e-Sveučilišta

Osnove kibernetičke zaštite i prepoznavanje kibernetičkih prijetnji

Priručnik

Autorica:

Marina Dimić Vugec

- CARNET, Sektor Nacionalni CERT

Zagreb, svibanj 2025.

Financira Europska unija NextGenerationEU

CARNET

Sadržaj

PREGLED

Cilj radionice

Prepoznavanje i postupanje kod kibernetičkih prijetnji i incidenata.

Naučiti kako se zaštititi i povećati kibernetičku otpornost ustanove (VU) i pojedinca – korisnika IKT resursa.

Usvojiti osnove kibernetičke zaštite na razini pojedinca.

Usvojiti osnove kibernetičke zaštite na razini ustanove.

Ishodi učenja

Nakon ove radionice polaznici će:

- Znati prepoznati kibernetičke prijetnje
- Ispravno postupati kod pojave kibernetičkog incidenta
- Znati osnovne oblike zaštite i povećanja kibernetičke otpornosti na razini pojedinca i ustanove
- Primijeniti znanje u praktičnom radu

1. UVOD

Definicija kibernetičke sigurnosti

Kako bismo razumjeli svrhu, primjenu i održavanje kibernetičke zaštite važno je pojasniti pojam kibernetičke sigurnosti.

Kibernetička sigurnost ima brojne definicije ovisno o kontekstu i prigodi. Jedna od definicija navodi da su to sve aktivnosti koje su nužne za zaštitu od kibernetičkih prijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu.

Druga je definicija više usmjerena na organizacijske i tehničke aspekte i definira kibernetičku sigurnost kao sustav organizacijskih i tehničkih aktivnosti te mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru.

Definicija kibernetičke zaštite

Kibernetička se zaštita može koristiti kao sinonim kibernetičke sigurnosti, ali postoji razlika ovih pojmova u vidu obuhvata i primjene svakog od njih u praksi.

Kibernetička je zaštita također skup tehnologije, procesa, aktivnosti i praksi osmišljenih za zaštitu računalnih sustava, mreža, uređaja i podataka od neovlaštenog pristupa, oštećenja, krađe ili drugih oblika napada.

Glavni cilj kibernetičke sigurnosti i zaštite je zaštita podataka prema tzv. načelima CIA trijade:

- Povjerljivost (Confidentiality) – zaštita podataka od neovlaštenog pristupa.

- Cjelovitost (Integrity) – zaštita podataka od neovlaštenih izmjena ili brisanja.
- Dostupnost (Availability) – zaštita dostupnosti sustava i podataka ovlaštenim korisnicima kad god su im potrebni.

Područja kibernetičke zaštite uključuju sigurnost mreže, aplikacija, korisničkih uređaja, upravljanje identitetima i pristupima, edukaciju zaposlenika i postupanje s kibernetičkim incidentima.

Razlika između kibernetičke sigurnosti i kibernetičke zaštite

Kibernetička sigurnost širi je pojam koji obuhvaća zaštitu sustava, mreže i podataka i odnosi se na strategije, politike, tehnologije i procese koji štite od kibernetičkih prijetnji i osiguravaju određenu razinu otpornosti na kibernetičke napade. Kibernetička sigurnost uključuje prevenciju kibernetičkih napada, upravljanje rizicima, postupanje s incidentima, edukaciju korisnika i usklađenost s pravnim i regulatornim okvirima. Primjer dokumenta iz područja kibernetičke sigurnosti je sigurnosna politika ustanove.

Kibernetička zaštita konkretne su mjere i alati koji se koriste u zaštiti sustava i podataka i odnosi se na operativnu provedbu mjera sigurnosti i zaštitu u praksi. Kibernetička zaštita uključuje antivirusne programe, postavke vatrozida, postavke sigurnosnog kopiranja, šifriranje podataka, kontrolu pristupa i edukaciju zaposlenika. Primjer je konfiguracija vatrozida na poslužitelju.

Važnost kibernetičke zaštite ustanove (VU)

Obrazovne su ustanove česta meta kibernetičkih napada zbog osjetljivih podataka koje posjeduju.

Mjere kibernetičke zaštite obuhvaćaju organizacijske, tehničke i mjere koje se odnose na jačanje otpornosti ljudskih potencijala i korisnika.

Glavni razlozi zašto uspostave i primjene mjera kibernetičke zaštite:

- Zaštita podataka zaposlenika, studenata, suradnika i partnera ustanove
- Usklađenost s propisima
- Sigurnost istraživačkih i znanstvenih radova
- Održavanje kontinuiteta rada i ugleda

Fakulteti kao obrazovne, znanstvene i istraživačke ustanove obrađuju velike količine osjetljivih podataka i suočavaju se s raznim prijetnjama. Kibernetička zaštita podrazumijeva zaštitu podataka studenata, zaposlenika i fakulteta.

Bez odgovarajuće razine kibernetičke zaštite postoji rizik od curenja, gubitka ili zloupotrebe podataka, što može narušiti povjerenje studenata i partnera i izazvati pravne, reputacijske i financijske posljedice.

Fakulteti su obvezni uskladiti svoje prakse s pravnim i regulatornim okvirima koji se odnose na zaštitu podataka i kibernetičku sigurnost:

- GDPR (Opća uredba o zaštiti podataka):

  - Štiti osobne podatke građana EU-a i obvezuje fakultete na sigurno prikupljanje, obradu i pohranu podataka.
  - U slučaju kršenja, prijete visoke kazne i narušavanje ugleda institucije.
- Zakon o kibernetičkoj sigurnosti:
  - Definira obveze za sigurnost IT infrastrukture, uključujući mreže i sustave koji su ključni za rad fakulteta.
  - Fokus je na prevenciji napada i odgovoru na incidente.

Fakulteti posjeduju brojna znanstvena istraživanja, baze podataka i informacije o inovativnim projektima poput:

- Povjerljivih rezultata istraživanja.
- Suradnje s industrijom i partnerima (patenti, komercijalno vrijedni podaci).

Kibernetičke prijetnje koje mogu ugroziti takvu informacijsku imovinu:

- Krađa intelektualnog vlasništva.
- Curenje osjetljivih podataka prije objavljivanja ili komercijalizacije.

Kibernetička zaštita obuhvaća:

- Jasno definirana pravila i tehničke mjere (npr. kriptiranje podataka, kontrola pristupa) štite znanstvene i istraživačke projekte od neovlaštenog pristupa i kibernetičkih napada.

Kibernetički napadi poput ransomwarea ili DDoS napada mogu paralizirati rad fakulteta, onemogućiti pristup e-učenju, istraživačkim bazama i administrativnim sustavima.

