german
cooperation
DEUTSCHE ZUSAMMENARBEIT

Sigurnost i zaštita poslovnih podataka

Priručnik za preduzeća

Implemented by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

In cooperation with

datalab

Imprint

Izdavač
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Sjedište firme
Bonn i Eschborn, SR Njemačka
Projekat: Inovacije i digitalizacija u MSP u BiH
Vrbanja 1 (SCC Office Tower/ 12. Floor)
71 000 Sarajevo, Bosna i Hercegovina
Tel +387 33 564 530
Fax +387 33 261 566
karin.rau@giz.de
www.giz.de/bosna-i-hercegovina
www.b2bit.ba

Izdanje
Novembar 2020.

Dizajn
Studio Mars d.o.o.
Ljubljana

Fotografije
photo Bigstock: str. 1, 5, 8

Tekst
Datalab BH d.o.o. Sarajevo
www.datalab.ba

U ime
Njemačkog saveznog ministarstva za ekonomsku saradnju i razvoj (BMZ)

SADRŽAJ

UVOD

Većina vlasnika malih i srednjih preduzeća smatra da njihovo poslovanje nije meta hakerskih napada, te ne smatraju da bi trebali preduzeti preventivne mjere. Upravo takvo razmišljanje dovodi do činjenice da je sve veći broj malih i srednjih preduzeća žrtva hakerskih napada.

Tokom pandemije COVID-19 broj ransomware (ucjenjivački software koji korisniku onemogućava pristup računarskim resursima) napada je dodatno porastao. Vanredna situacija je cyber kriminalcima dala jedinstvenu priliku da iskoriste prednost novog načina rada, rada od kuće ili drugih udaljenih lokacija koje su manje sigurne a u cilju krađe podataka odnosno zarade na prodaji istih.

Proaktivnost u zaštiti podataka i pravilna pripremljenost u slučaju nesreće, nisu samo preporučljivi, već su neophodni. Cilj ovog priručnika je podstaknuti i proširiti svijest o potrebnoj brizi o zaštiti podataka i sigurnosti unutar malih i srednjih preduzeća te vas informisati na koji način možete preventivno djelovati.

Koja je cijena gubitka podataka?

Podaci su jezgro svake kompanije i **gubljenje bilo koje količine podataka predstavlja ozbiljan problem u poslovanju iste**, a nekada toliki da poslovanje nije moguće uopće nastaviti. Iz tog razloga zaštita i sigurnost naših podataka i pristupa istim je u današnjem modernom informacijskom načinu poslovanja od krucijalne važnosti.

Preduzeće, kojem je vrhunac sigurnosti pohrana podataka na obične hard diskove i sl., dakle preduzeće koje ne brine adekvatno o zaštiti svojih podataka, nema backup strategiju, definisana pravila ili sigurnosnu politiku unutar preduzeća, u opasnosti je da usljed iznenadnog napada i gubitka podataka u potpunosti obustavi svoje poslovanje, nerijetko i trajno.

O gubitku podataka nikada ne razmišljamo kao o trošku dok nam se ne dogodi.

Šta više, statistički podaci nam to i govore. Stručnjaci kažu da više od pola malih i srednjih kompanija koje se nađu u ovakvoj situaciji, u narednih godinu dana gase svoje poslovanje zbog gubitka profita izazvanog gubitkom podataka.

Gubitak podataka može imati ozbiljne i trajne posljedice

- **Gubitak produktivnosti:**
  Produktivnost se smanjuje, jer je preduzeće fokusirano na vraćanje podataka, pregled više izvora i mogućih uzroka. Organiziranost i produktivnost radnika, kao i poslovni procesi naglo padaju.

- **Propuštanje ili kašnjenje u isporuci:**
  Gubitak podataka može dovesti do velikih zastoja u unaprijed dogovorenim isporukama, pa čak i do gubitka najodanijih klijenata što posljedično može voditi čak i do gašenja preduzeća.

- **Zaostala plaćanja:**
  Zaostala plaćanja, kao i nedostatak uvida u dospjela potraživanja i slično. Nedovoljno informacija o dospjelim potraživanjima, s povećanjem troškova za pokušaj ili uspješni povrat podataka, smanjuje likvidnost preduzeća u već teškom trenutku.

- **Veliki troškovi u slučaju mogućnosti povrata podataka:**
  Troškovi povrata bitnih podataka mogu biti čak veći i od početne investicije i kreiranja sigurnosnog sistema koji bi preventivno isključio mogućnost gubitka podataka.

