Udruženje
e-Transformacija

10

KORAKA DA OSIGURATE VAŠ BIZNIS U DIGITALNOM SVIJETU

www. e- transformacija.ba

1 ZAŠTITITE SVOJE POSLOVANJE KROZ EDUKACIJU ZAPOSLENIKA

Jedan od najčešćih uzroka cyber incidenata je ljudska greška. Čak i najbolje tehničke mjere mogu biti ugrožene ako zaposleni nisu pravilno obučeni da prepoznaju prijetnje kao što su phishing, socijalni inženjering, ili lažni emailovi.

Napadači često ciljaju na ljude unutar kompanije jer znaju da su oni najranjiviji dio sistema. Zbog toga je podizanje svijesti i redovna obuka zaposlenih o cyber sigurnosti od ključne važnosti.

PREPORUKA ZA SME:

SME bi trebali organizovati redovne treninge i simulacije kako bi zaposlenici naučili prepoznati i prijaviti sumnjive aktivnosti. Uspostavljanje kulture sigurnosti unutar kompanije može značajno smanjiti broj incidenata.

Podizanje svijesti među zaposlenima ne bi trebalo biti jednokratan proces. Tehnologija se brzo mijenja, a s njom i prijetnje. Zaposleni moraju biti stalno informisani o najnovijim metodama napada i kako ih prepoznati. Phishing emailovi su postali sve sofisticiraniji, pa samo osnovno znanje o cyber sigurnosti često nije dovoljno. Napredni treninzi i stalna komunikacija ključ su za smanjenje ljudskih grešaka.

NAJBOLJE PRAKSE:

- Održavajte obuke na kvartalnom ili polugodišnjem nivou kako biste osvježili znanje zaposlenika o najnovijim prijetnjama i tehnikama zaštite.
- Koristite simulirane phishing napade kako biste provjerili da li zaposleni mogu prepoznati lažne emailove. Ovo može biti posebno korisno za identifikaciju slabih tačaka u obuci.
- Uspostavite jasne procedure za prijavljivanje sumnjivih aktivnosti i osigurajte da zaposleni znaju kome se obratiti u slučaju sumnje.

2 KORIŠTENJE JAKIH LOZINKI I AUTENTIFIKACIJE U VIŠE FAKTORA (MFA)

Jake lozinke i MFA su ključne mjere za zaštitu podataka i sistema od cyber napada. Mnoge kompanije i dalje koriste slabe lozinke ili ponavljaju iste lozinke za više sistema, što značajno povećava rizik od napada. MFA omogućava dodatni nivo sigurnosti tako što zahtijeva više načina verifikacije identiteta (npr. lozinka plus kod poslan na mobilni telefon).

PREPORUKA ZA SME:

SME bi trebali obavezati sve zaposlene da koriste jake lozinke koje sadrže kombinaciju slova, brojeva i specijalnih znakova. Također, MFA bi trebao biti implementiran za sve osjetljive sisteme, posebno za pristup cloud uslugama i korporativnim aplikacijama.

Jake lozinke nisu dovoljne same po sebi. Korisnici su skloni pravljenju grešaka, poput korištenja istih lozinki na više mjesta ili upotrebe jednostavnih lozinki. Upravo zbog toga je MFA postao standard u sigurnosti. Čak i ako napadač uspije doći do lozinke, ne može ući u sistem bez drugog faktora autentifikacije. Ovo čini MFA jednom od najefikasnijih mjera zaštite danas.

NAJBOLJE PRAKSE:

- Upravitelji lozinki (npr. LastPass, Dashlane) omogućavaju zaposlenima da koriste složene i jedinstvene lozinke za svaki sistem bez potrebe da ih pamte.
- Implementirajte MFA za sve aplikacije i servise koji sadrže osjetljive podatke, kao što su emailovi, CRM sistemi, i cloud platforme. MFA značajno smanjuje mogućnost napada čak i ako napadač dođe u posjed lozinke.
- Postavite politiku koja zahtijeva redovnu promjenu lozinki svakih nekoliko mjeseci i zabranite ponovnu upotrebu starih lozinki.

