ZAŠTITA OD RAČUNALNIH PRIJEVARA U FINANCIJSKOM POSLOVANJU TRGOVAČKIH DRUŠTAVA I USTANOVA

Prelog, 24. studenog 2023.

DEFINICIJA KIBERNETIČKOG KRIMINALA

Svaka kriminalna aktivnost koja uključuje računalo, mrežni uređaj ili mrežu.

Razlikujemo u 2 kategorije:

1. Napadi u kojima je računalo/mreža cilj napada
2. Napadi u kojima je računalo sredstvo napada

KATEGORIJE KIBERNETIČKOG KRIMINALA

- **Neovlašteni pristup:**

  neovlašteni pristup vlasništvu druge osobe i /ili činjenje štete (npr. „hakiranje“, računalni virusi, obezličenje web-stranica)

- **Cyber-prijevare i krađe:**

  krađa novca i privatnog vlasništva (npr. prijevare s kreditnim karticama; povrede intelektualnog vlasništva - poput „piratstva”)

- **Cyber-pornografija:**

  aktivnosti koje krše zakone opscenosti i pristojnosti

- **Cyber-nasilje:**

  nanošenje psihološke štete ili poticanje fizičkog nasilja, tj. Kršenja prava osoba koje su napadnute (npr. govor mržnje; uhođenje)

CILJEVI KIBERNETIČKOG KRIMINALA

- Financijska korist
- Osobna korist
- Politička korist

FINANCIJSKI UČINAK NA GLOBALNOJ RAZINI

- 15 % rasta godišnje
- do 2025. procjena financijskog učinka = 10,5 bilijuna USD

- Organizirani kriminal
- Stopa otkrivanja počinitelja u USA iznosi 0,05 %

- AI - 45 milijardi USD

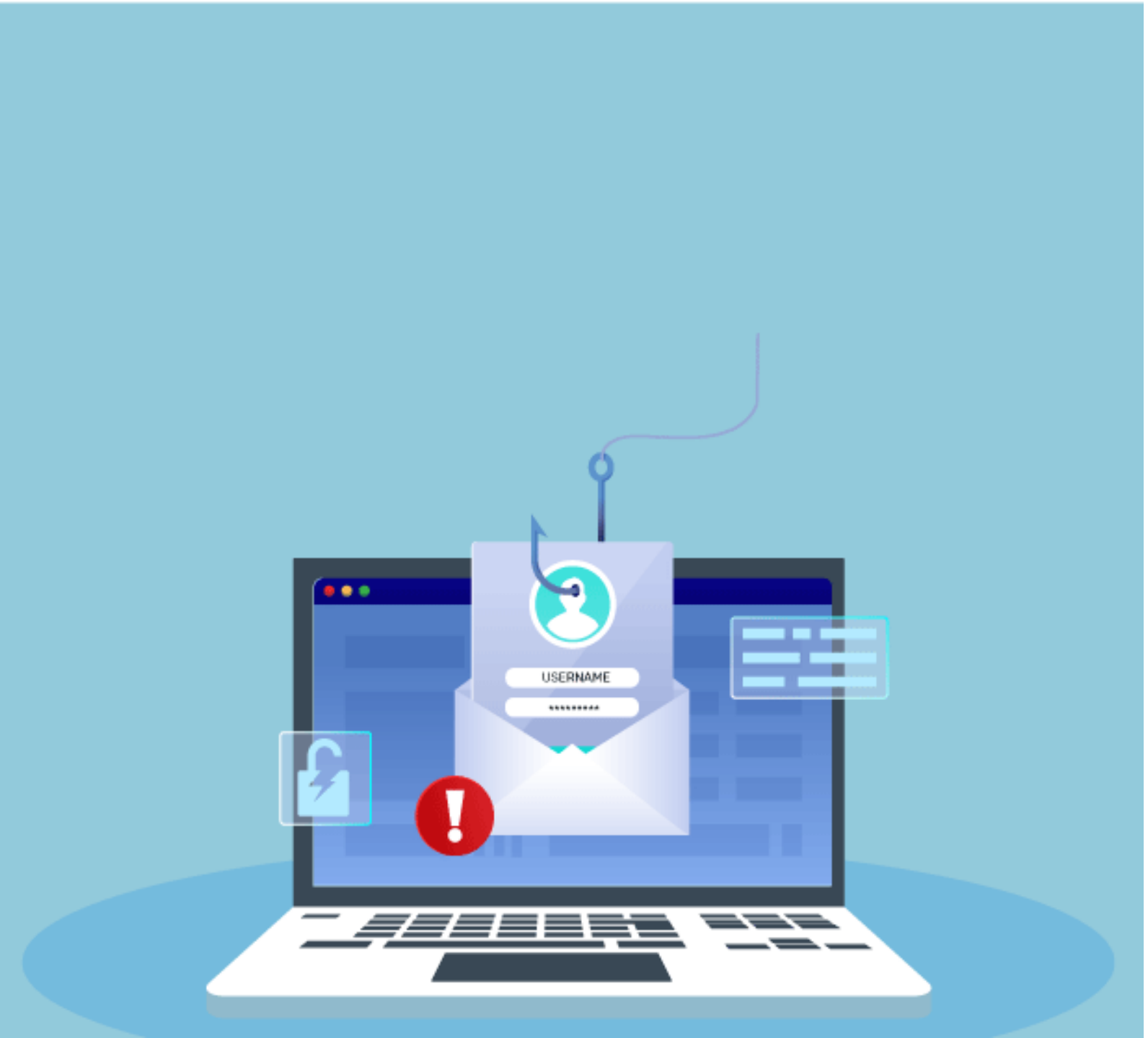
PODACI O SIGURNOSNIM INCIDENTIMA ZA 2023.