U mjere zaštite spadaju:

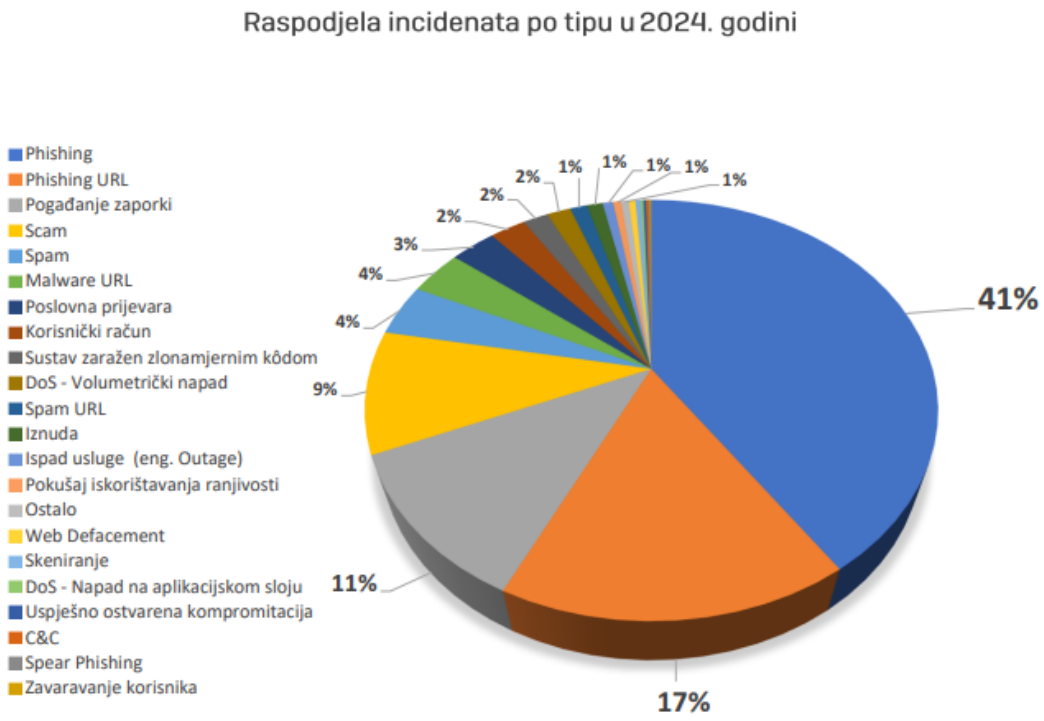
  - Jasna podjela zaduženja i odgovornosti u zaštiti podataka
  - Plan upravljanja incidentima (brži oporavak i nastavak rada)
  - Tehničke mjere poput sigurnosnih kopija podataka (backup)
  - Edukaciju korisnika (zaposlenika i studenata) kako bi smanjili ljudske pogreške

Važnost: Prevencija incidenata smanjuje prekide u radu i štiti ugled fakulteta kao pouzdane institucije.

2. NAJČEŠĆI TIPOVI KIBERNETIČKIH PRIJETNJI I INCIDENATA NA VISOKIM UČILIŠTIMA

- Phishing kampanje
- CEO fraud
- Scam
- Sustavi zaraženi zlonamjernim kôdom
- Kompromitacija korisničkih računa
- Ransomware

Prikaz tipova incidenata u 2024. godini



U 2024. godini Nacionalni CERT obradio je 1113 kibernetičkih incidenata od kojih je 58 % pripadalo tipu phishing i phishing URL. Neprestano se bilježi porast ovog tipa incidenta u službenim statistikama, a ono što je važno naglasiti odnosi se na različite tehnike i njihov stalni razvoj koji se primjenjuju u provedbi takvih napada s ciljem krađe podataka ili stjecanja novčane koristi.

Phishing

Phishing je pokušaj navođenja korisnika na odavanje povjerljivih podataka ili pokretanje zlonamjerog programa, putem elektroničke pošte; SMS-a (smishing), poziva (vishing), QR kôda (quishing).

Postoje različite vrste phishinga:

- *whaling, spearphishing* = lažna poruka koja cilja određenu osobu ili tvrtku
- *catfishing* = romantična prijevara u kojoj se razvija emocionalni odnos s napadačem kojem je najčešće cilj ostvarivanje novčane koristi ili zadobivanje povjerenja za neke druge napade ili izvlačenje podataka
- *scam* = pokušaj navođenja potencijalne žrtve na djelovanje u korist prevaranta npr. „nigerian scam“ ili „419 fraud“
- *iznuda* = pokušaj navođenja korisnika na plaćanje otkupnine, najčešće lažnim informacijama i zastrašivanjem, npr. sextortion

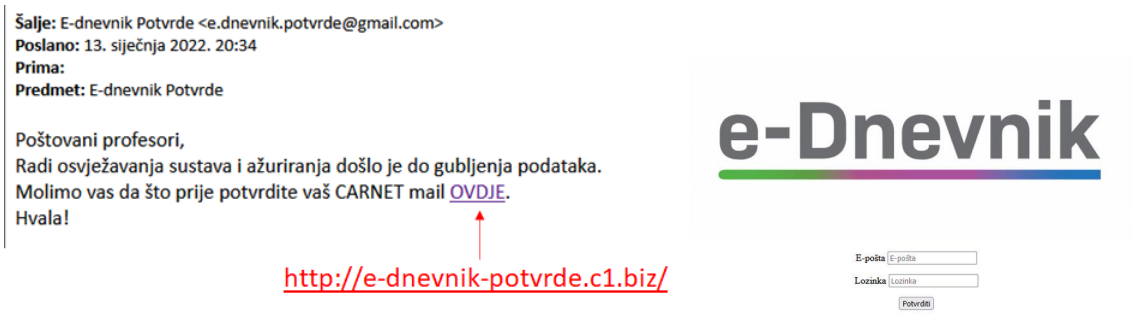
- *poslovna prijevara* = napad kod kojeg napadač lažnim predstavljanjem pokušava steći ili stekne financijsku korist od ciljanog poslovnog korisnika, npr. „CEO fraud“ ili „BEC - Business Email Compromise“ prijevare.

Phishing poruke važno je prepoznati zato što one mogu biti samo početna točka za druge i daljnje napade, prikupljanje povjerljivih podataka (osobni podaci, podaci bankovnih kartica, podaci korisničkih računa, podaci o ustanovi i slično). Posljedice uspješnih phishing napada mogu biti financijski gubici, krađe identiteta, reputacijska šteta.

U phishing kampanjama koje ciljaju veći broj korisnika najčešće se pojavljuju ključne riječi, teme i sadržaji:

- Verifikacija računa
- Dijeljenje datoteka putem oblaka
- Dostava paketa
- Poruke Porezne uprave
- Poruke o obavijestima MUP-a
- Lažni računi
- Kompromitirani računi e-pošte
- Poruke vezane uz GDPR
- Sextortion
- Kriptovalute
- Političke kampanje
- Hrana / lijekovi

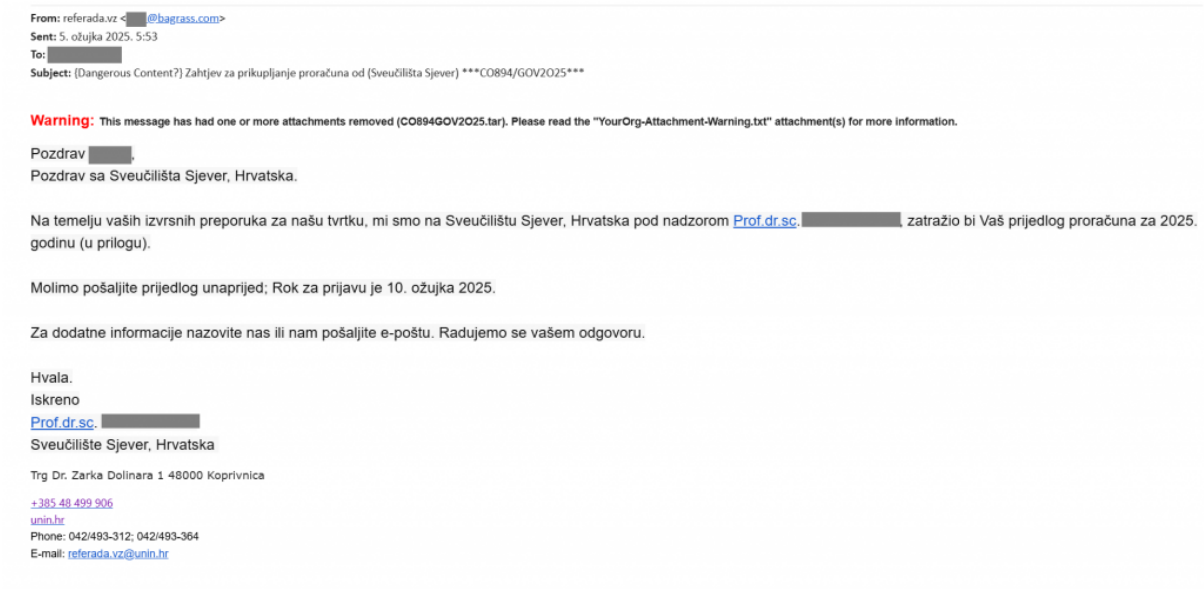
Primjeri phishinga



Znakovi alarma:

- U e-poruci dostavlja se informacija u kojoj se traži brza reakcija primatelja i lažni URL – poveznica
- Poruka stiže s adrese gmail.com
- Traži se brza reakcija i izaziva osjećaj straha radi gubitka podataka
- Nudi se poveznica koja je vidljiva prijelazom miša preko nje i koja ne vodi na ispravnu domenu

Klikom na lažnu poveznicu traže se podaci za ulazak u servis koji imitira e-Dnevnik sustava i traži unos korisničkih podataka. Unosom podataka omogućili smo napadaču da se s našim podacima ulogiraju u legitiman servis e-Dnevnik ili na druge servise na kojima koristimo iste korisničke podatke. Podaci se mogu iskoristiti za druge napade ili prodati na *dark webu*.



From: referada.vz <[redacted]@bagrass.com>
Sent: 5. ožujka 2025. 5:53
To: [redacted]
Subject: {Dangerous Content?} Zahtjev za prikupljanje proračuna od {Sveučilišta Sjever} ***CO894/GOV2O25***

Warning: **This message has had one or more attachments removed (CO894GOV2O25.tar). Please read the "YourOrg-Attachment-Warning.txt" attachment(s) for more information.**

Pozdrav [redacted],
Pozdrav sa Sveučilišta Sjever, Hrvatska.

Na temelju vaših izvrsnih preporuka za našu tvrtku, mi smo na Sveučilištu Sjever, Hrvatska pod nadzorom Prof.dr.sc. [redacted], zatražio bi Vaš prijedlog proračuna za 2025. godinu (u prilogu).

Molimo pošaljite prijedlog unaprijed; Rok za prijavu je 10. ožujka 2025.

Za dodatne informacije nazovite nas ili nam pošaljite e-poštu. Radujemo se vašem odgovoru.

Hvala.
Iskreno
Prof.dr.sc. [redacted]
Sveučilište Sjever, Hrvatska
Trg Dr. Zarka Dolinara 1 48000 Koprivnica
+385 48 499 906
unin.hr
Phone: 042/493-312; 042/493-364
E-mail: referada.vz@unin.hr

Znakovi alarma:

- Poruka stiže s nepoznate adrese i nije iz domene potpisanog pošiljatelja
- Kratak rok
- Nedovoljno definiran i neočekivan privitak i zadatak
- Legitiman potpis, ali nema poveznice s adresom pošiljatelja

Zlonamjeran privitak može sadržavati malver koji se pokreće u pozadini i može pokrenuti napad npr. ransomwarom jer nam zaključava datoteke i stiže nam poruka uz traženje otkupnine za dekriptor i ključ za dešifriranje naših datoteka.

ZAHTJEV ZA PONUDU (Sveučilište u Zagrebu) EUI894/BU466

SU Incident <incident-bounces@cert.hr> on behalf of Sveučilište u Zagrebu <admin@unizg.hr>
To undisclosed-recipients:

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

ZAHTJEV ZA PONUDU 16-08-2023.rar 888 KB
Untitled attachment 00046.txt 128 bytes

University of Zagreb

Pozdrav sa Sveučilišta u Zagrebu,

Pažnja:

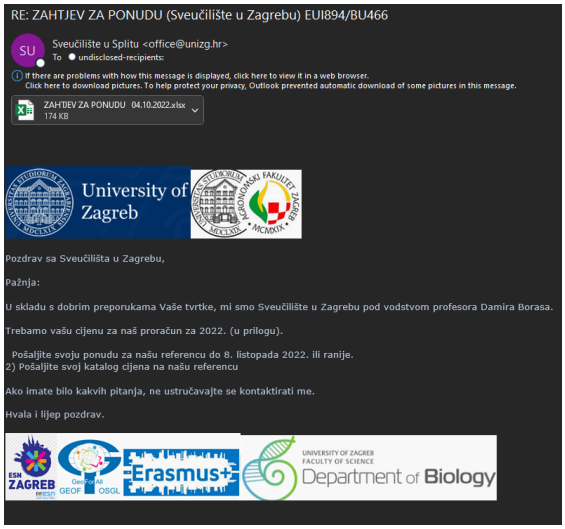
U skladu s dobrim preporukama vaše tvrtke, mi smo Sveučilište u Zagrebu pod vodstvom profesora Damira Borasa.

Potrebna nam je vaša cijena za naš proračun za 2023. godinu (u prilogu).

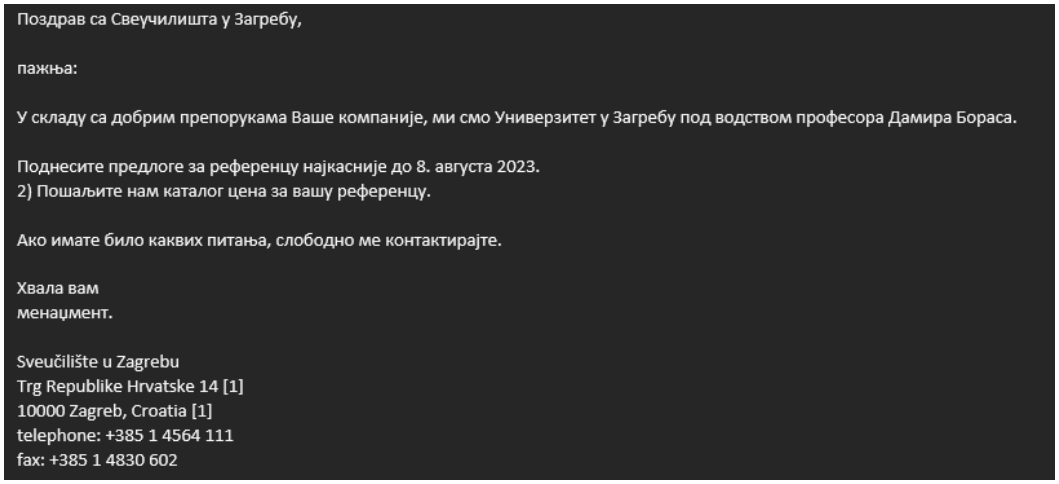
Pošaljite svoju ponudu na rok od 20. kolovoza 2023. ili prije njega.