3 REDOVNO AŽURIRANJE SOFTVERA I SISTEMA

Svaki softver i operativni sistem sadrži ranjivosti koje se otkrivaju tokom vremena. Hakeri koriste te ranjivosti kako bi napali sisteme koji nisu ažurirani. Redovna ažuriranja i zakrpe koje ispravljaju sigurnosne rupe ključne su za zaštitu poslovanja. Bez ažuriranja, softver može postati ulazna tačka za napadače.

PREPORUKA ZA SME:

SME bi trebali omogućiti automatsko ažuriranje softverskih sistema kako bi osigurali da uvijek koriste najnovije sigurnosne zakrpe. Ovo uključuje operativne sisteme, antivirusne programe, aplikacije i sve ključne sisteme. Jedna neprimijenjena zakrpa može omogućiti napadačima pristup cijeloj mreži. SME-ovi, zbog svojih ograničenih resursa, često zaborave ili odgode ažuriranja, ali ovo može imati katastrofalne posljedice. Ažuriranje ne treba shvatati kao teret, već kao preventivnu mjeru protiv napada.

NAJBOLJE PRAKSE:

- Uključite opciju automatskog ažuriranja na svim uređajima i aplikacijama kako biste smanjili mogućnost ljudske greške.
- Ako automatsko ažuriranje nije opcija, planirajte redovno ažuriranje sistema tokom vikenda ili izvan radnog vremena kako biste minimizirali prekide u radu.
- Koristite softver za upravljanje zakrpama kako biste osigurali da su svi uređaji unutar mreže ažurirani na najnoviju verziju.

4 SIGURNOSNE KOPIJE PODATAKA (BACKUP)

Redovno pravljenje sigurnosnih kopija podataka može spasiti firmu u slučaju ransomware napada, tehničkog kvara ili slučajnog brisanja podataka. Ako su podaci backupovani na siguran način, kompanija može brzo vratiti poslovanje u normalu bez značajnih gubitaka.

PREPORUKA ZA SME:

SME trebaju uvesti **pravilo 3-2-1** za sigurnosne kopije: tri kopije podataka, na dva različita medija, i najmanje jedna kopija vanmrežna (offline). Ova strategija omogućava brz oporavak podataka u slučaju kvara ili napada.

Sigurnosne kopije su ključna mjera zaštite od ransomware napada, gdje napadači šifriraju podatke i traže otkupninu. Ako firma ima ažurirane sigurnosne kopije, može jednostavno vratiti podatke bez potrebe za plaćanjem otkupnine. Također, sigurnosne kopije mogu pomoći u slučaju tehničkih kvarova ili slučajnog brisanja podataka. Backup podaci trebaju biti pohranjeni na različitim lokacijama kako bi se izbjegla opasnost od gubitka u slučaju požara ili drugih katastrofa.

NAJBOLJE PRAKSE:

- Cloud servisi kao što su Google Drive ili Dropbox omogućavaju automatske backupove i zaštitu podataka na više različitih servera, što smanjuje rizik od gubitka podataka.
- Redovno testirajte procedure vraćanja podataka iz sigurnosnih kopija kako biste osigurali da su podaci sigurni i dostupni u slučaju potrebe.
- Osigurajte da su svi backup podaci enkriptovani kako bi bili zaštićeni čak i ako dođe do proboja sigurnosti.

5 ENKRIPCIJA PODATAKA

Enkripcija je proces šifriranja podataka kako bi se osigurali protiv neovlaštenog pristupa. Kada su podaci enkriptovani, oni postaju nečitljivi bez odgovarajućeg ključa za dešifriranje. Ovo je kritično za zaštitu osjetljivih podataka, bilo da se prenose putem interneta ili pohranjuju na računarima ili cloud servisima. Enkripcija je posebno važna za SME koje obrađuju osjetljive podatke kao što su informacije o klijentima, finansijski podaci ili poslovne tajne.

