ZAŠTITITE SVOJU FIRMU I ZAPOSLENE

https://www.pexels.com/photo/email-blocks-on-gray-surface-1591062/

BUSINESS EMAIL COMPROMISE (BEC)

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

ŠTA PREDSTAVLJA *BUSINESS EMAIL COMPROMISE (BEC)*?

Kompromitovanje poslovne elektronske pošte *(Business email compromise - BEC*) je vrsta prevare u kojoj napadač ima za cilj nanošenje štete kompaniji, koristeći lažne imejl naloge te kompanije.

BEC predstavlja veliki i rastući problem koji može pogoditi različite tipove organizacija, bez obzira na njihovu veličinu. *BEC* predstavlja jednu od najtežih finansijskih prevara na mreži, koja iskorišćava činjenicu da se u svakodnevnom radu većina organizacija, za poslovnu komunikaciju, oslanja na elektronsku poštu. Ovakav tip prevare je pojedine organizacije izložio velikim gubicima, koji se mogu meriti u milijardama eura.

Kompromitovanje naloga elektronske pošte (*Email account compromise - EAC*) ili preuzimanje naloga elektronske pošte je pretnja koja se ubrzano razvija u eri poslovanja zasnovanoj na cloudinfrastrukturi. *EAC* je često povezan sa *BEC*-om, jer se kompromitovani nalozi koriste u sve većem broju prevara u sajber prostoru.

Veliki izazov predstavlja otkrivanje i sprečavanje *BEC* i *EAC* tipova napada, posebno sa postojećim alatima, *endpoint* rešenjima i aktuelnim rešenjima koja se koriste za odbranu *cloud* platformi.

U *BEC* prevari, zlonamerni napadač se predstavlja kao neko kome primalac takve poruke treba da veruje - obično kao kolega, šef ili kompanija sa kojom, posredno ili neposredno, sarađuju. Zlonamerni napadač šalje imejl poruku za koju se čini da dolazi od poznatog izvora koji postavlja legitiman zahtev, kao npr. da izvrši transfer novca sa jednog na drugi račun, preusmeri platni spisak, promeni bankarske detalje za buduća plaćanja i sl.

VRSTE *BEC* PREVARA

Postoji nekoliko vrsta *BEC* prevara:

Izvršni direktor (*chief executive officer - CEO*) prevara: Ovde se zlonameni napadači predstavljaju kao izvršni direktor ili rukovodilac kompanije i obično elektronskom poštom pošalju zahtev pojedincu iz sektora finansija, da se sredstva prebace na račun koji kontroliše napadač.

Kompromitovan nalog: Nalog elektronske pošte zaposlenog je hakovan i koristi se za potraživanje plaćanja usluga i proizvoda kompanija sa kojom posmatrana organizacija sarađuje. Uplate se zatim šalju na lažne bankovne račune u vlasništvu napadača.

Lažna faktura: Napadači obično ciljaju strane dobavljače putem ove taktike. Zlonamerni napadač se predstavlja kao da je dobavljač i zahteva prebacivanje sredstava na lažne račune.

Lažno predstavljanje advokata: To je slučaj kada se zlonamerni napadač lažno predstavlja kao advokat ili zakonski zastupnik. Zaposleni na izvršnim pozicijama su obično meta ovakve vrste napada, jer ne dovede u pitanje validnost ovakvog zahteva.

Krađa podataka: Ove vrste napada obično ciljaju zaposlene u ljudskim resursima, gde zlonamerni napadači pokušavaju da dobiju lične ili osetljive informacije o pojedincima unutar kompanije, poput izvršnih direktora i rukovodilaca. Ovi podaci se mogu iskoristiti za buduće napade, poput pomenutog tipa - Izvršni direktor.

NA KOJI NAČIN ZLONAMERNI NAPADAČI IZVRŠAVAJU *BEC* PREVARE?

Mogući su sledeće tehnike izvršavanja *BEC* prevara:

- **Podmetanje (*spoof*) imejl naloga, veb sajta i domena**. Male varijacije na legitimnim imejl adresama (npr. petar.petrovic@primer.com nasuprot petar.petrovc@primer.com), koje zavaraju žrtve da su imejl nalozi autentični i nastave da komuniciraju sa zlonamernim napadačem, misleći da se komunikacija odvija sa legitimnim pošiljaocem. Još jedna od tehnika lažnog predstavljanja je podmetanje (*spoofing*) domena i domena nalik legitimnim domenima. Ovi napadi su veoma efikasni jer je zloupotreba domena složen problem. Zaustavljanje podmetanja domena dovoljno je teško, a predvideti svaki potencijalni domen koji liči na legitimni je još teže. Ova poteškoća se samo umnožava sa svakim domenom koji koriste spoljni partneri, a koji bi mogli da se koriste u *BEC* napadima, sa ciljem da se zloupotrebi poverenje korisnika. Više o ovoj temi možete pogledati na linku.

