Savjet za poduzetnike - kako ne nasjesti na lažne poslovne poruke

U svijetu je vrsta prijevare izvedena lažnom poslovnom porukom već viđena stvar, a u nas su potencijalne žrtve sve tvrtke koje ne provjeravaju vjerodostojnost svoje poslovne korespondencije - posebno one koje posluju s inozemstvom

Prijevara lažnom poslovnom porukom počinje tako što se kriminalci „**ubace“ u korespondenciju** koja se između tvrtki odvija putem elektroničke pošte. Zatim, kad dođe vrijeme za plaćanje naručene robe ili usluge, šalju lažnu poruku, tako oblikovanu da ju je vrlo teško razlikovati od prethodnih poruka koje su tvrtke međusobno razmijenile dogovarajući i obavljajući tu poslovnu transakciju.
Kriminalci se u tim porukama predstavljaju kao osoba iz tvrtke kojoj treba platiti naručeni proizvod ili uslugu i pri tome tvrde da se promijenio broj računa i banka putem koje je potrebno izvršiti plaćanje. U poruci navode podatke o tom drugom računu, kojeg su otvorili u svrhu prijevare i žrtvu navode na uplatu novca na taj račun.

Bitno pridržavati se provjeri vjerodostojnosti

Obrana od ove vrste kriminalnog napada relativno je jednostavna, no zahtijeva strogo i stalno pridržavanje pravila o provjeravanju vjerodostojnosti poslovnog dopisivanja.
Ljudi koji su u tvrtkama zaduženi za plaćanja ili ljudi u knjigovodstvenim servisima koje su tvrtke angažirale da za njih obavljaju i taj dio poslovanja, moraju - u svakom pojedinom slučaju u kojem zaprime poruke elektroničke pošte kojim ih trgovačka društva s kojima posluju obavještavaju da je u međuvremenu došlo do promjene banke i računa na koji je potrebno izvršiti uplatu za kupljenu robu, prije nego što izvrše uplatu - putem telefona i-ili video-konferencijskog poziva provjeriti vjerodostojnost i istinitost takve poruke.
Ukoliko ustanove da je riječ o prijevari, moraju o tome odmah obavijestiti i MUP, prijavom u najbližoj policijskoj postaji.

Kako dolaze do podataka?

Kriminalci obično prvo saznaju ime točno određene osobe. No, kako to rade? Najčešće, tzv. socijalnim inženjeringom: skupljanjem podataka s društvenih mreža i tvrtkinih web stranica, presretanjem pošte koja dolazi u tvrtku koja im je cilj, pa čak i prisluškivanjem razgovora u kafiću u kojem se zaposlenici tvrtke-žrtve okupljaju u stankama za ručak ili poslije posla.
Nakon toga, toj osobi pošalju e-mail s tzv. spear-phishing zlćudnim softverom. Kad se taj softver aktivira (nepromišljenim klikom na poveznicu u poruci ili na zaraženu datoteku u privitku te poruke) kriminalac dobije pristup žrtvinu računalu. To je jedna varijanta takvog napada. Druga varijanta izvodi se tako što taj, potajno instalirani zlćudni softver proslijedi sve poruke iz mape s poslanim porukama - ravno do elektroničkog poštanskog sandučića kojeg je za tu svrhu kreirao napadač.

Nakon analize tih poruka, kao što smo uvodno već opisali, haker dizajnira lažnu poruku tako da žrtva teško može ustanoviti kako je riječ o poruci koja nije došla od osobe s kojom inače komunicira u vezi plaćanja računa toj drugoj tvrtki.

