Awareness raising campaign for SMEs

# Kratki vodič

# Phisihing i socijalni inženjering

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

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

Jedna od glavnih obveza prema Općoj uredbi o zaštiti podataka (GDPR) za organizacije koje obrađuju osobne podatke („voditelji obrade") jest da to moraju učiniti na način koji **osigurava odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštenih ili nezakonitih obrada (uključujući krađu, uništavanje ili oštećenje, ili otkrivanje) korištenjem "odgovarajućih tehničkih ili organizacijskih mjera". To se ponekad naziva načelom 'cjelovitosti i povjerljivosti' ili 'načelom sigurnosti'.**

Ova je obveza svakako važna, te bi voditelji obrade trebali biti svjesni njene važnosti, posebice oni koji koriste ili pohranjuju osjetljive osobne podatke. Ima li, ili ne, organizacija odgovarajuće tehničke i organizacijske mjere kako bi osigurala sigurnost osobnih podataka koje obrađuje jedno je od prvih pitanja koje će Komisija za zaštitu podataka (DPC) vjerojatno postaviti u slučaju povrede osobnih podataka ili pri izvršavanju istražnih ovlasti DPC-a. Voditelji obrade također mogu konzultirati smjernice DPC-a za voditelje obrade o sigurnosti podataka kada procjenjuju odgovarajuće sigurnosne mjere koje trebaju provesti.

Jedan od načina na koji se mogu pojaviti rizici vezani uz sigurnost osobnih podataka su napadi koji su poznati kao 'phishing' ili 'socijalni inženjering'. Phishing je primjer vrste socijalnog inženjeringa koji se obično koristi za obmanu korisnika. Pod phishingom podrazumijevamo vrstu prijevare u kojoj napadač pokušava navesti korisnike da otkriju osjetljive podatke, kao što su korisnička imena, lozinke ili pojedinosti o kreditnoj kartici, prikazivajući se kao pouzdani izvor u elektroničkoj komunikaciji. Korištenjem pouzdanog izvora, imena ili poznatog logotipa kao 'mamca', napadači mogu krenuti u 'pecanje' osjetljivih informacija, poput osobnih podataka.

To se može učiniti na mnogo načina, kao što je 'lažiranje e-pošte' (gdje se koriste klonirane ili slične adrese e-pošte ili imena) i pogrešno usmjeravanje korisnika da unesu osjetljive informacije na lažnu web stranicu (koja sliči na ispravnu) ili preuzmu bezopasan, ali zlonamjeran softver koji se često nalazi u privitke e-pošte.

## Savjeti: kako prepoznati phishing ili socijalni inženjering

**Email Spoofing (Lažiranje e-pošte)**: Lažiranje e-pošte uključuje napadača koji šalje poruke s krivotvorenom adresom pošiljatelja. Budući da temeljni tehnički protokoli za e-poštu nemaju mehanizam za provjeru autentičnosti, napadači često koriste lažiranje kako bi zavarali primatelja o podrijetlu poruke. Sustavi kao što je SSL/TLS za enkripciju e-pošte mogu pomoći u izbjegavanju ovog rizika, ali često nisu dostupni niti se koriste u tu svrhu u mnogim organizacijama.

- Većina pružatelja usluga e-pošte pruža neke sigurnosne mjere za zaštitu od ovakvih vrsta e-pošte, ali važno je još jednom provjeriti podatke pošiljatelja, osobito ako je e-pošta inače sumnjiva.
- Na primjer, uvjerite se da se sama adresa e-pošte, kao i bilo koje ime ili ime kontakta u tijelu e-pošte podudaraju.

**Spear phishing (ciljani phishing):** Spear phishing je ciljani oblik phishinga, pri čemu zlonamjernik napad kreira i prilagođava žrtvi na koju je napad usmjeren. Najčešće se radi o e-mailovima koji su upućeni starijim zaposlenicima poduzeća ili zaposlenicima koji imaju odgovornost u područjima poslovanja kao što su financije. Napadač je prethodno prikupio informacije o zaposleniku koje mu omogućuju da zaposleniku uputi vrlo uvjerljivi e-mail koji djeluje vjerodostojno, može uključivati osobne podatke potencijalne žrtve, naziv radnog mjesta,

neke poslovne informacije i sl. Zaposlenik neće posumnjati da se radi o prijevari te će otvoriti privitak ili link u e-mailu i na taj način aktivirati zlonamjerni softver koji će napadaču omogućiti pristup informacijskim sustavima poduzeća.