Lijep pozdrav

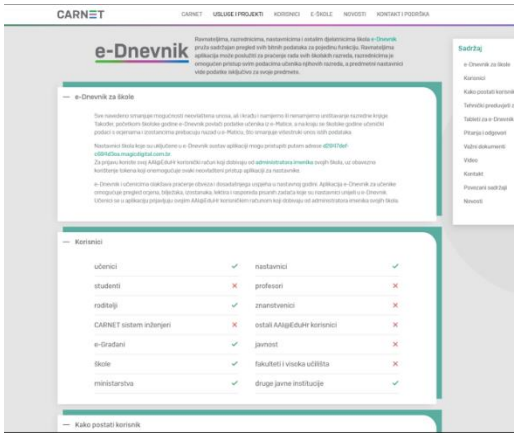
Admin

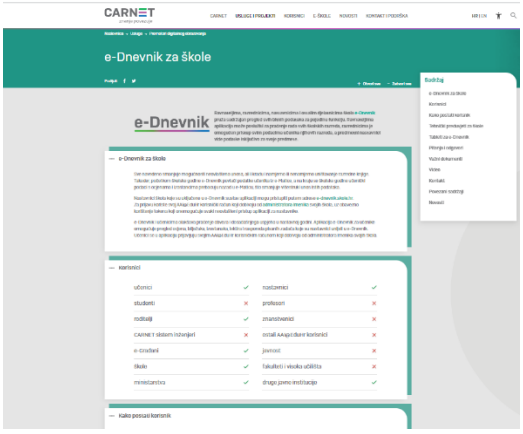


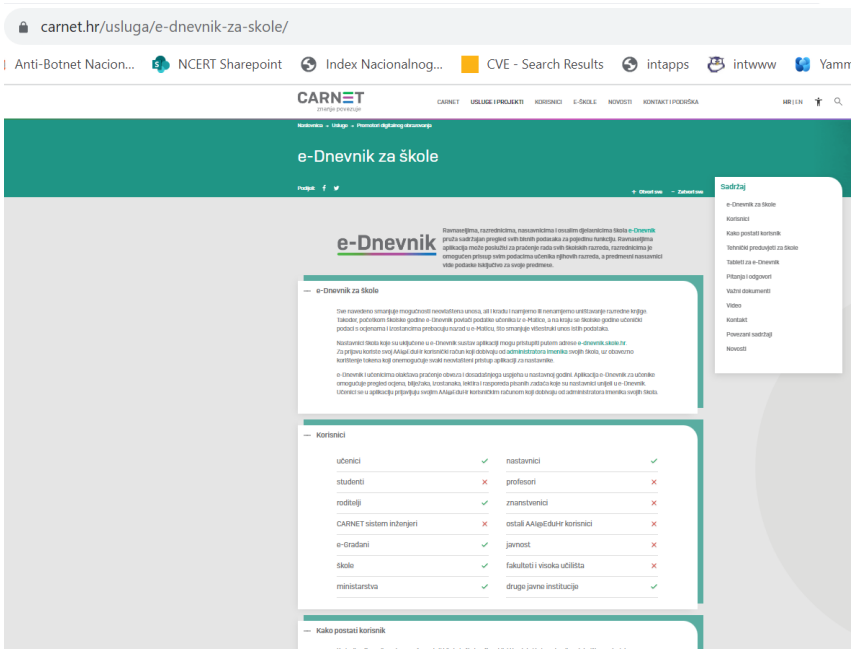
Primjer phishing kampanje u kojima se koriste podaci različitih visokih učilišta kao pošiljatelja e-poruke, a u poruci se nalazi privitak čijim se otvaranjem pokreće neki zlonamjerni program. Na takav način može se pokrenuti i malver za šifriranje datoteka – ransomware.

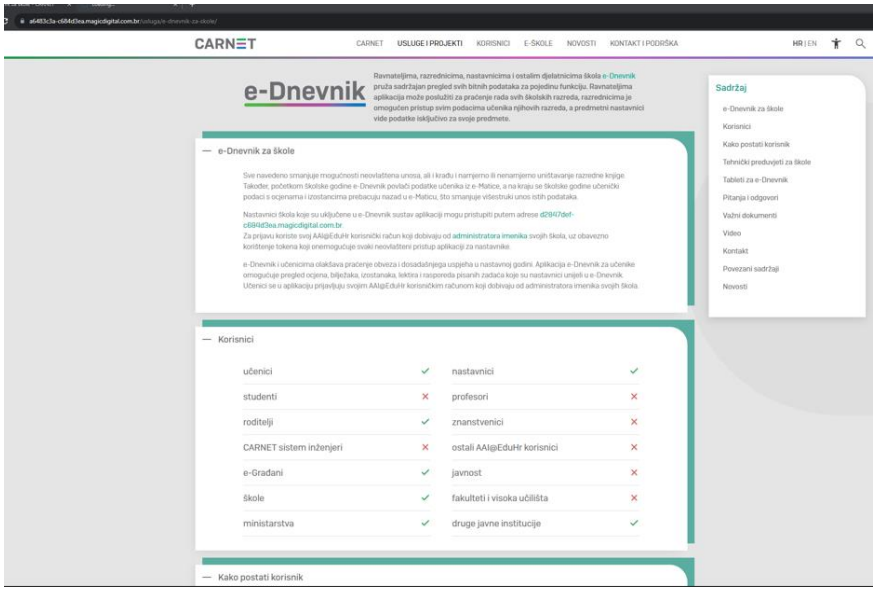


Primjer loše phishing poruke u kojoj je napadač pisao ćirilicom, a u potpisu iskoristio legitiman potpis institucije.









Primjer imitacije legitimne stranice. Većim dijelom sadržaja lažna stranica u potpunosti kopira izvornu legitimnu stranicu, ali nedostaju neki vizualni elementi i sam URL stranice ne odgovara domeni e-dnevnika.

Kako prepoznati phishing?[1]

Phishing smatramo ozbiljnom prijetnjom zbog njegove česte uporabe, ali i zato što od njega mogu krenuti brojni drugi napadi.

[1] https://www.cert.hr/prepoznaj-phishing-u-5-koraka/

Također, u posljednje vrijeme primijetili smo povećan broj naprednih phishing napada koji koriste ispravnu gramatiku i nove tehnike prijevare kao što je korištenje QR kôda umjesto poveznice.

Budući da je pokušaje phishinga gotovo nemoguće spriječiti, moramo raditi na prevenciji stalnom edukacijom.

CEO fraud

Ovakva vrsta napada najčešće započinje istraživanjem i prikupljanjem podataka o nadležnim osobama ili osobama na rukovodećim pozicijama (CEO, ravnatelj). To se može provesti tzv. OSINT metodom – prikupljanjem svih dostupnih podataka na internetu o određenoj osobi, podataka dostupnih na društvenim mrežama, povezane osobe, tvrtke ili socijalnim inženjeringom na način da se kontaktira zaposlenik

izravno, telefonom ili nekim drugim putem i dobiju potrebne informacije za nastavak napada.

U primjeru napadač lažira polje pošiljatelja da izgleda kao da je e-pošta poslana s legitimne adrese ili kompromitira stvarni korisnički račun e-pošte. Najčešće su cilj napada službe ljudskih potencijala, kadrovska ili službe financija, računovodstvo.

Poruka sadrži zahtjev za nekom financijskom transakcijom i traži se hitno postupanje. Može se tražiti i dostava nekog npr. financijskog plana, izvješća ili podataka koji se smatraju povjerljivim internim podacima ustanove.

Cilj napada može biti ostvarivanje novčane koristi, prikupljanje povjerljivih informacija i iskorištavanje prikupljenih podataka za planiranje daljnjeg napada, počinjenje reputacijske štete i slično.

Koristi se pozicija autoriteta i traži se žurna reakcija.

