Uvod u bezbednost informacionih sistema

Predmet: Zaštita podataka u komunikacionim mrežama

Predavač: dr Dušan Stefanović

Kome je namenjen predmet zaštita podataka u komunikacionim mrežama?

Administratori Sistema

Programeri

Security Analist – Osobe koje žele da se usavrše na polju bezbednosti informacionih sistema

Šta ćete naučiti?

Na koji način se napadači ponašaju u stvarnom svetu

Koji aspekti treba da budu uključeni za kreiranje bezbednijih aplikacija i sistema

Na koji način detektovati zlonamerno (maliciozno) ponašanje

Sadržaj predmeta za I kolokvijum

0. Uvod u bezbednost informacionih sistema

1. Opšti pojmovi o sigurnosti, pretnje, napadi i metode zaštite

2. Procene rizika od napada i neovlašćenog pristupa

3. Osnovni kriptografski pojmovi i njihova primena

4. Kriptografija sa javnim ključevima, heš funkcije, digitalni potpisi i sertifikati

5. Sigurnosne arhitekture i protokoli, IPSec, SSL

Sadržaj predmeta za II kolokvijum

6. Sigurnosni protokoli - SSH, Kerberos, Radius

7. Kontrola pristupa i zaštita operativnog sistema

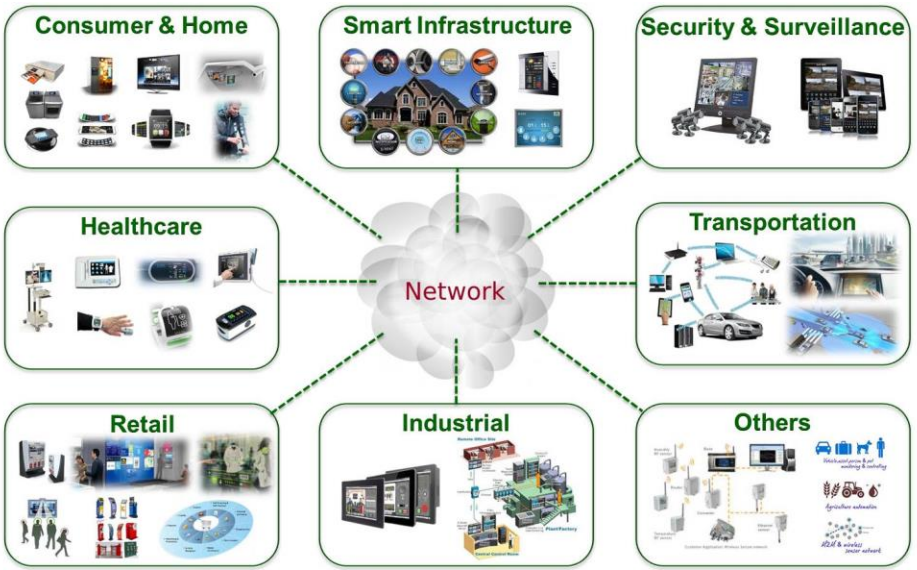
8. Sigurnost baza podataka i sigurnosni aspekti programiranja

9. Bezbednost elektronskog poslovanja i interneta

Informacioni i komunikacioni sistemi

Tip aplikacije koji je danas najzastupljeniji u svim kompanijama

Aplikacije za mobilne telefone i IoT uređaji koriste web komponente kroz web servise i interfejse koji su ugrađeni u njih



Potreba za testiranjem aplikacija

Web serveri i web aplikacije su atraktivne mete za napadače zbog velikog broja web sajtova na Internetu i organizacija koje svoje poslovanje obavljaju online.

Za interakciju sa web aplikacijom dovoljan je samo pretraživač (web browser)

Sajber kriminalci ostvaruju znatne finansijske dobitke eksploatisanjem web aplikacija I instaliranjem zlonamernih programa koji se prosleđuju korisnicima aplikacija

HTTP saobraćaj je dozvoljen od strane firewall-a, napadačima nisu potrebni posebni otvoreni portovi.

HTTP protokol nema ugrađene bezbednosne funkcije, ne obezbeđuje identifikaciju individualnih sesija što znači da je na programeru da ih dizajnira.

Bezbednost se uključuje u fazi projektovanja aplikacije.

Kasnije integrisanje bezbednosti je veoma teško i zahteva prilično prerade koda.