- ✓ **Osobito je važno za poduzeća da svoje zaposlenike upoznaju s rizikom od ciljanih napada i osiguraju da budu oprezni u vezi s bilo kakvom elektroničkom korespondencijom koju ne očekuju**.

**Manipulacija poveznicama**: često uključuje tehničku prijevaru osmišljenu kako bi poveznica u elektroničkoj komunikaciji izgledala kao da pripada pouzdanom izvoru. Napadači mogu koristiti pogrešno napisane URL-ove ili poddomene koje zvuče legitimno kako bi prevarili korisnike da kliknu poveznicu. Na primjer, URL "www.truztedsource.hr" mogao bi se koristiti da se korisnici prevare da kliknu poveznicu za koju misle da je za "www.trustedsource.hr". Isto tako, napadači mogu koristiti poveznicu kao što je 'www.trustedsource.secureinfo.hr' kako bi prevarili korisnike da pomisle da se povezuje na stranicu sa 'sigurnim informacijama' na web-mjestu 'trustedsource', ali bi zapravo povezivala na web-stranicu 'secureinfo.hr', što bi mogla biti lažna stranica koju je postavio napadač. Ponekad prikazani tekst za poveznicu izgleda kao legitiman URL, ali veza kada kliknete na nju vodi negdje drugdje - na primjer, http://www.trustedsource.hr/ zapravo vodi do "www.notatrustedsource.hr". Često možete vidjeti kamo vodi prava poveznica tako da zadržite miš iznad veze, no važno je zapamtiti da to nije uvijek moguće, kao u slučaju većine mobilnih aplikacija.

 **Poduzeća moraju osigurati da zaposlenici budu oprezni prilikom otvaranja poveznica koje zaprimaju u e-mailovima, osobito na mobilnim uređajima.**

 **Poduzeća bi trebala razmotriti provedbu tehničkih sigurnosnih mjera koje mogu pomoći u otkrivanju i zaštiti od manipulacije poveznicama.**

**Socijalni inženjering**: Socijalni inženjering može imati mnogo oblika i obično koristi suptilne psihološke tehnike kako bi prevario korisnike da poduzmu određenu radnju. Korisnici se mogu potaknuti da kliknu na različite vrste neočekivanog sadržaja, kao što su poveznice ili privitci, iz različitih profesionalnih, tehničkih ili društvenih razloga. E-poruka može doći u radnu poštu s oznakom "Važno!" ili "HITNO", s naslovom i tekstom koji nastoji navesti zaposlenike da brzo otvori privitak ili klikne na poveznicu. Lažni sigurnosni skočni prozor može uplašiti korisnika da klikne na poveznicu govoreći mu da je zaražen zlonamjernim softverom ili da treba ažurirati svoj sigurnosni softver. Oglas ili e-pošta sa šokantnim naslovom mogu jednostavno potaknuti zaposlenika da klikne na poveznicu.

 Poduzeća moraju educirati svoje zaposlenike o gore navedenim opasnostima

 Poduzeća bi trebala razmotriti organizacijske ili tehničke mjere u vezi s tim koje poveznice i privitke zaposlenici smiju otvarati

**Phishing i druge prakse socijalnog inženjeringa mogu biti vrlo uvjerljive i predstavljati stvarni rizik za poduzeća, osobito na radnim mjestima s mnogo zaposlenika i/ili velikim brojem elektroničkih komunikacija**. Važno je da, kao dio svoje cjelokupne politike sigurnosti podataka, poduzeća razmotre jesu li ranjiva na takve napade i koje 'prikladne tehničke ili organizacijske mjere' mogu poduzeti kako bi smanjile sve ranjivosti.

## Pristupi ublažavanju rizika od napada

Poduzeća mogu poduzeti mnoge korake kako bi se zaštitile od sigurnosnih rizika podataka kao što su phishing i socijalni inženjering, kao što su: provođenje redovitih i detaljnih analiza rizika; pregled internih komunikacijskih i IT politika; provođenje mjera fizičkog i tehničkog osiguranja te edukacija zaposlenika.