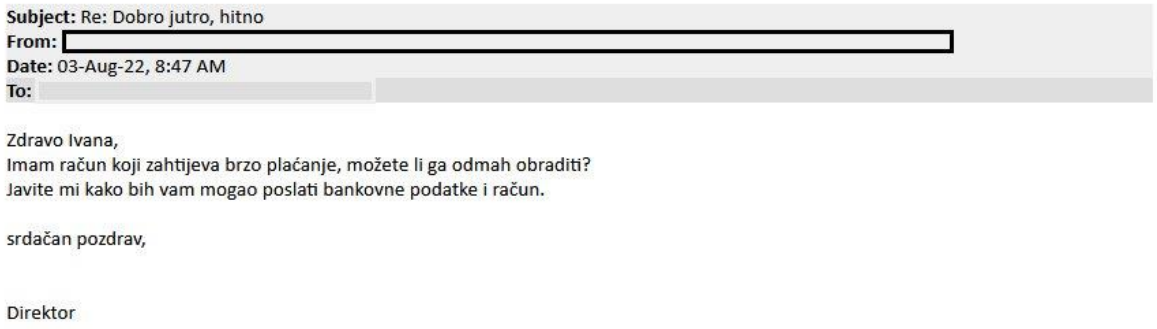
From: [redacted]
Sent: Tuesday, October 3, 2017 9:43 AM
To: [redacted]
Subject: RE: Bankovni transfer

zdravo,

Morate se pobrinuti za medunarodne doznake danas. Jesi li na vasem stolu? Pustiti mene znati tako ja mogu poslati te podatke o banci.

Hvala

S postovanjem,
[redacted]



Subject: Re: Dobro jutro, hitno
From: [redacted]
Date: 03-Aug-22, 8:47 AM
To: [redacted]

Zdravo Ivana,
Imam račun koji zahtijeva brzo plaćanje, možete li ga odmah obraditi?
Javite mi kako bih vam mogao poslati bankovne podatke i račun.

srdačan pozdrav,

Direktor

Ransomware

Jedna je od najvećih prijetnji, vrsta zlonamjernog programa kojem je cilj šifriranje računalnog sustava ili datoteka žrtve i traženje otkupnine. U takvim napadima traži se hitna reakcija i postavljen je vremenski rok za plaćanje otkupnine u obliku tzv. ransom note ili poruke.

Ransomware se može pokrenuti kao zlonamjerni program putem elektroničke pošte, web stranica ili fizičkog uređaja.

Za neke poznatije vrste ransomware malvera postoje tzv. dekriptori ili ključevi za dešifriranje. Određeni projekti međuinstitucionalne i međunarodne suradnje dijele

informacije, preporuke i podatke o dekriptorima i omogućavaju servise za dešifriranje datoteka ako je ključ dostupan. (NoMoreRansom[2], Kripto šerif[3]).

Kod sumnje na zarazu računala i mreže ransomwarom vrlo je važna brza reakcija (posložen interni sustav; alocirano osoblje; procedure/sig. politika), ukloniti zaražene sustave s mreže i provjeriti stanje sigurnosne kopije podataka.[4]

Zaštita i prevencija od ransomware napada obuhvaća redovito ažuriranje i praćenje kritičnih ranjivosti, izradu sigurnosnih kopija i njihovog testiranja, segmentaciju mreže, složene lozinke i korištenje 2FA (dvofaktorske) i MFA (multifaktorske) verifikacije, edukaciju korisnika, zaposlenika, partnera, suradnika, studenata i omogućavanje pristupa sustavima samo autoriziranim i ovlaštenim osobama.

Primjer ransomware poruke:

Scam

Scam je pokušaj vještog navođenja potencijalne žrtve na djelovanje u korist prevaranta npr. nigerijski princ / romantična prijevara / brza zarada / humanitarna akcija.

Primjer scam poruke:

Pažnja: korisnik sredstava,

Poslao sam vam ovo pismo prije mjesec dana, ali nisam se javio, nisam siguran da li ste ga dobili, i zato ga ponavljam. Prvo, ja sam gđa Kristalina Georgieva, generalni direktor i Predsjednica Međunarodnog monetarnog fonda.

Doista, pregledali smo sve prepreke i probleme koji okružuju vašu nedovršenu transakciju i vašu nemogućnost da se suočite s troškovima prijenosa koji su vam naplaćeni, za prethodne opcije prijenosa, pogledajte našu stranicu za svoju potvrdu www.imf.org

Mi smo Upravni odbor Svjetske banke i Međunarodnog monetarnog fonda
(MMF) Washington, D.C. u suradnji s Ministarstvom financija SAD-a i nekim drugim relevantnim istražnim agencijama ovdje u Sjedinjenim Američkim Državama. je naredio našoj jedinici za doznake stranih plaćanja, United Bank of Africa Lome Togo da vam izda VISA karticu, na koju će se učitati vaš fond od 1,5 milijuna USD, za daljnje povlačenje vašeg fonda.

Tijekom naše istrage, sa zaprepaštenjem smo otkrili da je vaše plaćanje nepotrebno odgođeno od strane korumpiranih službenika Banke koji pokušavaju preusmjeriti vaša sredstva na svoje privatne račune.

I danas vas obavještavamo da je vaš fond uplaćen na VISA karticu od strane UBA Banke i da je spreman za isporuku. Sada kontaktirajte pomoć UBA banke g. Tony Elumelu E-mail (mr.tonyelumelu10@gmail.com) Pošaljite joj sljedeće informacije za dostavu vaše akreditirane VISA kartice na bankomatu na vašu adresu.

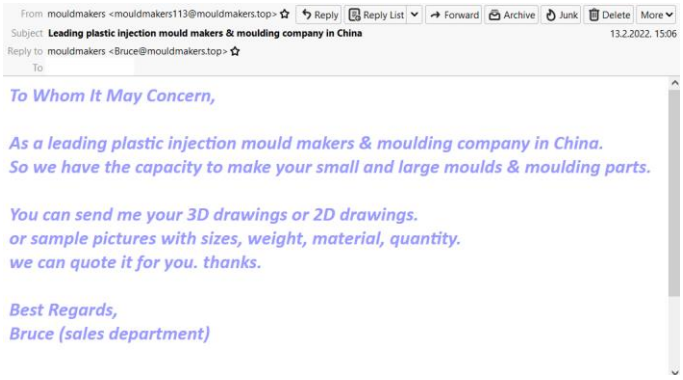
Vaše puno ime==========
Vaša zemlja podrijetla==========
Vaša kućna adresa ==========
Vaš telefonski broj ==========

[2] https://www.nomoreransom.org/cro/index.html
[3] https://www.nomoreransom.org/crypto-sheriff.php?lang=cro
[4] https://www.cert.hr/newsletter-nacionalnog-cert-a-cert-info-3/

Spam

Spam je neželjena elektronička poruka reklamnog sadržaja.

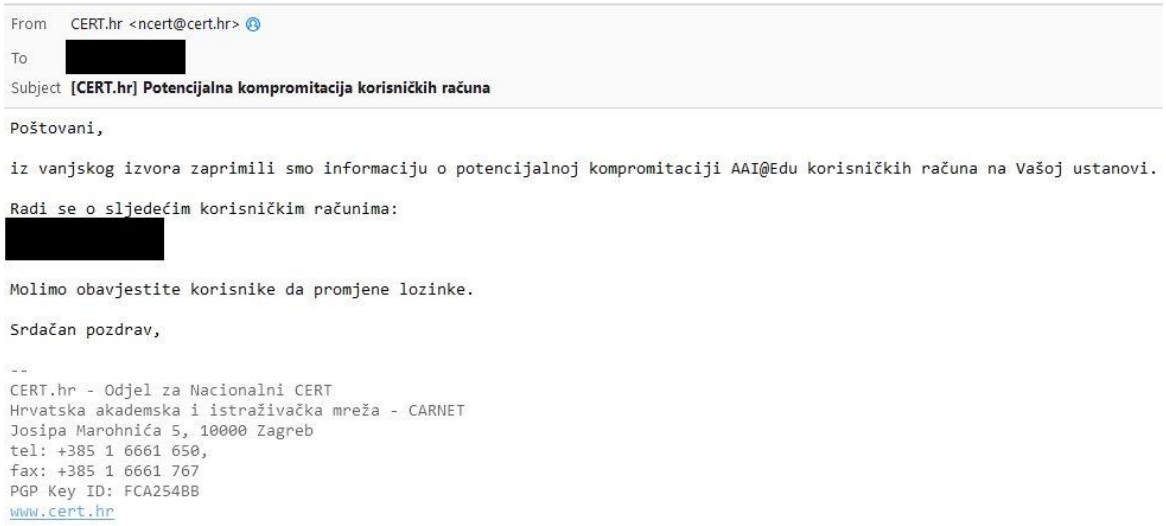
Primjer spam poruke:



Kompromitacija korisničkog računa

Nacionalni CERT šalje obavijesti ustanovama u vezi informacija o kompromitiranim računima uz uputu što se treba poduzeti u vezi toga.