Potreba za zaštitiom od napada

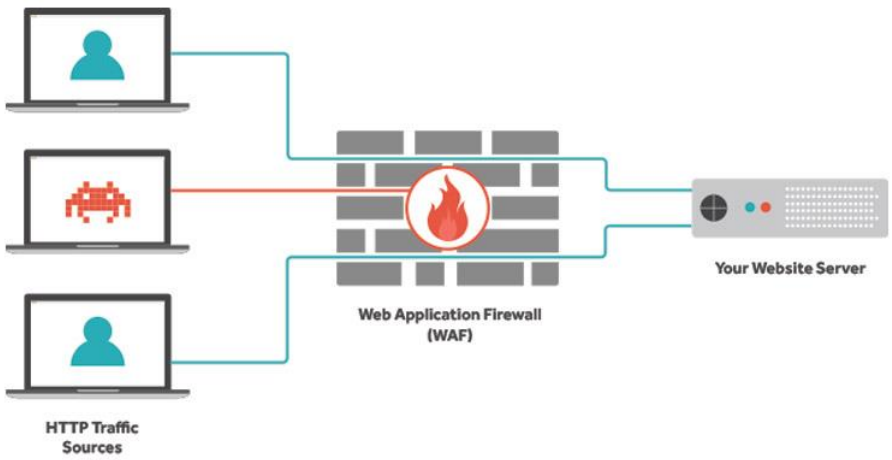
Zaštita podataka klijenata

Gubitak prihoda

Zaštita od prekida poslovanja

Gubitak reputacije

Usklađenost sa zakonima i propisima



Zašto je teško zaštiti računarski sistem

Kod koji sadrži greške u smislu bezbedonosnih propusta i koji se ne pridržava preporuka koje se odnose na bezbednost

Socijalni inženjering – prevarom do poverljivih informacija

- Novac može da se zaradi traženjem i eksplotacijom ranjivih aplikacija
- Market gde mogu da se nađu i kupe informacije o ranjivim aplikacijama
- Market za ukradene podatke i mašine koje su van kontrole vlasnika
- Postoji mnogo načina da se uzme profit od ukradenih podataka ili kompromitovanih mašina

Zašto se napada kompijuterski sistem

Spam

- Slanje sa legitimne IP adrese ima manju verovatnoću da sadržaj bude blokiran

DoS

- Napad na konkurente ili da se traži otkupnina

Inficiranje posetioca malware skriptom

- Jedan inficiran server može da inficira na stotine hiljada klijenata

Krađa podataka

- Krađa poverljivih podataka, brojeva kreditnih kartica, intelektualne svojine

Uvod u Cyber Bezbednost

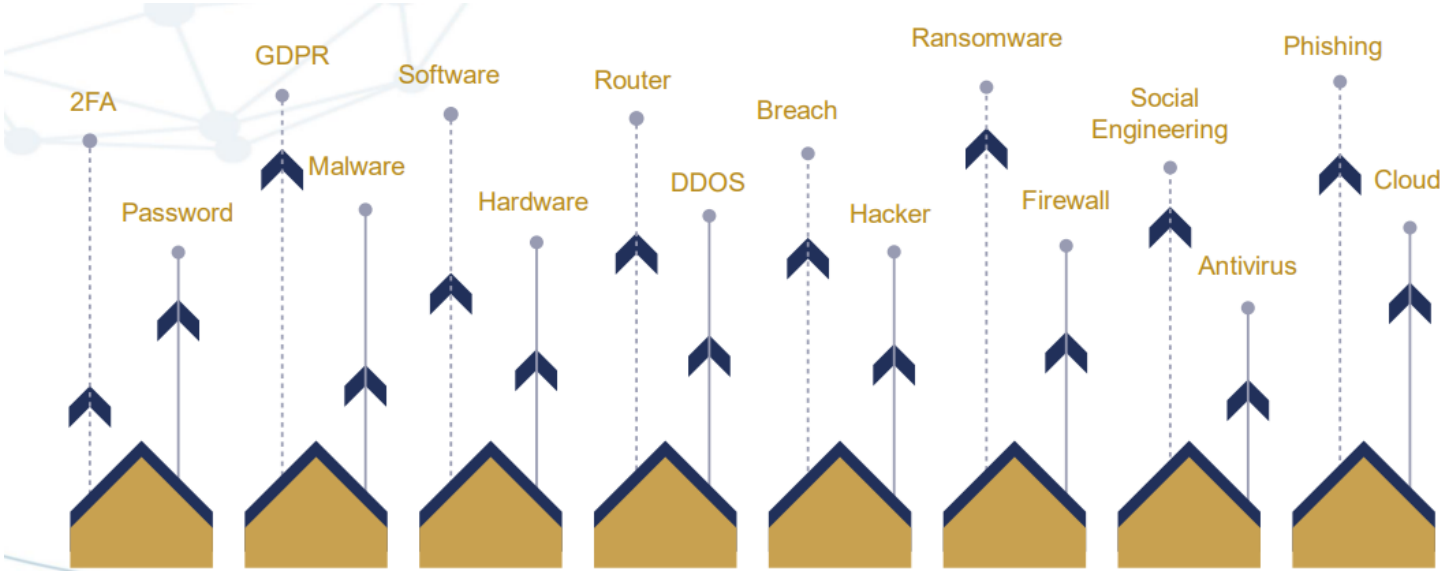
Syber Bezbednost

Sajber bezbednost je način na koji pojedinci i organizacije smanjuju rizik od sajber napada.