- **Povećanje troškova:**
  Posljedični porast svih troškova, smanjenje likvidnosti i sve teža finansijska slika preduzeća jasno ugrožavaju opstanak na tržištu.

Šta može uzrokovati gubitak podataka?

Ljudski faktor: Slučajno brisanje ili uništavanja podataka, pogrešno formatiranje diskova, administracijske greške u održavanju IT rješenja, loše rukovanje računarom ili softwareskim rješenjima, fizička oštećenja hardware-a (računara, laptopa i sl.).

Uništenje usljed neispravnosti električnih sistema: Hardware ili neispravnost samog sistema su, pored ljudskog faktora, također veoma česti incidenati gubitka podataka koji su obično uzrokovani električnim kvarovima, rušenjem sistema ili hardware-skom greškom/neispravnosti.

Software-ske korupcije: nestručno rukovanje dijagnostičkim programima.

Računarski virusi, hakerski napadi, krađe

Prirodne katastrofe: Poplave, požari, zemljotresi i sl.

Kako se pripremiti i djelovati proaktivno?

Prvo i najbitnije je ne ignorisati činjenicu mogućnosti gubitka podataka. Potrebno je kreirati te simulirati sigurnosnu politiku, tj. plan u slučaju nekog proboja u sistem ili gubitka podataka, kao i koje radnje ćemo preduzeti u slučaju recimo krađe hardware-a, oštećenja, ljudske greške, katastrofe i sl.

Potrebno je unaprijed definisati uloge i odgovornosti u tom procesu, šta raditi sa informacijama i sistemom u slučaju gubitka te ko su osobe koje se prvo kontaktiraju. Simulirati čitav plan i izvršiti restore (povrat) izgubljenih podataka u testnom okruženju i što brže i jednostavnije vraćanje na normalno produkcijsko stanje – normalno poslovanje.

Od krucijalne važnosti je jasna strategija sigurnosti i zaštite podataka kako biste obezbijedili bezbrižno poslovanje.

Provjerite da li je vaše preduzeće preduzelo sve potrebne mjere?

Odgovorom na pitanja sami ćete biti svjesni vaše posvećenosti sigurnosti unutar preduzeća i da li ste pripremljeni da što bezbolnije pretrpite neku sigurnosnu prijetnju u vidu cyber napada ili gubitka podataka.

Ne posmatrajte sigurnost svojih podataka kao savršenu IT infrastrukturu gdje sve radi savršeno i nije moguće da će se baš vama desiti neki problem.

1 Da li ste definisali backup plan – plan kreiranja sigurnosih kopija?

Postoje mnoge sigurnosne i preventivne mjere koje je moguće usvojiti kako bi zaštitili poslovne podatke od sigurnog uništenja. Prvo i najbitnije je da uvijek imate rutinske i ispravne sigurnosne kopije podataka, što češće to bolje, ako ne svakodnevno onda barem sedmično. Iako se ovo čini sasvim normalno i razumno, iznenađujuće je da 99% malih i srednjih preduzeća ne vrši svakodnevni backup podataka.

2 Da li ste definisali ko od vaših uposlenika ima pravo pristupa podacima?

Za svakog radnika kreirajte sigurnosnu politiku i zahtijevajte korištenje individualnih korisničkih kredencijala za pristup podacima koji će vam garantovati ispravna autorizacijska prava i pristup samo onim podacima koje određeni korisnik treba da vidi/edituje/upravlja. Ovakvim sigurnosnim djelovanjem ćete uvijek znati ko i šta je radio na nekim podacima, u koje vrijeme i sl. te imati „izvještaj-log“ svih izmjena ili pregleda bitnih podataka unutar preduzeća kao što su finansijski podaci i sl.

3 Da li vršite dijagnostiku i pozadinske provjere?

Pravovremeno je potebno dijagnosticirati i vršiti pozadinske provjere kako hardware-skog dijela IT infrastrukture u preduzeću (računara, medija za pohranu, mrežne opreme), tako i samog software-skog dijela i provjere ispravnosti procesa koji se odvijaju nad podacima.

Standardni modem/router kojeg dobijete od ISP provideра i pružaoca usluga za ozbiljno preduzeće koje vodi brigu o svojim IT resursima i podacima nije dovoljna zaštita.