PREPORUKA ZA SME:

SME bi trebali implementirati enkripciju za sve osjetljive podatke, bilo da su u mirovanju (pohranjeni na diskovima ili u cloud-u) ili u prijenosu (tokom slanja emailova ili podataka putem interneta).

Iako mnoge SME koriste cloud servise koji nude ugrađenu enkripciju, preporučuje se da se provjeri gdje i kako se podaci enkriptiraju. Enkripcija osigurava da čak i ako napadači dođu do vaših podataka, oni neće moći da ih koriste bez ključa za dešifriranje.

NAJBOLJE PRAKSE:

- Osigurajte da sve web stranice i aplikacije koje vaša kompanija koristi imaju SSL/TLS certifikate kako bi enkriptovali podatke tokom prijenosa.
- Provjerite da li vaš cloud provajder nudi opciju enkripcije podataka u mirovanju i u prijenosu, i koristite tu opciju uvijek kada je moguće.
- Ako imate opciju, zadržite kontrolu nad enkripcijskim ključevima kako biste osigurali da samo vaša kompanija može dešifrirati podatke.

6 ZAŠTITA MREŽE (FIREWALL I ANTIVIRUS)

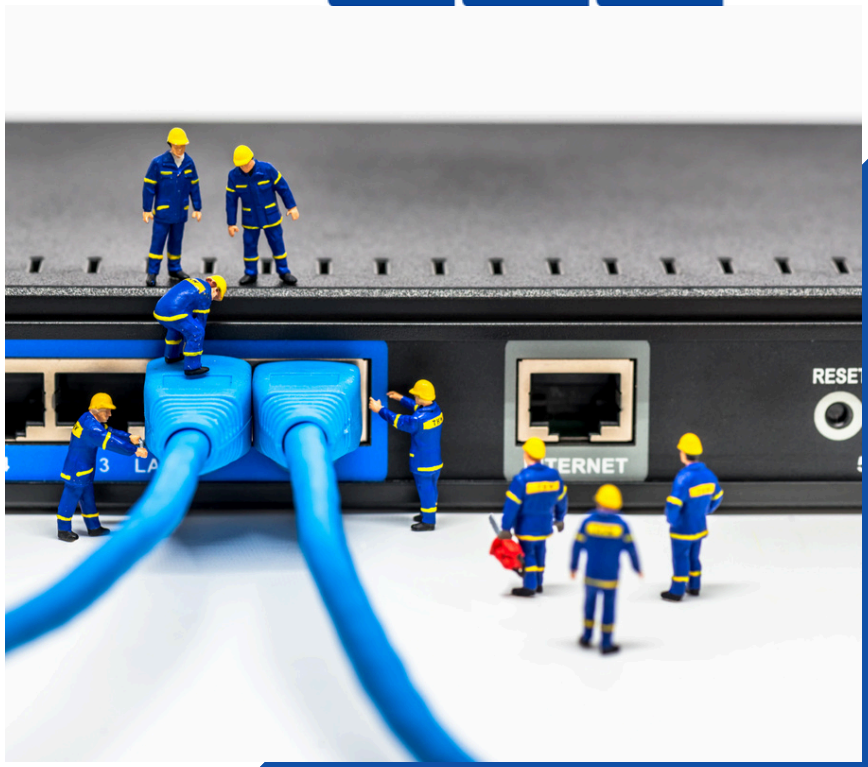
Firewall i antivirusni programi su temeljni alati za zaštitu mreža od neovlaštenih upada i malicioznih programa. Firewall djeluje kao barijera između vaše interne mreže i vanjskih prijetnji, dok antivirusni softver detektuje i uklanja maliciozne programe koji mogu oštetiti sistem ili omogućiti napadačima pristup osjetljivim podacima.

PREPORUKA ZA SME:

SME trebaju implementirati firewall rješenja za zaštitu mreže od vanjskih prijetnji i koristiti antivirusni softver na svim uređajima u mreži. SME-ovi bi trebali obratiti posebnu pažnju na pravilnu konfiguraciju firewall-a i osigurati da se svi uređaji redovno ažuriraju kako bi bili zaštićeni od najnovijih prijetnji.

