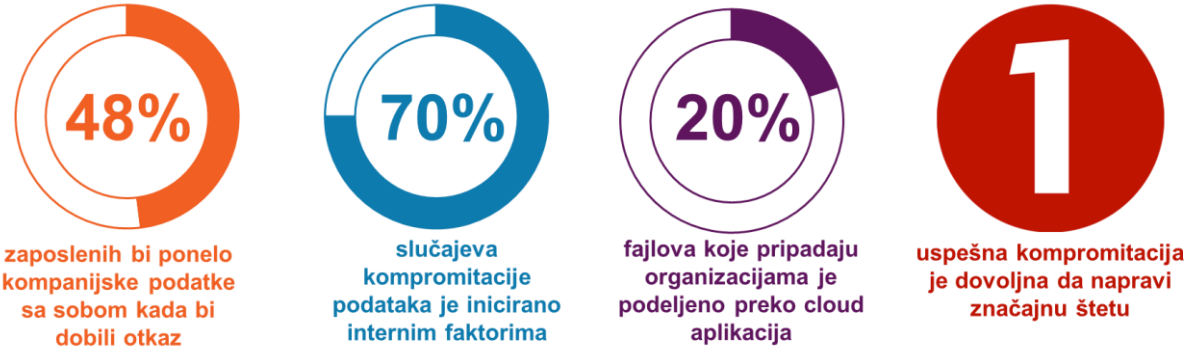
Zaštita informacija

Upravljana usluga zaštite informacija / zaštite od curenja podataka

Unicom Systems

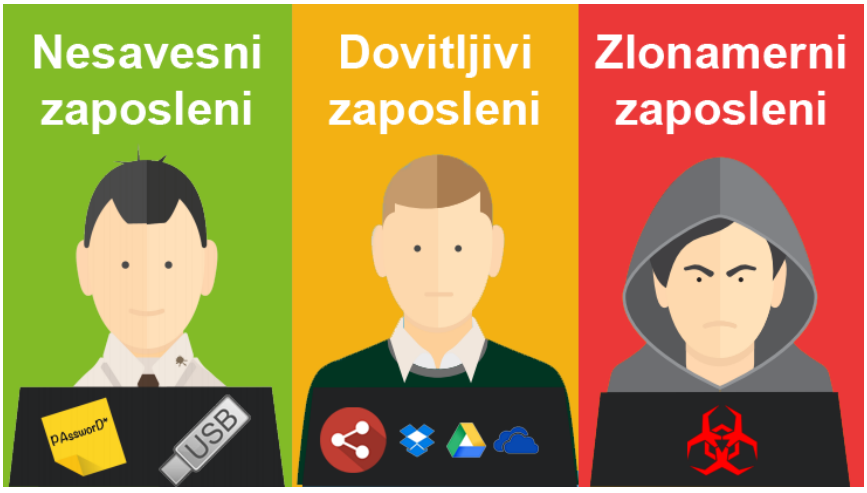
Informacije predstavljaju „krunske dragulje“ svake kompanije. Kompromitacija informacija (npr. krađa podataka o klijentima, finansijskih podatka ili neke intelektualne svojine) može prouzrokovati daleko veću štetu nego krađa materijalnih dobara. Svrha informacione bezbednosti jeste upravo zaštita ovih krunskih dragulja. Zaštita informacija se često ograničeno posmatra kao odbrana od spoljnih faktora rizika – hakera, sajber-kriminalaca koji na različite načine pokušavaju da kompromituju informacioni sistem. Sa druge strane, interni faktori rizika mogu biti znatno veći pošto je pristup informacijama lakši a samim tim i zloupotreba jednostavnija. Šteta prouzrokovana kompromitacijom informacija od strane zaposlenih može biti značajnija, pošto zaposleni imaju mnogo bolji uvid od spoljnih faktora - znaju koje su informacije najvrednije, gde se one nalaze i kako im se može pristupiti.