- Ukupan broj kompromitiranih podataka
  - 5.367.966.200

- Najznačajniji incident
  - DarkBeam (3.8 milijardi podataka)

TEHNIKE KIBERNETIČKIH NAPADA

- HAKIRANJE
  - Krađa informacijske imovine
  - Izmjena i uništavanje računalnog sustava
  - Obezličenje web stranica i ‘’Spoofing’’
  - Denial of Service Attack – DoS napadi
  - Distribucija malicioznog softvera
  - Povreda autorskih prava
- SOCIJALNI INŽENJERING



SOCIJALNI INŽENJERING

- Umijeće psihološke manipulacije ljudima korištenjem IKT tehnologija
- Prijevara ili varka u svrhu prikupljanja informacija

OBRASCI NAPADA

Priprema napada:

- Identifikacija mete
- Prikupljanje podataka o meti
- Odabir metode napada

Uspostava odnosa:

- uspostava interakcije s metom
- razvijanje interakcije priče
- kontrola interakcije

Iskorištavanje odnosa:

- uspostava jače veze
- otkrivanje podataka i informacija

Provedba napada:

- Ispunjavanje zahtjeva napadača
- Brisanje tragova
- Završetak napada

TEHNIKE Nnapada

Čovjek - Čovjek	• *Impersonation* • *Vishing* • *Eavesdroping* • *Shouldersurfing* • *Dumpster diving* • *Piggybacking/Tailgaiting* • *Honey trap/Catpishing* • *Baiting*
Čovjek - računalo	• *Phising* • *Skočni prozori* • *IM* • *Hoax, scam, lanci sreće, spam*
Čovjek – mobilni uređaj	• *Zlonamjerne aplikacije* • *Lažne sigurnosne aplikacije* • *Smishing*

Phishing

- Phising
- Spear phising
- Vishing
- Pharming
- Smishing

Prepoznavanje phising napada

- Nepoznat pošiljatelj
- Neubičajeno vrijeme i datum poruke
- Dojam hitnosti
- Privitci
- Zahtjev za otvaranjem linka
- Hyper link

---------- Forwarded message---------
From: **e-Građani** <info@egradani.com>
Subject: Potvrda o prihvaćanju automatskog zahtjeva za pomoć u stanovanju

Poštovani,

Obavještavamo Vas da je Vaš zahtjev za pomoć u stanovanju za 2023. godinu automatski odobren.

Temeljem Zakona o socijalnoj skrbi (»Narodne novine«, br. 18/22. i 46/22.), Republika Hrvatska će Vam pružiti financijsku pomoć z
stanovanje.
Nakon pregleda Vaših prihoda u prošloj godini, utvrđeno je da imate pravo na pomoć u iznosu od 250,89 €.