Osnovna funkcija sajber bezbednosti je da zaštitite :

1. Uređaje koje svi koristimo(pametni telefoni, laptopovi, tableti i računari)
2. Servise (usluge) kojima pristupamo na mreži i na poslu

od krađe, oštećenja ili nedostupnosti usluge



MIT ILI REALNOST

1. Sajber bezbednost je previše složena za razumevanje.
2. Sajber napadi su sofisticirani.Ne možemo ih zaustaviti.
3. Sajber napadi su visoko ciljani. Naša organizacija verovatno neće biti zanimljiva za napadača

MIT ILI REALNOST

4. Jaka lozinka je dovoljna da podaci budu bezbedni
5. Brisanjem fajlova je dovoljno da se neželjeni podatak trajno ukloni
6. Organizacijama i pojedincima nije potreban softver za enkripciju
7. Cyber Bezbednost je briga samo IT sektora

TRENUTNO STANJE
ŽRTVE CYBER SECURITY NAPADA

JBS Foods pays $14m to ransomware attackers

By Ry Crozier
Jun 10 2021
11:23AM

0 Comments

Says the decision to make payment was 'very difficult'.

JBS Foods, the meat processor whose Australian and US operations were hit by a ransomware attack earlier this month, paid "the equivalent of US$11 million" (A$14 million) to the group behind the attack.

The company made the payment despite the "vast majority of the company's facilities" already having been

Cyberattack Sees UniSA Systems Shut Down

BY ADMIN ON MAY 18, 2021
APP-ACSM, CYBER SECURITY, EDITOR'S DESK, FEATURED, GOVERNANCE, RISK & COMPLIANCE, HACKING & PENETRATION TESTING, INFORMATION SECURITY, VULNERABILITIES

A cyberattack at the University of South Australia is continuing to impact staff and students. The circumstances surrounding the attack remain unclear, but key systems are still offline two days after the University noticed the first outage.

"UniSA experienced a cyberattack on the weekend which caused an outage of its staff email system," a UniSA spokesperson told MySecurity Media. "The University is still investigating the issue."