Meta tvrtke koje rade s inozemstvom

Zloćudni softver koji služi na izvedbu ovakvih napada iznimno je sofisticiran, a hakeri se oko toga trude i dodatno, obrađujući ga tako kako bi bili sigurni da ga većina antivirusnih programa neće prepoznati - ili za taj napad koriste neke druge alate (primjerice, neki od alata za udaljeno upravljanje računalima) koje antivirusni programi neće prepoznati kao prijetnju.
U svijetu, ova vrsta prijevare (Business E-mail Compromise) nije nova stvar. Najviše se, tijekom posljednjih pet-šest godina, pojavljivala u Sjedinjenim Državama i Zapadnoj Europi, a najčešći cilj su joj bile tvrtke koje puno rade s inozemstvom. Banke koje su bile odredišta za plaćanje u tim slučajevima nalazile su se najviše u Kini.

Brošure vezano uz najčešće online prijevare:

- „Direktorska“ prijevara
- Prijevara s računima
- „Phishing“ – mrežna krađa identiteta
- Krađa identiteta pozivom
- Krađa identiteta SMS-om

otpbanka

"DIREKTORSKA" PRIJEVARA

"Direktorska" prijevara događa se kada je zaposlenik koji je ovlašten za provođenje plaćanja prevaren na način da plati lažni račun ili provede neovlašteni prijenos s računa tvrtke.

KAKO SE TO RADI?

Prevarant zove ili šalje poruke predstavljajući se kao direktor ili član uprave tvrtke.

Dobro poznaju organizaciju tvrtke.

Traže hitno provođenje plaćanja.

Koriste fraze kao "povjerljivost", "tvrtka ima povjerenje u vas", "trenutno sam nedostupan".

Kažu da se radi o osjetljivoj situaciji (npr. porezna kontrola, preuzimanje i spajanje poduzeća).

Često se zahtjev odnosi na međunarodna plaćanja bankama izvan Europe.

Zaposlenik prenosi sredstva na račun koji kontrolira prevarant.

Upute o tome kako postupiti mogu se dati kasnije, putem treće osobe ili e-pošte.

Od zaposlenika se traži da ne slijedi redovne autorizacijske postupke.

KAKO PREPOZNATI ZNAKOVE?

- Neočekivani poziv/poruka
- Izravni kontakt od visokog dužnosnika u tvrtki s kojim obično niste u kontaktu
- Zahtijeva se apsolutna povjerljivost
- Pritisak i uvjeravanje u hitnost
- Neuobičajen zahtjev u suprotnosti s internim postupcima
- Prijetnje, neobična laskanja ili obećanja nagrade

ŠTO MOŽETE UČINITI?

KAO TVRTKA

Budite svjesni rizika i pobrinite se da **zaposlenici budu informirani i upoznati**.

Potaknite zaposlenike da budu **oprezni sa svim zahtjevima za plaćanje.**

Provoditi interne protokole vezane uz plaćanja.

Propisati postupak provjere legitimnosti zahtjeva za plaćanjem primljenih putem e-pošte.

Uspostaviti **pravila za izvještaje** o prijevarama.

Pregledajte informacije objavljene na stranicama svoje tvrtke, **ograničite informacije i pripazite** na društvene medije.

Nadogradite i ažurirajte tehničku sigurnost.

Uvijek se obratite policiji u slučaju pokušaja prijevare, čak i ako niste postali žrtvom.

KAO ZAPOSLENIK

Strogo poštujte sigurnosne postupke za plaćanja i nabave. **Ne preskačite niti jedan korak i ne popuštajte pritisku.**

Uvijek **pažljivo provjeravajte adrese e-pošte** kada se radi o osjetljivim informacijama ili prijenosu sredstava.

U slučaju sumnje o nalogu za prijenos, **obratite se nadležnom kolegi**.

Nikad ne otvarajte sumnjive poveznice ili privitke primljene putem e-pošte. Budite posebno oprezni kada čitate svoju privatnu e-poštu na računalima tvrtke.

Ograničite informacije i budite oprezni s obzirom na društvene medije.

Izbjegavajte dijeljenje informacija o internoj organizaciji tvrtke, sigurnosti i procedurama.

Ako primite sumnjivu e-poštu ili poziv, uvijek obavijestite IT odjel.

EUROPOL EC3 European Cybercrime Centre

#CyberScams