NAJBOLJE PRAKSE:

- Postavite firewall pravila koja ograničavaju pristup osjetljivim dijelovima mreže, posebno za pristup s vanjskih mreža.
- Instalirajte antivirusni softver na svim računalima i serverima, i redovno ažurirajte definicije virusa kako biste ostali zaštićeni od novih prijetnji.
- Podijelite mrežu u sigurnosne zone (segmentiranje mreže) kako bi se smanjio rizik od širenja napada unutar mreže u slučaju upada.



7 KONTROLA PRISTUPA

Kontrola pristupa omogućava da samo ovlašteni korisnici imaju pristup osjetljivim podacima i sistemima. Ova mjera sprječava neovlašteni pristup i zloupotrebu sistema.
Kontrola pristupa je posebno važna u okruženjima gdje različiti zaposlenici imaju različite odgovornosti i nivoe ovlasti.

PREPORUKA ZA SME:

SME bi trebali implementirati kontrolu pristupa zasnovanu na ulogama (Role-Based Access Control - RBAC) kako bi osigurali da zaposlenici imaju pristup samo onim podacima i resursima koji su im potrebni za obavljanje posla. Redovna revizija pristupnih prava može spriječiti eventualne sigurnosne propuste. Pored tehničkih mjera, SME-ovi bi trebali postaviti jasne interne procedure i pravilnike o tome ko i kada može pristupiti određenim podacima

NAJBOLJE PRAKSE:

- Ograničite pristup podacima na osnovu uloge zaposlenika unutar kompanije (Role- Based Access Control (RBAC)).
- Implementirajte logove kako bi pratili aktivnosti korisnika na osjetljivim sistemima.
- Redovno provodite reviziju pristupnih prava, posebno nakon promjena u kadrovima ili organizacionoj strukturi.

8 REDOVNO TESTIRANJE I PROCJENA SIGURNOSTI (PEN TESTING)

Penetracijsko testiranje (Pen Testing) simulira stvarne cyber napade kako bi otkrilo ranjivosti u mreži, aplikacijama ili sistemima. Cilj testiranja je otkriti slabe tačke koje napadači mogu iskoristiti i omogućiti kompaniji da te ranjivosti ispravi prije nego što budu eksploatisane. Redovno testiranje sigurnosnih sistema je važno za održavanje visokog nivoa zaštite, jer prijetnje i metode napada evoluiraju.

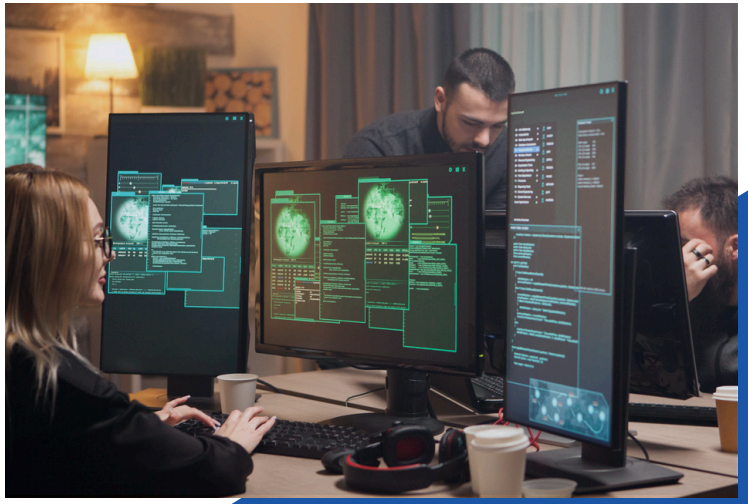
PREPORUKA ZA SME:

SME bi trebali redovno organizovati penetracijska testiranja, posebno nakon značajnih promjena u IT infrastrukturi, kao što su migracije na nove sisteme ili uvođenje novih aplikacija.

Iako SME-ovi često smatraju da nisu interesantni napadačima, stvarnost je da su male i srednje firme često primarna meta jer nemaju sofisticirane sigurnosne sisteme. Pen Testing omogućava kompanijama da identifikuju slabosti i brzo poduzmu mjere za njihovo ispravljanje i omogućava firmama da preduhitre napadače i smanje šanse za uspješan napad.