Rizik ne predstavljaju samo zlonamerne aktivnosti, kompromitacija informacija često može bude prouzrokovana nesavesnim i nenamernim akcijama. Interne pretnje možemo klasifikovati u tri kategorije:

1. **Nesavesno i slučajno delovanje** – zaposleni često nisu svesni posledica svojih akcija u radu sa informacionim sistemom i informacijama - čuvanje informacija na radnim stanicama, snimanje podataka na USB, jednostavne lozinke, slanje informacija na pogrešne email adrese itd. Često i kada postoje bezbednosne polise, zaposleni nisu u potpunosti upoznati sa njima.
2. **Linija manjeg otpora, dovitljivost** – preduzimanje koraka koji nisu u skladu sa bezbednosnim polisama i dobrom praksom bez zle namere već radi lakšeg obavljanja nekih poslova – upotreba javnih cloud usluga, chata, socijalnih aplikacija, privatnog maila radi prebacivanja podataka, deljenje lozinki, kopiranje osetljivih dokumenata
3. **Zlonamerne aktivnosti** – sve aktivnosti zaposlenih i saradnika sa pristupom internim resursima sa namerom zloupotrebe informacija. Najčešće se svodi na krađu informacija. Nesavesno i slučajno delovanje takođe može da preraste u zlonamernu aktivnost npr. kada zaposleni bez inicijalne loše namere čuva podatke na svom računaru, a kasnije kada napusti kompaniju te informacije pokuša da zloupotrebi.

Interni faktori dovode i do većeg rizika od eksterne kompromitacije naročito kod nesavesnog i slučajnog delovanja – ukoliko korisnici nesavesno čuvaju informacije na svojim računarima - upadom na te računare dolazi se direktno do osetljivih informacija, što ne bi bio slučaj da se pridržavaju u skladu sa polisama i dobrom praksom.



Pored dobre prakse postoje različite regulative koje zahtevaju sprovođenje efikasne politike zaštite informacija. Najznačajniji akt koji stavlja na centralno mesto zaštitu privatnih podataka je evropska GDPR regulativa koja se primenjuje od maja 2018. godine. Pored ekstrateritorijalne primene GDPR-a (treba da se primenjuje u celom svetu ukoliko se informacije odnose na građane EU ma gde one bile smeštene), značajan je i domaći Zakon o zaštiti podataka o ličnosti treba u potpunosti da se uskladi sa GDPR regulativom.

Opis usluge

Usluga zaštite informacija predstavlja upravljanu uslugu zaštite od curenja informacija (*Data Loss Prevention* - DLP). Cilj zaštite od curenja podataka je da onemogući osetljive informacije da napuste organizaciju uz što manji negativni uticaj na produktivnost tj. redovne aktivnosti zaposlenih. Zaštita se ostvaruje otkrivanjem, nadgledanjem i sprečavanjem nedozvoljene upotrebe poverljivih podataka na radnim stanicama. Značajno smanjuje rizik od svih kategorija interne zloupotrebe, od nesavesnih do zlonamernih aktivnosti kroz:

- prepoznavanje nedozvoljene upotrebe - prepoznavanje poverljivih podataka, detekcija nedozvoljenih akcija (npr. pokušaj kopiranja na USB, slanje na email van kompanije, prebacivanje podataka na cloud servis itd.)
- upozoravanje zaposlenog da vrši neku radnju koja nije dozvoljena i/ili da se prate i snimaju njegove aktivnosti upotrebe podataka. Na ovaj način se podiže svest i odvraćaju se zaposleni od nesavesne i zlonamerne upotrebe
- sprečavanje aktivnosti koje nisu dozvoljene (npr. nije dozvoljeno kopiranje podataka na USB ili cloud servise) i takve aktivnosti se automatski sprečavaju
- automatsku zaštitu informacija enkripcijom ili brisanjem (npr. dozvoljeno je snimanje podataka na USB ali samo uz enkripciju podataka, automatska enkripcija ili brisanje podataka ukoliko usluga prepozna poverljive dokumente na radnoj stanici a nisu dozvoljeni definisanim pravilima)