Nine Network under attack by cyber hackers, threatening news services nationwide

By 9News Staff | 7:04am Mar 29, 2021

Tweet | Facebook | Mail

NEW ZEALAND / MEDIA & TECHNOLOGY

Waikato DHB cyber attack: Medical files may have been taken

5:46 pm on 24 May 2021

Share this

POLITICS

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

PUBLISHED TUE, JUN 8 2021·10:17 AM EDT | UPDATED WED, JUN 9 2021·8:24 AM EDT

NSW driver's licence data stolen in Accellion breach

By Justin Hendry
Feb 25 2022
6:30AM

4 Comments

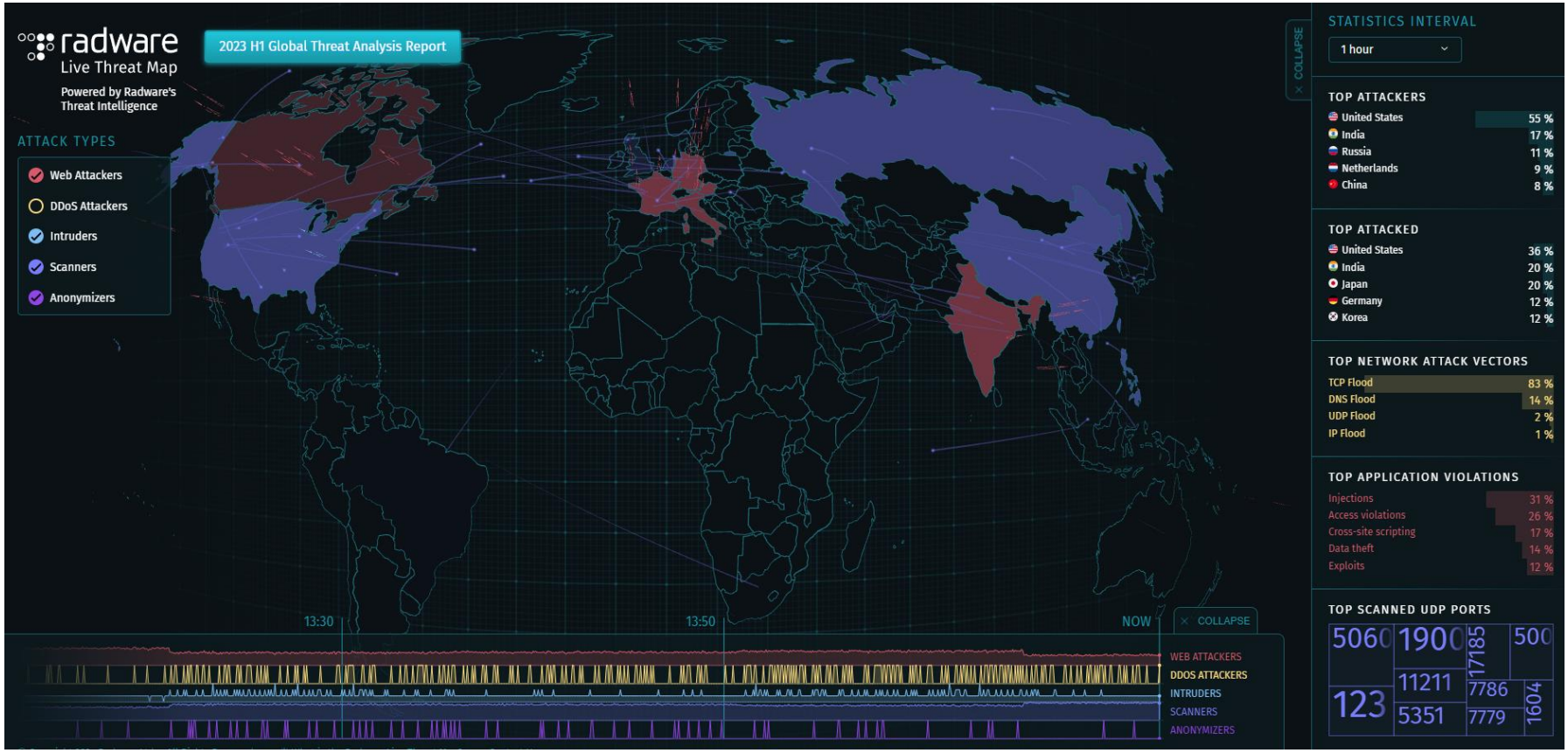
Some customers, agency staff only now being notified.

Driver's licence details were among the personal information stolen from Transport for NSW in the Accellion data breach last year, *iTnews* can reveal.

