvih priključaka otvorenim prema zadanim postavkama za sve korisnike.

Autentifikacija pristupa

Korisnici bi trebali imati jedinstveni identifikator (kao što je lozinka, šifra, pametna kartica ili drugi token) kako bi im se omogućio pristup osobnim podacima.

Lozinke su riječ ili niz znakova. Jaka lozinka treba sadržavati najmanje dvanaest znakova (što je lozinka duža, to je računalu teže pogoditi) i može sadržavati jedno ili više od sljedećeg:

Snažna sigurnosna lozinka sadrži:

- 16 ili više znakova, što više to bolje,

- velika slova (ABCDEFGH...),

- mala slova (abcdefgh...),

- brojke (0 – 9=

- simbole (@#$%{ } [ ] ( ) / \ ' " , ; : . < >...)

- interpunkciju (?, ", !)l

<u>Kod kreiranja lozinke treba izbjegavati:</u>

- 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.

Voditelji obrade trebali bi provoditi složenost i duljinu lozinki, kao što su pravila koja osiguravaju da se slabe lozinke i ponovno korištene lozinke odbijaju. Od korisnika ne bi trebalo zahtijevati da proizvoljno mijenjaju svoju lozinku ili šifru (npr. prečesto), jer to zapravo može smanjiti sigurnost lozinki (na primjer, povećanjem oslanjanja na jednostavne lozinke ili ponovnom upotrebom lozinki). Međutim, korisnici bi trebali promijeniti svoju lozinku ili šifru ako postoje dokazi da su ugroženi ili otkriveni, ili kada postoji neka druga promjena u opasnosti. Voditelji obrade nikada ne bi trebali pohranjivati korisničke lozinke kao običan tekst, ali bi trebali koristiti snažno i nepovratno kriptografsko raspršivanje kako bi ih zaštitili i omogućili sigurnu provjeru za potrebe prijave.

Voditelji obrade podataka trebali bi osigurati da korisnici budu svjesni da je njihova lozinka jedinstvena za njih i da se ne smije otkriti nikome drugome. Dijeljene vjerodajnice (gdje više korisnika koristi istu prijavu i lozinku) nikada ne bi trebalo biti dopušteno. Zadane postavke za lozinke sustava i druge sigurnosne parametre koje je dostavio dobavljač nikada ne bi smjele ostati na mjestu. Voditelji obrade podataka moraju osigurati da partnerske organizacije s pristupom njihovim sustavima ili osobnim podacima poštuju ove kontrole. Gdje je moguće, voditelji obrade podataka trebali bi promicati raznolikost lozinki podsjećajući korisnike na rizike povezane s ponovnom upotrebom lozinki na drugim internetskim uslugama.

Višefaktorska autentifikacija

Višefaktorska provjera autentičnosti odnosi se na to da se za provjeru autentičnosti pristupa koristi više od jednog faktora identiteta. Opcija koja se često koristi u mnogim uslugama je '2FA', što znači da se koriste dva faktora za autentifikaciju. Na primjer, umjesto da samo koristi zaporku po svom izboru, korisnik može imati drugi faktor kao što je biometrijski (npr. skener otiska prsta) ili "vanpojasni" ili alternativni komunikacijski kanal koji šalje šifru sekundarnoj adresi e-pošte, telefonskom broju ili uređaju. Međutim, treba napomenuti da su neki od tih sekundarnih kanala sigurniji od drugih.

Uređaji kao što su pametne kartice ili tokeni, kao i samostalne mobilne aplikacije, mogu se koristiti kao dio gore navedenog, za pružanje provjere autentičnosti bilo generiranjem koda kojeg treba unijeti ili sadržavanjem čipa koji se autentificira sa sustavom kojem se pristupa. Oni mogu generirati PIN broj koji vrijedi vrlo kratko vrijeme. Ovo se koristi zajedno s korisničkim imenom i lozinkom za provjeru autentičnosti korisnika i može smanjiti rizik od napada u kojima su lozinke ukradene.

Automatski čuvari zaslona (screen savers)

Većina sustava omogućuje aktiviranje čuvara zaslona nakon razdoblja neaktivnosti na računalu, što zahtijeva lozinku za ponovno uspostavljanje pristupa. Ova automatska aktivacija zaključavanja korisna je jer alternativno ručno zaključavanje radne stanice zahtijeva pozitivnu radnju od strane korisnika svaki put kada on/ona ostavi računalo bez nadzora.

Bez obzira koju metodu organizacija koristi, računala bi trebala biti zaključana kada nema nadzora. Ovo se ne odnosi samo na računala u javnim prostorima, već i na sva računala. Besmisleno je imati sustav kontrole pristupa ako bilo koji član osoblja može pristupiti računalima bez nadzora.