Potrebno je brzo postupanje i izvještavanje Nacionalnog CERT-a o poduzetim mjerama.



Kratka vježba! – Provjerite je li vaš mail kompromitiran

Korištenjem servisa Have I been Pwned? za provjeru kompromitacije adrese elektroničke pošte dostupnog na *https://haveibeenpwned.com/* provjerite nalazi li se vaša adresa elektroničke pošte u nekoj od kompromitiranih baza podataka.

U slučaju kompromitacije savjetujemo promjenu lozinke na svim servisima gdje koristite te korisničke podatke odnosno povezano s adresom e-pošte koju ste provjeravali.

3. OSNOVE KIBERNETIČKE ZAŠTITE ZA POJEDINCE

Osnove kibernetičke zaštite za pojedince obuhvaćaju skup pravila, alata i ponašanja koji pomažu u zaštiti osobnih podataka i uređaja od kibernetičkih prijetnji.

- Pridržavati se pravila kibernetičke higijene
- Upoznati se sa sigurnosnom politikom ustanove
- Edukacija i pozornost – promisliti prije bilo kakve akcije, provjeriti sve sumnjivo ili neočekivano drugim kanalima komunikacije
- Uvijek koristiti drugi kanal komunikacije za provjeru sumnjivih poruka
- Prijaviti sumnjive aktivnosti, e-poruke, pozive i zahtjeve
- Paziti na sigurnost web stranice kojoj pristupate i upisujete osjetljive podatke (https://, lokot)
- Informacije o poslovanju dijeliti samo ovlaštenim osobama
- Ne komunicirati s nepoznatim, sumnjivim ili neprovjerenim e-adresama
- Ne posjećivati sumnjive stranice i učitavati neprovjerene sadržaje
- Svjesno djelovati kao dio cjeline u kojoj svojim ponašanjem doprinosite sigurnosti

Praktični savjeti

Kako obavljati svoje zadatke ispravno i kako doprinijeti sigurnosti i zaštiti organizacije?

Zaštita vlastitog identiteta

- Korisnička imena i lozinke štite od neovlaštenih pristupa sustavima i osiguravaju pristup samo ovlaštenim osobama
- Upravljanje lozinkama – složene lozinke i različite za različite servise

Oprezno korištenje e-poruka i interneta

- Posjećivanje sigurnih web sjedišta
- Provjera sigurnosti web sjedišta na https://www.circl.lu/urlabuse/
- Povjerljivost e-poruka
- Onemogućiti automatsko preuzimanje datoteka u pregledniku i mail klijentu
- Onemogućiti medijski sadržaj e-pošte
- Ako koristite Wi-Fi bežično spajanje spajajte se samo na poznate uređaje i provjerene mreže

Briga o digitalnom tragu i oprezno s objavljivanjem sadržaja na društvenim stranicama posebno sadržaja poslovne naravi

Briga o opremi i uređajima:

- Vaš uređaj nikada ne smije ostati bez vašeg prisustva i mora biti zaštićen lozinkom ili PIN-om
- Spajajte svoje uređaje samo na provjerene uređaje za pohranu podataka ili za prijenos podataka

- Ista pravila koristite za privatne uređaje kao i za uređaje koje koristite u poslovne svrhe
- Redovito radite sigurnosne kopije poslovno vezanih informacija koristeći mrežne uređaje
- Ne nosite uređaje koji sadrže informacije o tvrtki sa sobom ako ih ne trebate
- Sigurnosne postavke na svim poslovnim uređajima

Zaštita na radu od kuće[5]

Kibernetička zaštita kao i praktični savjeti vrijede i u slučajevima kada radimo od kuće ili iz udaljene lokacije spajamo se na resurse ili koristimo resurse ustanove. Kao zaposlenik svijest o komunikaciji putem elektroničke pošte i dalje treba biti na visokoj razini te treba znati kako postupiti u slučaju zaprimanja sumnjivih poruka koje sadrže zahtjev za hitnom akcijom, stvaraju pritisak ili izazivaju strah.

U situacijama kada radimo od kuće ili udaljeno mogući su zahtjevi kolega za zaobilaženjem sigurnosnih procedura i takvu praksu nikako ne biste trebali dopustiti ili podržati.

Za spajanje na resurse ustanove važno je imati pristup na zaštićenu privatnu mrežu putem VPN spajanja. Osim toga važno je da pri korištenju kućne mreže imamo vlastitu lozinku (ne onu tvorničku koja je došla kao naljepnica na routeru). Na vašu kućnu mrežu omogućite pristup samo osobama od povjerenja i čuvajte pristupne podatke.

Važno je redovito izvršavati ažuriranja, nadogradnje i zakrpe na uređajima, aplikacijama, sustavima i antivirusnim programima koje koristimo.

Poslovni bi uređaji trebali biti posebno zaštićeni od nenamjernog oštećivanja uređaja ili podataka od strane ukućana – djece, gostiju, kućnih ljubimaca.

Budite svjesni svoga okruženja

Kao pojedinac jačajte svoju percepciju i situacijsku svjesnost na načine:

- provjerite je li osoba koja zahtijeva pristup ograničenim informacijama ovlaštena za dobivanje tih informacija
- tiskajte i kopirajte dokumente ili podatke samo kada je to zbilja potrebno jer stvaranjem kopija ili fizičkih dokumenata povećavamo rizik njihove zloupotrebe ako se s njima nepravilno barata
- kada trebate raditi u suradnji s kolegama na nekom dokumentu preporučujemo korištenje poveznice na dokument kako bi se vidjele sve izmjene i postojao trag o pristupu i izmjenama na dokumentu
- u poslovnom okruženju trebamo osvijestiti prisutnost i interese okoline u kojoj se nalazimo jer mogu u našoj blizini postojati ljudi koji prikupljaju informacije, gledaju preko ramena, prisluškuju

[5] https://www.cert.hr/ROKCERT ; https://www.cert.hr/europski-mjesec-kiberneticke-sigurnosti-2021/

- ne bismo trebali koristiti javna računala za rad s poslovnim dokumentima, povjerljivim informacijama ili pristupati poslovnim resursima
- trebamo biti svjesni ljudi koji ulaze u zaštićene administrativne prostore bez određenog povoda ili razloga
- svaku sumnjivu aktivnost trebamo provjeriti i prijaviti nadležnim osobama ili službama te postupati po procedurama koje su navedene u sigurnosnoj politici

Odgovornosti i uloge moraju biti jasno definirane unutar organizacije. Prilikom raspoređivanja uloga i odgovornosti vezano uz informacijsku sigurnost važno je voditi računa o segregaciji (razdvajanju) dužnosti.