Poduzeća trebaju uzeti u obzir troškove i proporcionalnost provedbe određenih mjera – odluka treba uzeti u obzir ne samo najbolju i najprikladniju primjenjivu tehnologiju, već i veličinu i prirodu poduzeća, kao i obujam i prirodu osobnih podataka koji se obrađuju i pohranjuju.

Poduzeća također moraju uzeti u obzir **obveze koje se odnose na osiguranje sigurnosti i integriteta svake obrade podataka koju u njihovo ime obavljaju izvršitelji obrade, uključujući i pokrivaju li ugovori o obradi podataka zahtjeve u vezi sa sigurnošću i integritetom obrade i što učiniti u u slučaju sigurnosnog incidenta ili povrede osobnih podataka.**

Određene usluge koje koriste organizacije, kao što su usluge e-pošte u Cloud-u, mogu ponuditi mnoge prednosti organizacijama. Međutim, takve usluge također mogu uzrokovati tehničke sigurnosne ranjivosti, koje organizacije moraju prepoznati. Neprovođenje odgovarajuće kontrole usklađenosti i sigurnosti može povećati rizik od povrede osobnih podataka u slučajevima phishinga ili neke od tehnika socijalnog inženjeringa. Poduzeća moraju uvijek provoditi mjere za zaštitu od prijetnji (kao što su neovlašteni pristup osobnim podacima, otmica računa, krađa identiteta, cyber prijevara i hakiranje), a posebno kad se uvodi korištenje novog softvera ili usluga.

'Grupni softver' utemeljen u Cloudu (softver koji pomaže grupama kolega da surađuju i organiziraju svoje aktivnosti), za e-poštu i druge profesionalne funkcije, kao što su Microsoftov Office 365 i Googleov G Suite, pruža napredne postavke i rješenja, koja mogu pomoći organizacijama u osiguravanju i borbi protiv ovih prijetnji. Pružatelji usluga e-pošte u većini slučajeva, također pružaju smjernice o najboljoj praksi kako bi pomogli organizacijama u osiguravanju svoje usluge e-pošte.

**Uz odgovarajuće tehničke sigurnosne mjere, obuka zaposlenika očito je jedan od najboljih načina na koji organizacija može smanjiti svoju ranjivost na phishing napade ili socijalni inženjering.** Obuka može – uz odgovarajuće tehničke sigurnosne mjere – osigurati da zaposlenici, posebno oni zaposlenici koje radi s osjetljivim informacijama kao što su osobni podaci, razumiju rizike i da su upućeni kako izbjeći rizik, kao što je neotvaranje e-pošte od nepoznatih pošiljatelja, te izbjegavanje klikanja na poveznice sadržane u e-poruci osim ako znaju točno kamo ih vodi.

Slojeviti pristup sigurnosti ublažava rizik od neuspjeha sigurnosne mjere koji je mogao rezultirati povredom osobnih podataka od strane organizacije.

## Preporuke : kako se obraniti od napada

Sljedeće preporuke mogu pomoći poduzećima pri razmatranju koje tehničke i organizacijske mjere treba provesti kako bi se osigurala sigurnost i integritet osobnih podataka koje obrađuju i zaštitili phishinga i napada socijalnog inženjeringa. Neće sve preporuke biti relevantne za svaku

organizaciju, ali ih treba razmotriti u kontekstu rada organizacije i vrsta obrade podataka, kako bi se implementirale one koje su najprikladnije u svakom pojedinom slučaju:

- ✓ Pregledajte sve zadane sigurnosne postavke, uključujući lozinke i vjerodajnice, koje pruža bilo koja usluga e-pošte ili grupni softver koji koristi organizacija.
- ✓ Primijenite višefaktorsku autentifikaciju za administratore, web-bazirane ili udaljene korisnike e-pošte, baza podataka ili organizacijskih sustava, uključujući bilo kojeg partnera za usluge ili administratore.
- ✓ Implementirajte pravila za filtriranje i otkrivanje sumnjivih i/ili neželjenih e-poruka.
- ✓ Stvorite pravila za rukovanje porukama i privitcima na temelju uvjeta kao što su vrsta datoteke ili veličina poruke.
- ✓ Uključite reviziju kako biste osigurali da je dostupan zapisnik revizije za praćenje radnji korisnika na sustavu e-pošte.
- ✓ Osigurajte da korisnici imaju ispravna dopuštenja e-pošte temeljena na njihovoj ulozi - s obzirom na prava na sustav, upravljanje ili konfiguraciju.
- ✓ Onemogućite daljinski ili web-baziran pristup e-pošti, bazama podataka ili drugim sustavima za osoblje koje je prvenstveno vezano za ured.
- ✓ Implementirajte kontrole kako biste spriječili korisnike da automatski prosljeđuju e-poštu(e) na vanjske adrese e-pošte.
- ✓ Redovito provjeravajte sva pravila prosljeđivanja omogućena za grupni softver koji se temelji na e-pošti kako biste bili sigurni da nema nepotrebnih ili neodobrenih pravila.
- ✓ Konfigurirajte pravila za pružanje upozorenja (vizualni znak) kada se e-pošta pošalje vanjskom kontaktu ili organizaciji (npr. Sigurnosni savjeti za Office 365).
- ✓ Konfigurirajte pravila za pružanje upozorenja o ponašanju prijave kao što je nepravilan pristup geolokaciji.
- ✓ Konfigurirajte politiku sprječavanja gubitka podataka kako biste automatski identificirali i nadzirali sve osjetljive podatke (npr. bankovni podaci) koji se šalju e-poštom na vanjske adrese.

  Redovito provjeravajte pravila pristupa webu (filtriranje) kako biste zabranili pristup zlonamjernim (phishing) ili neprikladnim web stranicama.
- ✓ Implementirajte kontrolni proces za odobravanje i osiguranje svih uređaja koji pristupaju e-pošti.
- ✓ Stvorite odgovarajuća pravila pristupa službenoj e-pošti u slučajevima kad se zaposlenici koriste svojim uređajima za pristup službenoj e-pošti
- ✓ za upravljanje mobilnim uređajima (za potencijalno lociranje, zaključavanje i brisanje u slučaju gubitka).
- ✓ Čuvajte i redovito pregledavajte popis mobilnih uređaja odobrenih za pristup e-pošti i uklanjajte sve uređaje koji više nisu potrebni.
- ✓ Razvijte plan odgovora na incidente kako bi se osigurao okvir za upravljanje bilo kojim sigurnosnim incidentom(ima).
- ✓ Zahtijevajte da se e-poruke prenose putem sigurne (kriptirane) veze kao što je TLS 1.2.
- ✓ Pregledajte sva pravila arhiviranja e-pošte kako biste smanjili količinu informacija sadržanih u poštanskim sandučićima.
- ✓ Implementirajte enkripciju u mirovanju za sandučiće e-pošte.
- ✓ Izdajte relevantna ažuriranja za zaposlenike o važnosti opreza u pokušajima socijalnog inženjeringa putem e-pošte i drugih pokušaja napada. Integrirajte ova ažuriranja u kontinuirani obrazovni proces o kibernetičkoj sigurnosti i povezanim prijetnjama.

- ✓ Osigurajte da zaposlenici mogu kontaktirati stručnu osobu, kao što je interni ili vanjski IT stručnjak, ako su zabrinuti ili sumnjaju u sigurnosni rizik, kao što su sumnjiva komunikacija, poveznica, privitak ili skočni prozor.
- ✓ Razmislite o implementaciji naprednih metoda zaštite e-pošte kao što su Sender Policy Framenwork (SPF), DomainKeys Identified Mail (DKIM), Provjera autentičnosti poruka na temelju domene, izvješćivanje i usklađenost (DMARC).

Podsjećamo organizacije da prema GDPR-u organizacije moraju prijaviti povredu osobnih podataka nadležnom nadzornom tijelu ako povreda predstavlja rizik za pogođene pojedince. Organizacije to moraju učiniti u roku od 72 sata od saznanja o povredi. Ako je vjerojatno da će povreda rezultirati visokim rizikom za pogođene pojedince, organizacije također moraju obavijestiti te pojedince bez nepotrebnog odgađanja. Daljnje upute o obavijestima o povredama mogu se pronaći na web stranici AZOP-a https://azop.hr/izvjescivanje-o-povredi-osobnih-podataka/.

Ispunite upitnik za samoprocjenu: https://arc-rec-project.eu/upitnik-tehnicke-i-organizacijske-mjere-zastite-osobnih-podataka/