Vaš privremeni lozinka za pristup pomoćnom dodatku je 651811.

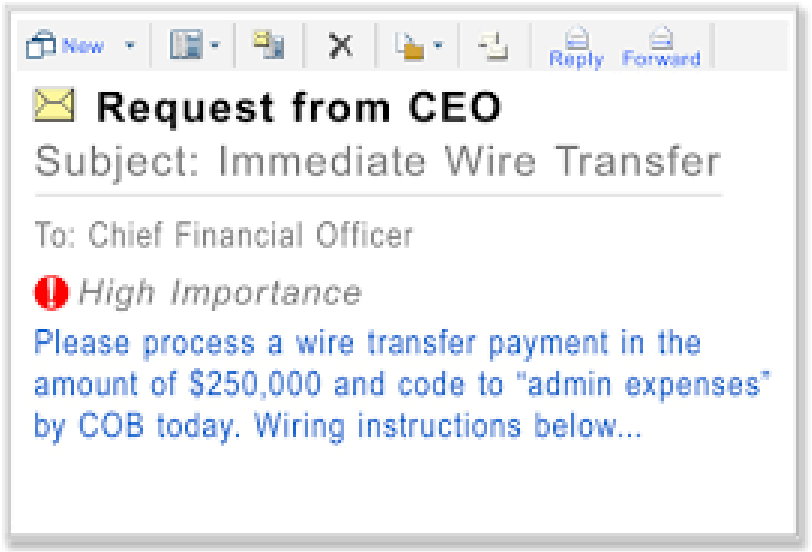
Kako bismo osigurali sigurnost naših korisnika, skenirajte ovaj QR kod za pristup našem portalu e-Gradani.

Radi vaše sigurnosti, vaša će privremena zaporka isteći za 48 sati.

Zahvaljujemo Vam na povjerenju.
S poštovanjem,
Ministarstvo rada, mirovinskoga sustava, obitelji i socijalne politike

e-Građani, Ulica grada Vukovara 33, 1000 Zagreb, Croatia

CEO/Direktorska prijevara



- Vrsta spear phising-a
- Prevarant se predstavlja kao direktor ili član uprave društva
  - Uplata na račun
  - Dostava osjetljivih informacija

2 oblika:

- *name spoofing*
- *Name and e-mail spoofing*

Prepoznavanje napada

- Traži hitna plaćanja
- Međunarodni račun
- ‘’povjerljivost’’, ‘’nedostupnost’’
- Zahtjeva se odstupanje od uobičajenih postupaka

Prijevara s računima

- varalice se pretvaraju da su vaši klijenti/dobavljači i navode vas da platite buduće račune na drugi bankovni račun

ZAŠTITA OD CEO PRIJEVARE I PRIJEVARES RAČUNIMA

Organizacijske mjere

- Informiranje i upoznavanje zaposlenika s rizicima
- Oprez prilikom svih zahtjeva za plaćanje
- Uspostaviti interne protokole vezane za plaćanja
- Propisati postupak provjere legitimnosti zahtjeva za plaćanjem
- Uspostaviti financijske standarde i standarde informacijske sigurnosti za sprečavanje napada
- Uspostaviti tehničke kontrole zaustavljanja zlonamjernih poruka (e-mail filteri, DMARC).
- Definiranje plana rizika i periodična edukacija postojećih i novih zaposlenika
- Provođenje izvanrednih kontrola

ZAŠTITA OD CEO PRIJEVARE I PRIJEVARES RAČUNIMA

Zaposlenici:

- Poštivanje sigurnosnih postupaka i protokola
- Pažljiva provjera adrese e-pošte
- U slučaju sumnje obratiti se nadređenom ili IT službi
- Izbjegavati dijeljenje informacija o internoj organizaciji
- Ne otvarati poveznice ili privitke
- Ograničiti uporabu privatne e-pošte na službenom računalu

NAJSKUPLJI SLUČAJEVI

XOOM
https://www.reuters.com/article/us-xoom-fraud-idUSKBN0KE1WA20150105/

UBIQUITI
https://www.nbcnews.com/tech/security/ubiquiti-networks-says-it-was-victim-47-million-cyber-scam-n406201