Usluga je koncipirana sa prioritetom da se što lakše implementira kako u malim tako i u velikim organizacijama. Kako implementacija zaštite od curenja mora da prođe kroz više faza, posebna pažnja je posvećena unapred pripremljenom scenariju koji korisniku omogućavaju da sa minimalnim utroškom vremena i resursa efikasno prođe sve potrebne korake. Prva faza podrazumeva inicijalno upoznavanje sa uslugom i načinom implementacije, definišu se osnovne polise i pravila i vrši instalacija klijentskog softvera na radnim stanicama (ova faza može da se sprovede u 7 dana od inicijalizacije usluge). Osnovna polisa u ovoj fazi podrazumeva samo praćenje toka informacija, bez restriktivnih pravila. Druga faza predstavlja

„učenje“ tj. praćenje načina rada zaposlenih. Preporuka je da ova faza ne bi trebalo da traje manje od 15-30 dana. Nakon perioda učenja vrši se analiza na osnovu koje se utvrđuju ciljne polise, čime se završava osnovna implementacija. Polise, naravno, treba da podležu stalnim revizijama kako se menjaju poslovni procesi u organizaciji. Nakon osnovne implementacije operativni tim stoji na raspolaganju prateći po potrebi događaje i efikasnost rada servisa. Konsultantski tim je dostupan za sve savete oko regulativa, dobre prakse i prilagođavanja polisa poslovnim procesima. Usluga podrazumeva i isporuku periodičnih izveštaja na osnovu kojih se može pratiti efikasnost usluge. (*Napomena: Faze i vremena su dati za tipičnu implementaciju i mogu da budu drugačiji u zavisnosti od potreba organizacije u kojoj se implemetira, prirode podataka, specifičnih zahteva itd.*)

Šta je prednost naših usluga ?

Trenutna implementacija
Implementacija u istom danu od trenutka aktivacije servisa. Jednostavno puštanje u rad, tehnologija, procedure i ljudi spremni za pružanje usluge.

Vodeće tehnologije
Tehnologije koje se koriste u sklopu usluge prestavljaju vodeća rešenja iz svojih oblasti, odabrana da pruže najviši kvalitet i najbolju mogućnost integracije sa ostalim elementima usluge.

Operativni centar 24/7
U sklopu usluge na raspolaganju je stalno dostupan 24/7 operativni tim u okviru savremenog sigurnosnog operativnog centra (SOC)

Ekspertski tim
Pored operativnog tima, stručni tim sa višegodišnjim iskustvom iz domena sajber bezbednosti može uspešno da odgovori na sve izazove !

Bezbednost
Kako je naša osnovna delatnost informaciona bezbednost, pobrinuli smo se da vaši podaci budu bezbedni. Cela infrastruktura kao i data centar je pod našom direktnom kontrolom na teritoriji Republike Srbije.

Isporuka usluge - SLA
Precizno definisan nivo servisa (SLA), sa odgovarajućim ključnim indikatorima performansi (KPI). Kroz servisni model *garantujemo* efikasnu isporuku usluge !

Jasna komunikacija
Portal servisa i ticketing omogućavaju sledljivost međusobne komunikacije bez obzira na kanal – automatika sistema, portal, email ili usmena komunikacija. Pored dostupne tehnologije, naš tim je uvek spreman da direktno pomogne !

Smanjenje troškova
Sve gore navedene prednosti doprinose krajnjem cilju – smanjenju troškova. Bezbedniji sistem znači manje gubitaka, a uz efikasnu isporuku usluge smanjuje se potreba za ulaganjem u (skuplje) interne resurse.

Dodatne informacije o usluzi

Ukoliko želite da dobijete dodatne informacije u vezi usluge možete da nas kontaktirate putem email-a services@unicom.systems ili na telefon 011 / 735-7150. Moguće je i zakazivanje sastanka sa prodajnim timom u okviru kog možemo odgovoriti na sva vaša pitanja, ukazati na sve detalje naše usluge i demonstrirati samu uslugu kroz realne situacije.