- **Slanje *spearphishing* imejl poruka.** Imejl poruke izgledaju kao da su od pouzdanog pošiljaoca, kako bi se žrtva prevarila i otkrila poverljive informacije. Ove informacije omogućavaju zlonamernim napadačima pristup računima kompanija, kalendarima i podacima koji im daju detalje potrebne za sprovođenje *BEC* napada. Više o ovoj temi možete pogledati na linku.

- **Korišćenje malvera.** Ukoliko se pokrene zlonamerni softver u mreži organizacije, napadač može dobiti pristup legitimnim imejlovima o naplatama i fakturama. Tako prikupljene informacije se koriste za postavljanje zahteva ili slanje poruka, kako računovođe ili finansijski službenici ne bi doveli u pitanje zahteve za plaćanje. Zlonamerni softver, takođe omogućava zlonamernimnapadačima pristup podacima žrtve, uključujući lozinke i informacije o finansijskim računima.

Ipak zlonamerni softver se retko koristi u *BEC* napadima, jer se tada mogu lakše otkriti i analizirati sistemima za odbranu od sajber napada. *BEC* napadi se najčešće oslanjaju na lažno predstavljanje i druge tehnike socijalnog inženjeringa da bi se prevarili korisnici i stupili u interakciju sa napadačem. Ove napade je teško otkriti, zbog ciljane prirode napada i korišćenja socijalnog inženjeringa, a analiza i saniranje ovakvih napada je težak proces koji zahteva mnogo vremena, ali i novca.

Kod *EAC* napada, zlonamerni napadač dobija kontrolu nad legitimnim nalogom elektronske pošte, što mu dalje omogućava pokretanje *BEC* napada. Ali u ovim slučajevima napadač ne lažira da ima pristup sistemima kao i izabrana osoba – već zaista pristupa tim resursima.

Pošto se *BEC* i *EAC* fokusiraju na ljudske slabosti, a ne na ranjivost sistema, potrebno je da se odbrana usmeri na obučavanje korisnika kako da prepoznaju potencijalne pretnje i da se na taj način spreči, otkrije i odgovori na širok spektar *BEC* i *EAC* tehnika napada.

Faze odvijanja napada:

FAZA 1 - Ciljane liste elektronske pošte

Napadači počinju sa izradom ciljane liste imejlova. Uobičajene taktike uključuju prikupljanje podataka sa *Linkedin* profila, proveravanje kroz poslovne baze podataka elektronske pošte ili čak prolazak kroz razne veb stranice u potrazi za kontakt podacima.

FAZA 2 – Izvršavanje napada

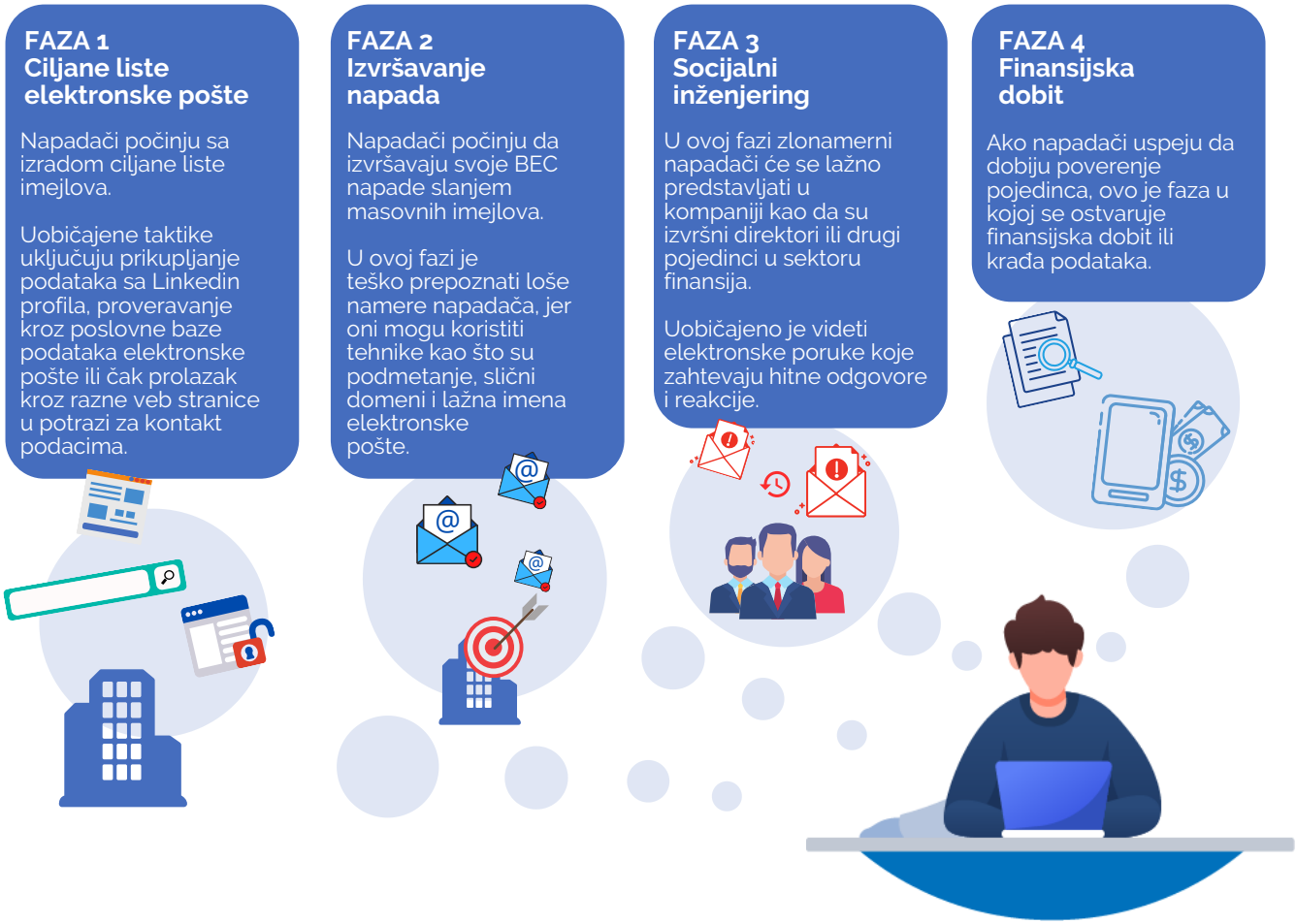
Napadači počinju da izvršavaju svoje *BEC* napade slanjem masovnih imejlova. U ovoj fazi je teško prepoznati loše namere napadača, jer oni mogu koristiti tehnike kao što su podmetanje, slični domeni i lažna imena elektronske pošte.