FACC
https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF/

Crelan Bank
https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/

Facebook and Google
https://www.goptg.com/blog/meet-the-man-whose-phishing-scam-robbed-google-and-facebook-of-millions

RH PRIMJERI

Prevarant se djelatnici tvrtke iz Valpova predstavio kao direktor i tražio da na neki račun uplati 31.000 eura: Nasjela je
https://www.jutarnji.hr/vijesti/crna-kronika/prevarant-se-djelatnici-tvrtke-iz-valpova-predstavio-kao-direktor-i-trazio-da-na-neki-racun-uplati-31-000-eura-nasjela-je-15296655

Na hakirani račun druge tvrtke direktor uplatio oko 200.000 kuna
https://glas-slavonije.hr/432696/8/Na-hakirani-racun-druge-tvrtke-direktor-uplatio-oko-200000-kuna

Najnovija prijevara kruži internetom: 45-godišnjakinja iz Bjelovara ostala bez 67.000 eura
https://www.poslovni.hr/hrvatska/najnovija-prijevara-kruzi-internetom-45-godisnjakinja-iz-bjelovara-ostala-bez-67-000-eura-4409599

2022.
1864 kaznena djela
6.000.000,00 EUR

Baiting

- obećanje nagrade
- temelji se na pohlepi žrtve

Impersonation

- Lažno predstavljanje
- Stvaranje uvjerenja kako se radi o legitimnom sugovorniku

Shoulder surfing

- potajno gledanje
- prisluškivanje

Dumpster diving

- Kopanje po smeću
- Rezultat nepropisnog zbrinjavanja dokumentacije

Pretexting

- Korištenje stvarnog ili izmišljenog scenarija
- Obrnuti socijalni inženjering
- Stvaranje laži

Piggybacking/ Tailgating

- Fizički pristup zaštićenim lokacijama
- Piggybacking – pristup lokaciji oponašanjem
- Tailgaiting – pristup lokaciji potajno

ORGANIZACIJSKE MJERE ZA SPRJEČAVANJE NAPADA

- Periodična edukacija o sigurnom radu i opasnostima socijalnog inženjeringa
- Uspostava jasnih politika i postupaka za zaposlenike
- Uspostava planova za upravljanje kriznim situacijama
- Ulaganje

TEHNIČKE MJERE ZA SPRJEČAVANJE NAPADA

- Nadogradnja hardvera i softvera
- Antivirusna zaštita i vatrozid
- Zaštita od neovlaštenog pristupa
- Dvovektorska autentifikacija
- Uspostava politike lozinki
- Korištenje spam filtera
- Backup
- Need to know princip

INDIVIDUALNE MJERE ZAŠTITE

- Automatsko zaključavanje uređaja u stanju mirovanja dulje od 5 minuta
- Redovita izmjena lozinki
- Postavke web pretraživača
- Ne otvarajte e-poštu iz nepouzdanih izvora.
- Zaključajte prijenosno računalo kad god niste na radnoj stanici
- Poznavanje pravila o zaštiti podataka i informacijske sigurnosti organizacije
- Poštivanje propisanih postupaka
- Ne koristiti neslužbenu perifernu računalnu opremu
- Backup

UČINCI CYBER KRIMINALA NA POSLOVANJE

- Izravni financijski učinak
  - Pretrpljeni financijski gubitak
  - Smanjenje vrijednosti kompanije
  - Novčane kazne
  - Ulaganja u sigurnost

- Neizravni financijski učinak
  - Reputacijska šteta
  - Gubitak poslovne tajne

KAZNENI ZAKON RH (''Narodne novine'' broj: 125/2011, 144/2012, 61/2015, 56/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022 i 114/2023)

KAZNENA DJELA PROTIV RAČUNALNIH SUSTAVA, PROGRAMA I PODATAKA

- (članci 266.-273.)

  - Neovlašteni pristup
  - Ometanje rada računalnog sustava
  - Oštećenje računalnih podataka
  - Neovlašteno presretanje računalnih podataka
  - Računalno krivotvorenje
  - Računalna prijevara
  - Zlouporaba naprava
  - Teška kaznena djela protiv računalnih sustava, programa i podataka

ZAHVALJUJEM NA PAŽNJI