Preporuka je odrediti povjerenstvo (članovi uprave i ostali ključni dionici) koje će biti zaduženo za praćenje stanja sigurnosti informacijskih sustava ustanove, donošenje odluka o provedbi mjera sigurnosti kojima je cilj unaprjeđenje sigurnosti.

Zaposlenici, studenti i suradnici važni su dionici uspješnog provođenja sustava informacijske sigurnosti zato je nužno da su i oni upoznati s politikom i procedurama koje su vezane uz njihovu radnu ulogu.

4. OSNOVE KIBERNETIČKE ZAŠTITE ZA USTANOVE

Regulativa u području kibernetičke sigurnosti

Zakon i Uredba o kibernetičkoj sigurnosti

Cilj je navedenog Zakona osigurati djelotvornu provedbu postupaka i mjera za postizanje visoke razine kibernetičke sigurnosti.

Zakonom se uspostavlja novi sustav upravljanja kibernetičkom sigurnošću u Hrvatskoj. Reorganizirane su dosadašnje nadležnosti u području kibernetičke sigurnosti te se u Sigurnosno-obavještajnoj agenciji ustrojava Nacionalni centar za kibernetičku sigurnost.

Zakon o kibernetičkoj sigurnosti sadrži odredbe o procesima, tijelima u sustavu i ljudima:

- procesima
- postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti
- revizija, samoprocjena, nadzor i prekršajna odgovornost
- tijelima u sustavu
- prava, obveze i nadležnosti tijela obuhvaćenih sustavom kibernetičke sigurnosti
- ljudima
- prava i obveze te odgovornosti pravnih subjekata na koje se zakon primjenjuje

Ako je ustanova obveznik primjene ili odluči dobrovoljno primjenjivati odredbe Zakona[6] i Uredbe[7] o kibernetičkoj sigurnosti tada treba imati uspostavljenu politiku

[6] https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html
[7] https://narodne-novine.nn.hr/clanci/sluzbeni/2024_11_135_2217.html

sigurnosti informacijskih sustava koja je jedna od mjera upravljanja kibernetičkim sigurnosnim rizicima.

Ostale su mjere: politika analize rizika, postupanje s incidentima, kontinuitet poslovanja, sigurnost lanca opskrbe, sigurnost u nabavi, politike procjene djelotvornosti mjere, osnove kibernetičke higijene, politike kriptografije, politike kontrole pristupa, politika lozinki.

Pravila i mjere

Mjere informacijske sigurnosti opća su pravila koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Zakon o kibernetičkoj sigurnosti kaže da je ..“cilj primjene mjera upravljanja kibernetičkim sigurnosnim rizicima zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata, uzimajući pritom u obzir sve opasnosti kojima su ti sustavi izloženi.“

Mjere su:

- tehničke mjere – uključuju kontrolu pristupa, kriptografiju, sigurnost mreže, redovito ažuriranje sustava i instaliranje zakrpa
- organizacijske mjere – uključuju politike sigurnosti, edukaciju zaposlenika, plan reakcije na incidente
- operativne mjere – uključuju praćenje, backup, sigurnost lanca opskrbe
- preventivne mjere – uključuju procjenu rizika, redovite provjere, simulacije napada
- mjere za oporavak – uključuju kontinuitet poslovanja, oporavak od katastrofe.

Za uključivanje određenih mjera u sigurnosnu politiku važno je pratiti odgovarajući propis ili odabrani standard, što znači pridržavati se pravila, smjernica ili zahtjeva propisanih tim zakonom ili standardom.

Proces upravljanja incidentom

Procesom upravljanja incidentom utvrđuju se postupci za brz i učinkovit odgovor na incidente. Za učinkovito upravljanje incidentima važno je:

- utvrditi način prijave incidenata (odrediti kanale prijave)
- propisati proceduru prijave incidenta
    - način prijave
    - obradu incidenta
    - analizu obrade incidenta.

Ciljevi upravljanja incidentima:

- minimizirati nepovoljne učinke na informacijski sustav ustanove
- uspostaviti normalan rad usluga u najkraćem mogućem roku
- osigurati/propisati da svi incidenti budu obrađeni
- smanjiti broj incidenata.

Incidenti se trebaju prijaviti putem odgovarajućih kanala što je prije moguće, sukladno propisanoj proceduri o prijavi incidenata. Procedura mora uključivati identifikaciju i obradu incidenta.

Obrada incidenta podrazumijeva prikupljanje svih relevantnih podataka za rješavanje incidenta, analizu prikupljenih podataka, smanjenje utjecaja ugroze na informacijski sustav ili njeno uklanjanje iz sustava i uspostavu stanja sustava sukladnog odredbama sigurnosne politike. Odgovaranje na incidente treba provoditi sukladno propisanoj proceduri. Potrebno je ukloniti ranjivosti koje su dovele do incidenta.

Na temelju provedene analize incidenta potrebno je izraditi sažetak obrade incidenta. Na temelju dobivenih saznanja može se predložiti propisivanje sankcija. Učenje stečeno analizom i rješavanjem incidenata treba iskoristiti za smanjenje vjerojatnosti ili utjecaja budućih incidenata.

Edukacija svih korisnika ustanove prilagođena pojedinim grupama korisnika provodi se o temama informacijske sigurnosti izravno povezanim s poslom koje pojedine grupe korisnika obavljaju, sukladno planu edukacija te se na taj način preventivno utječe na smanjenje mogućih incidenata. [8]

Edukacija i podizanje svijesti

Radi smanjivanja rizika ljudske pogreške prilikom korištenja informacijske imovine, potrebno je na odgovarajući način utvrditi odgovornosti vezane uz informacijsku sigurnost u radnoj okolini i osigurati da zaposlenici, vanjski suradnici i treće osobe razumiju svoje odgovornosti. Budući da su svi odgovorni za zaštitu informacija koje se koriste u bilo kojem obliku od neovlaštenog pristupa i korištenja na ustanovi, važno je da svi razumiju svoje odgovornosti sukladno svojoj ulozi i da se redovito educiraju temeljem prethodno utvrđenog plana edukacije.

Radi podizanja svijesti korisnika potrebno je na primjer osigurati potpisivanje izjave o upoznavanju s obvezama prije početka suradnje (prilikom testiranja kandidata, početka suradnje s dobavljačima). Tijekom zaposlenja/angažmana osigurati da svi primjenjuju informacijsku sigurnost u skladu s uspostavljenim politikama i procedurama. U slučaju opetovanog kršenja pravila informacijske sigurnosti, oduzeti prava pristupa i poduzeti radnje sukladno zakonskim propisima i internim pravilnicima ustanove. Zaposlenici koji imaju ulogu voditelja/rukovoditelja trebaju voditi računa da, zaposlenici koje vode i treće osobe s kojima surađuju, poštuju pravila sigurnosne politike.

[8] Nadležni CSIRT za visoka učilišta koja će biti kategorizirana kao obveznik primjene Zakona o kibernetičkoj sigurnosti u sektoru Sustav obrazovanja ili u sektoru Istraživanja je Nacionalni CERT. U tom slučaju se incidenti prijavljuju u PiXi platformu (nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima). U ostalim slučajevima nadležni CSIRT je isto Nacionalni CERT, ali se incident prijavljuje na e-mail *incident@cert.hr* prema uputama na interneta stranici *https://www.cert.hr/oincprijavi/*.

Plan revizija i ažuriranje sigurnosne politike

Cilj je sukladnosti sa zakonskim i ugovornim zahtjevima izbjegavanje kršenja zakonskih, statutarnih i ugovornih obveza povezanih s informacijskom sigurnosti i kršenje bilo kojih sigurnosnih zahtjeva.