Enkripcija

Enkripcija je proces kodiranja informacija pohranjenih na uređaju i može dodati korisni sloj sigurnosti. Smatra se bitnom sigurnosnom mjerom kada se osobni podaci pohranjuju na prijenosnom uređaju ili prenose putem javne mreže. Kao i kod lozinki, ova mjera je besmislena osim ako se ključ za dešifriranje podataka ne čuva na sigurnom. Ključ bi trebao zadovoljavati standarde složenosti potrebne za lozinke prema odjeljku iznad.

S obzirom na brzu stopu tehnološkog razvoja, nije moguće propisati standard šifriranja koji bi osigurao da podaci budu nedostupni neovlaštenim osobama**. Trenutno bi se 256-bitna enkripcija cijelog diska smatrala prihvatljivim standardom. Potvrđujemo da tržište nudi druge opcije za sigurno šifriranje podataka koje možda neće zahtijevati enkripciju cijelog diska i kada ih korisnik pravilno primjenjuje, one mogu postići isti sigurnosni ishod.**

Anti-virus software

Antivirusni softver nije potreban samo za sprječavanje zaraze s interneta (bilo e-pošte ili s web-izvora), već i za sprječavanje virusa koji se također mogu uvesti s prijenosnih uređaja, kao što su memorijski stickovi (čija bi upotreba trebala biti strogo ograničena). Nijedan antivirusni paket neće spriječiti sve infekcije, jer se ažuriraju samo kao odgovor na infekcije. Bitno je da se takav softver redovito ažurira i da politike podržavaju budnost u pogledu potencijalnih prijetnji. Politika neotvaranja privitaka e-pošte iz neočekivanih izvora može biti koristan način sprječavanja „zaraze“ virusnim kodom.

Vatrozid

Vatrozid je neophodan tamo gdje postoji bilo kakva vanjska povezanost, bilo s drugim mrežama ili s internetom. Važno je da su pravilno konfigurirani, jer su ključno oružje u borbi protiv pokušaja neovlaštenog pristupa. Važnost vatrozida je porasla kako organizacije i pojedinci sve više koriste "uvijek uključene" internetske veze, izlažući se većoj mogućnosti napada.

Softverska zakrpa

Zakrpe su najnovija ažuriranja od kreatora softvera vašeg operacijskog sustava ili aplikacijskog softvera. Obično sadrže ispravke za potencijalne sigurnosne probleme i mogu biti važan alat u sprječavanju hakiranja ili napada zlonamjernog softvera. Organizacije bi trebale osigurati da imaju redovite, dosljedne i sveobuhvatne postupke upravljanja zakrpama.

Gdje je moguće, prije instaliranja najnovijih zakrpa, dobra je praksa instalirati te zakrpe u testno okruženje kako biste osigurali da zakrpe ne stvaraju druge probleme s vašim sustavima. Također treba voditi evidenciju o datumu i zakrpi instaliranoj na sustav.

Daljinski pristup

Kada je članu osoblja/izvođaču dopušten pristup mreži s udaljene lokacije (npr. od kuće ili iz posjeta izvan mjesta), takav pristup stvara potencijalnu slabost u sustavu, ne samo kada se pristupa s bežične mreže. Iz tog razloga potrebu za takvim pristupom treba pravilno procijeniti i ponovno procijeniti sigurnosne mjere prije nego što se odobri daljinski pristup. Ako je moguće, pristup bi trebao biti ograničen na određene IP adrese. Sigurnost bi trebala biti na prvom mjestu pri odobravanju pristupa partnerskim organizacijama.

Tehničke sigurnosne mjere i sigurnosne procjene važni su aspekti u upravljanju ovim rizikom. Odgovornost je voditelja obrade podataka osigurati da, bez obzira na način na koji korisnik daljinski pristupa svom sustavu, sigurnost sustava ne može biti ugrožena.

Bežične mreže

Pristup poslužitelju putem bežične veze može izložiti mrežu napadima. Fizičko okruženje u kojem takvi sustavi rade također može biti čimbenik u određivanju postojanja slabosti u sigurnosti sustava. Kao i kod daljinskog pristupa, bežične mreže treba procjenjivati iz sigurnosnih razloga, a ne samo na temelju prividne jednostavnosti korištenja. Voditelji obrade moraju osigurati odgovarajuću razinu sigurnosti na mreži putem, na primjer, odgovarajućih mjera šifriranja ili specifikacije ovlaštenih uređaja.