NAJBOLJE PRAKSE:

- Angažujte vanjske stručnjake ili certificirane etičke hakere kako biste osigurali objektivnost i dubinsku procjenu sigurnosti.
- Provodite penetracijska testiranja barem jednom godišnje, a češće ako implementirate nove sisteme ili aplikacije.
- Nakon što test identifikuje slabosti, osigurajte da tim IT stručnjaka odmah poduzme korake za otklanjanje tih ranjivosti.



9 IZRADA PLANA ODGOVORA NA INCIDENTE

Cyber incidenti su neizbježni, ali brz i efikasan odgovor može minimizirati štetu. Plan odgovora na incidente treba uključivati jasne protokole za identifikaciju prijetnji, izolaciju pogođenih sistema, oporavak podataka i komunikaciju s relevantnim akterima. Kompanije koje imaju jasno definisan plan mogu smanjiti vrijeme oporavka i izbjegavati dodatne troškove uzrokovane probojem.

PREPORUKA ZA SME:

SME bi trebali izraditi i implementirati plan odgovora na incidente koji uključuje jasne korake za sve zaposlene u slučaju napada. Ovaj plan treba biti redovno ažuriran i testiran kako bi bio efektivan u slučaju stvarnog incidenta. Plan za odgovor na incidente ne bi trebao biti samo dokument koji se izrađuje i zaboravlja. Redovne vježbe, kao što su "tabletop" simulacije, omogućavaju timovima da u praksi primijene plan i otkriju eventualne nedostatke. Pored tehničkih timova, u plan treba uključiti i pravne i PR timove kako bi se osigurao sveobuhvatan odgovor na napad.

NAJBOLJE PRAKSE:

- Definirajte specifične uloge i odgovornosti svakog člana tima u slučaju incidenta. Svaki zaposlenik bi trebao znati kome prijaviti incident i kako reagirati.
- Uključite planove za brzo vraćanje podataka iz sigurnosnih kopija i obnavljanje poslovanja.
- Redovno provodite simulacije incidenata kako bi tim bio spreman i znao kako brzo reagirati u stvarnom scenariju.

10 PRAVOVREMENA REAKCIJA I PRIJAVA INCIDENATA

Pravovremena reakcija na cyber incidente i njihova prijava nadležnim tijelima je ključna za minimiziranje štete i zaštitu reputacije kompanije. U mnogim zemljama postoje zakoni i regulative koje zahtijevaju prijavu cyber incidenata nadležnim organima unutar određenog vremenskog okvira. Također, transparentna komunikacija s klijentima i partnerima može pomoći u izgradnji povjerenja nakon incidenta.

PREPORUKA ZA SME:

SSME bi trebali razviti protokole za prijavu incidenata, kako unutar firme tako i prema vanjskim nadležnim tijelima. Pravovremeno reagovanje može smanjiti posljedice napada i osigurati poštivanje zakonskih obaveza.

Brza prijava incidenata može pomoći u smanjenju finansijskih i pravnih posljedica. Također, klijenti cijene transparentnost, a brza i iskrena komunikacija može smanjiti gubitak povjerenja nakon incidenta.

NAJBOLJE PRAKSE:

- Definirajte proces za prijavu incidenata unutar firme, uključujući odgovornost tehničkih i upravljačkih timova.
- Ako incident uključuje curenje podataka klijenata, važno je da pravovremeno obavijestite pogođene strane i pružite im smjernice za zaštitu njihovih podataka.

Udruženje
e-Transformacija

www.e-transformacija.ba

Implemented by:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Ova publikacija je izađena uz finansijsku podršku Ministarstva ekonomskog razvoja i saradnje Savezne Republike Njemačke (BMZ) i Vlade Švicarske. Sadržaj ove publikacije je isključiva odgovornost Udruženja e-Transformacija i ne odražava nužno stanovišta njemačke i švicarske vlade.