4 Imate li sigurnosnu politiku koju slijede svi radnici i nije je moguće izbjeći?

Unutar preduzeća obavezno kreirajte sigurnosnu politiku koje treba da se pridržavaju svi radnici unutar preduzeća. Definišite pravila za kreiranje šifre, pravila za rad od kuće, korištenje VPN software-a, firewall-a, investirajte u endpoint security alate, koji će garantovati ista pravila sigurnosti da li radnik radio iz preduzeća ili od kuće. Osigurajte računarsku mrežu kvalitetnim Firewall/IDS rješenjem i definišite pravila koja su dozvoljena unutar mreže.

5 Radite li redovan i obavezan update?

Jedna od najjednostavnijih i najučinkovitijih zaštita je da redovno radite nadogadnju vašeg software-a, kako operativnog sistema tako i aplikativnog software-a kojeg koristite unutar preduzeća. Redovnim ažuriranjem smanjujete ranjivost software-a na napade koji su već otkriveni i pridonosite svojoj sigurnosti.

6 Da li ispravno uništavate stare računare i hard diskove ?

Pobrinite se o ispravnom načinu uništavanja i odlaganja starih računara i starih hard diskova kako vaše poslovne informacije ne bi dospjele u ruke zlonamjernika koji vam mogu naštetiti posjedovanjem vaših podataka.

7 Imaju li zaposleni limitiran pristup podacima i poslovnim infromacijama?

Svakom radniku, korisniku vaših baza podataka i informacija dodijelite limitirani pristup i dodijelite samo ona autorizacijska prava koja su mu dovoljna za obavljanje poslovnog procesa čime smanjujete mogućnost korisničke greške nad podacima, a i privatnost podataka je veća.

8 Koristite li prednosti cloud-a?

Za skladištenje vaših sigurnosnih kopija koristite cloud rješenja čime dodatno povećavate sigurnost i ispravnost samih sigurnosnih kopija. Bazu podataka vašeg Enterprise Resource Planning (ERP) software-a odnosno poslovnog programa obavezno čuvajte na više lokacija, a preporuka je i da **koristite sigurnosnu kopiju u cloud-u.**

Sigurnosne kopije (Backup) u cloud-u

Odaberite kvalitetno sigurnosno rješenje za pohranu najbitnijih podataka unutar preduzeća u kojem imate definisan i inkorporiran proces kreiranja backup-a, recovery i restore podataka u slučaju neželjenog gubitka.

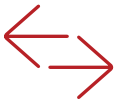
Primjer sistema cloud pohrane ERP baze podataka je PANTHEON Sigurnosna kopija (Backup) u cloud-u.

Sigurnosna kopija omogućava da baze podataka čuvamo na udaljenoj i sigurnoj lokaciji u oblaku. **U slučaju PANTHEON baza podataka to je data centar BH Telecoma.** Tako automatizujemo dnevnu izradu rezervnih kopija najvažnijih podataka preduzeća. Usluga PANTHEON Sigurnosne kopije je odlična opcija za sve PANTHEON onpremise korisnike (program koriste lokalno odnosno imaju vlastite PANTHEON licence), jer vam **obezbjeđuje isti nivo sigurnosti podataka kao da koristite poslovni program PANTHEON u oblaku**, gdje je sigurnost podataka zagarantovana od samog početka korištenja.

Snimanje cijele baze podataka

Mogućnost enkripcije prije kompresije

Kompresija u manji format (7z)



Prenos sigurnosne kopije na Cloud server

Zaključak

Podaci su temelj današnjeg poslovanja i donošenja odluka te bilo kakav gubitak ili zastoj može imati ozbiljne posljedice po svako preduzeće. Iako su se mala i srednja preduzeća ranije smatrala premalim i nevažnim kao cilj hakerskih napada, njihovo posljedično zanemarivanje potrebe za investiranjem u odgovarajuće IT resurse ili edukaciju ih je dovelo do najveće mete, kako cyber napada tako i žrtvi gubitka podataka druge prirode.

Strategija sigurnosnih kopija (backup) se stalno poboljšava i sve se više teži prema cloud rješenjima, ali čak i ona ne uspijevaju nekad spriječiti gubitak podataka koji nastaje korisničkim greškama, lošim upravljanjem i sl. **Od krucijalne važnosti je jasna strategija sigurnosti i zaštite podataka kako biste obezbijedili bezbrižno poslovanje.**

Želite na najbolji način zaštititi vaše podatke?

E: godigital@datalab.ba
T: 033 652 101
W: datalab.ba/eposlovanje/sigurnosna-kopija-backup/