Posebne ranjivosti povezane su s korištenjem nezaštićenih WiFi mreža trećih strana (npr. one u zračnim lukama, hotelima itd.). Uređaj koji koristi takvu mrežu može biti otvoren za napade drugih uređaja na mreži. Na prijenosnom uređaju treba instalirati učinkovit vatrozid kako bi se spriječili takvi napadi. Uređaj bi se trebao spojiti na mrežu samo kada je to potrebno. Prilikom korištenja nezaštićenog WiFi-a za prijenos osobnih ili osjetljivih podataka, trebala bi biti uspostavljena sigurna web sesija radi zaštite podataka.

Prijenosni uređaj

Prijenosna računala, USB stickovi, pametni telefoni i drugi oblici prijenosnih uređaja posebno su osjetljivi na krađu i slučajni gubitak. Ako voditelj obrade smatra da je bitno pohraniti osobne podatke na prijenosni uređaj, ti uređaji trebaju biti enkriptirani. Enkripcija cijelog diska trebala bi se koristiti za ublažavanje pohrane datoteka izvan enkriptiranog segmenta diska.

U slučaju pametnih telefona, jaka lozinka bi trebala biti potrebna pri pokretanju i nakon nekoliko minuta neaktivnosti. **Kada se takav uređaj izgubi, potrebno je odmah poduzeti korake kako bi se osiguralo da se aktivira mogućnost udaljenog brisanja memorije.** Osoblje kojem su dodijeljeni takvi uređaji trebalo bi biti upoznato s relevantnim postupcima.

Logovi i revizijski tragovi

Sustavi kontrole pristupa i sigurnosne politike su narušeni ako sustav ne može identificirati zlouporabe. Posljedično, sustav bi trebao moći identificirati korisničko ime koje je pristupilo datoteci i vrijeme pristupa. Također treba izraditi zapisnik izvršenih izmjena, zajedno s autorom/urednikom.

Logovi (zapisi) i revizijski tragovi mogu pomoći u učinkovitoj administraciji sigurnosnog sustava i mogu odvratiti članove osoblja od iskušenja da zlouporabe sustav. Osoblje treba obavijestiti da je evidentiranje uspostavljeno i da se korisnički zapisi redovito pregledavaju. Procesi nadzora trebali bi se usredotočiti ne samo na mreže, operativne sustave, sustave za otkrivanje uljeza i vatrozid, već bi trebali uključivati usluge daljinskog pristupa, web aplikacije i baze podataka.

Sustav za otkrivanje uljeza djeluje kao interni alarmni sustav koji nadzire i izvještava o zlonamjernim aktivnostima na mreži ili sustavu. Takvi sustavi također imaju za cilj otkriti napade koji potječu iz samog sustava. Svaka organizacija koja obrađuje velike količine osobnih podataka trebala bi imati instaliran i aktiviran sustav. U slučaju kad se upozorenja/događaji generiraju putem bilo kojeg takvog sustava, mora postojati smislen sustav za njihovo pravovremeno ispitivanje. Ovo je za pomoć pri identificiranju neobične aktivnosti i poduzimanje trenutnih korektivnih radnji ako postoji kontinuirana povreda sigurnosti.

Rezervni (Back-up) sustavi

Rezervni sigurnosni sustav je bitno sredstvo za oporavak od gubitka ili uništenja podataka. Iako bi određeni sustav trebao biti uspostavljen, učestalost i priroda sigurnosnog kopiranja ovisit će, između ostalih čimbenika, o vrsti organizacije i prirodi podataka koji se obrađuju.

Planovi odgovora na incidente

Čak i uz najbolje dizajnirane sustave, greške se mogu dogoditi. Kao dio politike sigurnosti podataka, organizacija bi trebala predvidjeti što će učiniti ako dođe do povrede podataka kako bi mogla biti spremna odgovoriti. Neka pitanja koja si možete postaviti:

- Što bi vaša organizacija poduzela u slučaju incidenta povrede podataka?
- Imate li uspostavljenu politiku koja precizira što je povreda podataka? (To nije samo izgubljeni USB stick/diskovi/prijenosna računala. Ona može uključivati bilo kakav gubitak kontrole nad osobnim podacima povjerenim organizacijama, uključujući neprikladan pristup osobnim podacima na vašim sustavima ili slanje osobnih podataka pogrešnim osobama).
- Kako biste znali da je vaša organizacija pretrpjela povredu podataka? Razumije li osoblje organizacije (na svim razinama) posljedice gubitka osobnih podataka?

- Je li vaša organizacija navela kome se osoblje obraća ako je izgubilo kontrolu nad osobnim podacima?
- Pokazuje li Vaša politika jasno tko je odgovoran za rješavanje incidenta?