Nužno je:

- Identificirati zakonske i ugovorne zahtjeve – navedeni zahtjevi trebaju biti definirani, dokumentirani i ažurirani
- Implementirati procedure za osiguravanje sukladnosti sa zakonskim i ugovornim zahtjevima povezanim s pravima intelektualnog vlasništva (autorska prava, pravo na kopiranje, pravo na dizajn, licenčni ugovori za softver i slično).

Zato je potrebno:

- provoditi procese provjere usklađenosti provedenih mjera i propisanih zahtjeva
- donijeti plan revizije i ažuriranja politike
- izvršavati sve u propisanim intervalima
- sastavljati izvještaje o usklađenosti

Sve politike i procedure primjenjuju na način da se izvrše mjere i zahtjevi jednom godišnje ili nakon što se dogodi značajna promjena. Potrebno je i redovito pratiti propise, standarde i organizacijske i poslovne promjene u ustanovi i sukladno njima uskladiti politiku.

Procese usklađivanja kojima se utvrđuje usklađenost provedenih mjera i propisanih zahtjeva potrebno je provoditi u intervalima kako je to propisano ili zakonom ili internim pravilima.

Savjeti za ustanove

- donijeti i provoditi sigurnosnu politiku
- redovito revidirati i procjenjivati kibernetičku sigurnost ustanove
- osigurati infrastrukturu koja odgovara zahtjevima poslovanja
- upoznati zaposlenike i druge korisnike sa sadržajem sigurnosne politike, pravilima i procedurama
- upoznati zaposlenike i korisnike s rizicima nepravilnog i neodgovornog korištenja podacima i opremom tvrtke
- organizirati redovite edukacije zaposlenika i korisnika
- popisati svoju imovinu, osvijestiti ključne ili kritične podatke, sustave ili usluge i ulagati u njihovu zaštitu
- upoznati se i pratiti potencijalne kibernetičke prijetnje
- postaviti kibernetičku zaštitu kao integralni dio poslovne strategije
- ulagati u kibernetičku otpornost ustanove.

Važnost prijavljivanja kibernetičkih incidenata

Kibernetičke prijetnje i incidenti trebaju se odmah prijaviti internim ili drugim nadležnim službama ovisno o proceduri koju ustanova ima propisanu i koja se primjenjuje u ustanovi.

Prijava se radi zato što može spriječiti nastanak incidenta (u slučaju prijave prijetnje), smanjiti štetu i zaustaviti širenje.

Incident se može prijaviti Nacionalnom CERT-u Sektoru pri Hrvatskoj akademskoj i istraživačkoj mreži – CARNET na e-adresu: *incident@cert.hr*

Prijava mora sadržavati:

1. Izvorne log datoteke s vremenskom oznakom i zonom
2. Opis incidenta
3. Izvornu IP adresu (napadača)
4. Odredišnu IP adresu (žrtve)
5. Zaglavlja e-mail poruke i/ili URL.

Potrebno je navesti datum i točno vrijeme (uz vremensku zonu) kada se incident dogodio (kod e-mail poruka se vrijeme već nalazi u zaglavljima).

Prijava treba sadržavati opis incidenta u kojem je potrebno ukratko opisati sve informacije relevantne za incident.

Ako prijavljujete zlonamjernu elektroničku poštu, potrebno je poslati cijelu poruku kao privitak ili izvući njena zaglavlja[9]. Zaglavlje je zapis kojeg sadrži svaka poruka e-pošte, a u tom se zapisu nalaze podaci o pošiljatelju, primatelju, informacije o poslužiteljima preko kojih je poruka poslana.

Kada je riječ o napadima na infrastrukturu ili potencijalno zaraženim sustavima potrebno je poslati dnevničke zapise kako bi se iz njihove analize dobio detaljniji uvid u incident.

Također je potrebno navesti IP adrese koje su sudjelovale u napadu (izvori i mete)

Ako je riječ o zlonamjernim URL-ovima, onda je naravno potrebno poslati cijele URL-ove. Mogu se poslati slike zaslona i ostale informacije za koje mislite da mogu pomoći u obradi incidenta.

Ako se prijava odnosi na ransomware, potrebno je priložiti ransom note i jednu kriptiranu datoteku kako bi se moglo provjeriti postoji li dekriptor.

Prijava incidenta drugim službama

Potencijalna kaznena djela potrebno prijaviti policiji na *policija@mup.hr* ili odlaskom u najbližu policijsku postaju.

---

[9] *https://www.cert.hr/kakoizvucizaglavlje/* i *https://www.youtube.com/playlist?list=PLmQTle2bBZfnkzIXoQCJQNe037S9Il8qq*

Nacionalni CERT nema ovlasti kažnjavanja problematičnih korisnika niti pokretanja kaznenih prijava.

5. PRAKTIČNA VJEŽBA – Istraživanje profila na društvenim mrežama

Ovisno o broju sudionika radionice može se odrediti kao individualna ili grupna praktična vježba. Istražuju se javno dostupne informacije o izmišljenom liku Žiljcu prema kojima sudionici vježbe individualno ili grupno pripremaju phishing poruku koja bi bila upućena Žiljcu s ciljem ostvarivanja neke koristi: novčane, krađe podataka i ostvarivanja pristupa i dr.

Zadatak: Gdje je Žiljac? - https://www.facebook.com/zicjura54/?locale=hr_HR

Naš naivac Željko Jurić Žiljac ima vrlo osebujan profil na Facebook društvenoj mreži. Svakodnevno objavljuje mnoštvo informacija ni ne sumnjajući da bi ih netko mogao iskoristiti protiv njega.

Pronađi sljedeće informacije o našem Žiljcu:

- Mjesto stanovanja
- Datum rođenja
- Gdje i što radi
- Kako mu se zovu članovi obitelji
- Koji su mu interesi
- Koji je stupanj obrazovanja završio
- Bonus bodovi ☺
    - Lozinka
    - Ime udruge kojoj pripada
    - Adresa vikendice

- Osmislite jednu phishing poruku elektroničke pošte na koju bi naš Žiljac sigurno nasjeo
- Vrijeme rješavanja: 20 minuta

6. ZAKLJUČAK I PREPORUKE

Kibernetička zaštita ustanove kreće od njene uprave, zaposlenika, korisnika, suradnika i studenata.

Svaki pojedinac ima svoju ulogu u kibernetičkoj zaštiti ustanove i njenih resursa i njegova osnovna zaštita kreće od pridržavanja pravila kibernetičke higijene i postupanja prema sigurnosnoj politici ustanove, pravilima i procedurama.

Ustanova mora osigurati osnovnu kibernetičku zaštitu prema mjerama zaštite resursa, podataka i ugleda ustanove te provoditi programe edukacije o kibernetičkoj sigurnosti za sve zaposlenike.

Mnogi korisnici nisu svjesni važnosti informacijske sigurnosti. To se prevladava organizacijom edukativnih programa, radionica i dijeljenjem jasnih smjernica.

Impressum

Nakladnik: Hrvatska akademska i istraživačka mreža – CARNET

Projekt: e-Sveučilišta: Projekt digitalne preobrazbe visokog obrazovanja

Autorica: Marina Dimić Vugec

Zagreb, svibanj 2025.

Ovaj Priručnik možete citirati ovako:

Dimić Vugec, M. (2025). Osnovne kibernetičke zaštite i prepoznavanje kibernetičkih prijetnji - Priručnik. Preuzeto s [poveznica na sadržaj na edutoriju] [datum pristupa]

Kontakt

Hrvatska akademska i istraživačka mreža – CARNET

Josipa Marohnića 5, 10000 Zagreb

tel.: +385 1 6661 555

www.carnet.hr