FAZA 3 - Socijalni inženjering

U ovoj fazi zlonamerni napadači će se lažno predstavljati u kompaniji kao da su izvršni direktori ili drugi pojedinci u sektoru finansija. Uobičajeno je videti elektronske poruke koje zahtevaju hitne odgovore i reakcije.

FAZA 4 - Finansijska dobit

Ako napadači uspeju da dobiju poverenje pojedinca, ovo je faza u kojoj se ostvaruje finansijska dobit ili krađa podataka.



KAKO SE KORISNICI MOGU ZAŠTITITI?

- Neophodno je pažljivo rukovanje informacijama koje korisnici objavljuju na internetu, najčešće na društvenim mrežamama. Otvorenim deljenjem informacija poput imena kućnih ljubimaca, škola koje ste pohađali, veza sa članovima porodice i rođendana, dajete zlonamernom napadaču sve potrebne informacije i mogućnost da otkrije vašu lozinku ili odgovori na vaša bezbednosna pitanja.
- Treba voditi računa o linkovima ili dokumentima koje korisnik dobije u okviru elektronske pošte, ili SMS-a, a posebnu pažnju obratite na zahteve da ažurirate ili proverite/promenite informacije o nalogu. Dodatno je poželjna provera telefonskog broj kompanije u adresaru organizacije (ne treba koristiti onaj broj koji nudi potencijalni napadač u mejlu), kao i poziv kompaniji, ukoliko se bilo šta učini sumnjivim, kako bi se utvrdilo da li je zahtev legitiman.
- Pažljivo proveriti adresu elektronske pošte, URL i pravopis koji se koristi u bilo kojoj prepisci. Napadači koriste male razlike kako bi zavarali oko korisnika i stekli poverenje.
- Preuzimanje priloga predstavlja dodatni izazov kojem treba pristupiti sa više pažnje. Ne treba otvarati priloge elektronske pošte dobijene od nepoznatog pošiljaoca.
- Administrator imejl sistema može podesiti *Domain-Based Message Authentication*, *Reporting and Conformance Protocol* (*DMARC*) polisu, koja zajedno sa *Sender Policy Framework* (*SPF*) i *Domain Keys Identified Mail* (*DKIM*) mehanizmima značajno umanjuje rizik od prijema fišing imejl poruka. U naslove poruka koje nisu poslate sa kompanijskog servera može se dodati reč “eksterno” što može olakšati procenu da li je reč o prevari ili ne. Više o ovim mehanizmima možete pročitati na linku.
- Podešavanje dvofaktorske (ili multifaktorske) autentifikacije na bilo kom nalogu predstavlja dodatni vid zaštite i može značajno otežati zloupotrebu naloga.
- Poželjno je korišćenje opcije lične verifikacije zahteva za plaćanje i kupovinu ili da korisnik stupi u direktan kontakt sa osobom, kako bi se uverio da su primljeni nalozi legitimni. Ovaj princip treba primeniti posebno ukoliko dođe do bilo kakve promene broja računa ili procedure plaćanja sa osobom koja podnosi zahtev.
- Korisnik treba da bude posebno obazriv ukoliko pošiljalac vrši pritisak da se brzo postupi.

Nacionalni CERT Republike Srbije ne promoviše ili favorizuje bilo koji od korišćenih javnih izvora, među kojima su i komercijalni proizvodi i usluge. Sve preporuke, analize i predlozi dati su u cilju prevencije i zaštite od bezbednosnih rizika.

Izvori:

- FBI: Business Email Compromise
- Proofpoint: Business email compromise (BEC)
- Dmarcian: https://dmarcian.com/basic-bec-defense/

REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

#odbraniseznanjem

SRB-CERT