Zbrinjavanje opreme

Prilikom odlaganja zastarjele ili suvišne opreme mnogi voditelji obrade nude opremu na prodaju osoblju ili je doniraju u dobrotvorne svrhe. Odgovornost je voditelja obrade podataka osigurati da svi podaci koji su prethodno bili pohranjeni na uređajima budu uklonjeni prije odlaganja. **Nije dovoljno samo formatirati diskove uređaja, jer se podaci još uvijek mogu dohvatiti.** Dostupan je softver koji će prepisati sadržaj diska nizom 1 i 0 kako bi se osiguralo da se prethodni podaci ne mogu dohvatiti. Ovisno o prirodi pohranjenih podataka, preporuča se prepisivanje tvrdih diskova između tri i pet puta.

Tamo gdje se uređaji ne recikliraju/ponovno koriste, tvrdi diskovi se mogu fizički uništiti ili demagnetizirati.

Važno je razmotriti različite vrste opreme koja može sadržavati osobne podatke. Osim očitih primjera, kao što su serveri, računala i prijenosna računala, postoji niz drugih uređaja koji mogu pohranjivati osobne podatke. To može uključivati pametne telefone, digitalne fotokopirne uređaje, faks uređaje itd. Svi podaci pohranjeni na ovim uređajima također se moraju izbrisati prije odlaganja.

Fizičko osiguranje

- Osim tehničkih sigurnosnih mjera, voditelji obrade podataka moraju uzeti u obzir i fizičke sigurnosne mjere koje su potrebne kako bi se osigurala sigurnost i integritet svih osobnih podataka koje obrađuju. Kada procjenjuju potrebe fizičke sigurnosti, voditelji obrade podataka trebali bi uzeti u obzir brojne zaštitne mjere, uključujući, ali ne ograničavajući se na:
- sigurnost perimetra (nadzor pristupa, zaključan ured, i pod alarmom, kada se ne koristi);
- ograničenja pristupa osjetljivim područjima unutar zgrade (kao što su serverske sobe);
- lokacija računala (tako da ne može svatko vidjeti ekran);
- pohrana datoteka (datoteke koje nisu pohranjene na javnim mjestima s pristupom ograničenim na osoblje koje ima potrebu za pristupom određenim datotekama); i
- sigurno zbrinjavanje zapisa (učinkovito "brisanje" podataka pohranjenih elektronički; sigurno odlaganje papirnatih zapisa).

Ljudski faktor

Bez obzira koje tehničke ili fizičke kontrole su postavljene oko sustava, najvažnija sigurnosna mjera je osigurati da osoblje bude svjesno svojih odgovornosti. Lozinke se ne smiju zapisivati i ostavljati na neprikladnim mjestima; lozinke se ne smiju dijeliti među kolegama; neočekivani privitci e-pošte ne bi se trebali otvarati osim ako ih prethodno ne pregleda antivirusni softver. Učinkovita obuka zaposlenika o rizicima kompromitiranja

podataka, njihovoj ulozi u sprječavanju i kako reagirati u slučaju problema može biti vrlo učinkovita linija obrane. Mnoge organizacije postavljaju sigurnosne politike i procedure, ali ih ne provode dosljedno.

Kontrole usmjerene na individualnu i organizacijsku odgovornost i osiguravanje provedbe politika važan su dio svakog sustava dizajniranog za zaštitu osobnih podataka. **Prvo identificirajte bitne kontrole i osigurajte da se te kontrole provode u cijeloj organizaciji bez iznimke. Nakon što se to uspostavi, prijeđite na naprednije kontrole osmišljene za ublažavanje rizika specifičnih za organizaciju i vrstu(e) podataka koji se obrađuju.**

Voditelji obrade moraju imati uspostavljene procedure za upravljanje fluktuacijom osoblja, uključujući dohvat uređaja za pohranu podataka i brzo uklanjanje dozvola za pristup.

Certifikacija

Certifikacija može biti koristan način dokazivanja usklađenosti sa sigurnosnim zahtjevima zaštite podataka, gdje certifikacija ukazuje da su kontrole sigurnosti podataka bile predmet revizije ili pregleda u odnosu na priznati standard od strane ugledne organizacije treće strane. U kontekstu računarstva u cloudu, korisnici bi trebali pogledati mogu li pružatelji usluga u cloudu pružiti kopiju ovog revizorskog certifikata treće strane.

Međutim, ostaje na voditelju obrade podataka da osigura da je zadovoljan donesenim sigurnosnim odredbama i da odredi kako to može i dokazati kada je potrebno.