TRENUTNO STANJE

NAPADI I STATISTIKA NAPADA U REALNOM VREMENU

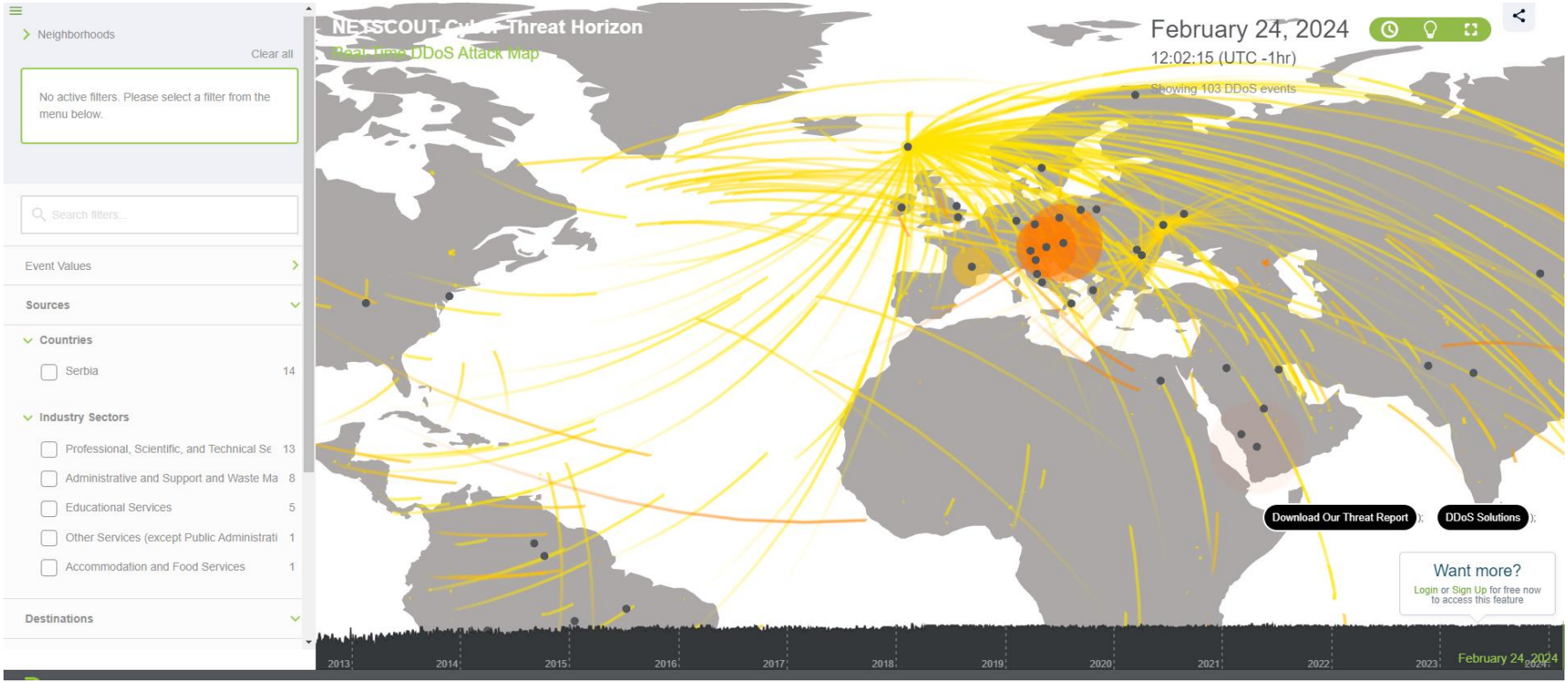
https://livethreatmap.radware.com/



TRENUTNO STANJE

DDOS NAPADI U REALNOM VREMENU

https://horizon.netscout.com/

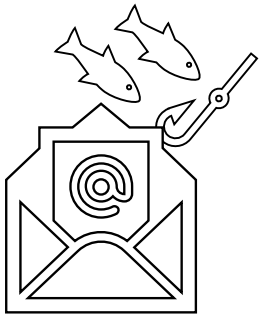


TRENUTNO STANJE

Kaspersky Cyber map

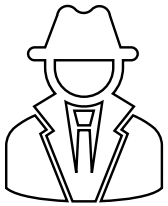
https://cybermap.kaspersky.com/

TRENUTNO STANJE



Phishing napad je i dalje napad broj 1

Ransomware napadi su u porastu



Social Engineering je vodeći napad za razne vrste prevara

VEKTORI NAPADA

Termin se odnosi na način ili put koji napadač koristi da bi izvršio napad na računarski sistem, mrežu ili aplikaciju.

Razlikuju se po vrsti napada i cilja a najdominatniji su:

Phishing

Napadači mogu koristiti phishing emailove ili poruke kako bi prevarili korisnike da otkriju svoje korisničko ime, lozinku ili druge osetljive informacije.

Ransomware

Ransomware je vrsta malicioznog softvera (malware-a) koji šifrira podatke na računaru ili mreži i zahteva otkup (ransom) od žrtve kako bi se dekriptovali podaci.

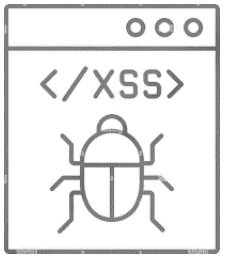
VEKTORI NAPADA

Brute Force

Napadači mogu koristiti brute force napade kako bi pokušali razbiti lozinke ili druge autentifikacione mehanizme pokušavanjem svih mogućih kombinacija sve dok ne pronađu ispravnu.

SQL Injection

Ovaj napad se koristi za ubacivanje zlonamernog SQL koda u SQL upite. To može omogućiti napadaču da izvršava neovlašćene operacije na bazi podataka, kao što su izvlačenje, menjanje ili brisanje podataka.



Cross-Site Scripting

XSS napadi se koriste za ubacivanje zlonamernog koda u web stranice ili aplikacije koje se zatim izvršavaju na uređajima korisnika koji pristupaju tim stranicama.
To može omogućiti napadaču da ukrade sesije korisnika

SCAM WATCH

Agencije usmerene ka otkrivanju, praćenju i sprečavanju različitih obmana i prevara u digitalnom svetu, kao i obaveštavanju javnosti o njima kako bi se smanjio njihov uticaj i zaštitile potencijalne žrtve.

SCAM WATCH IZVEŠTAJ ZA 2020

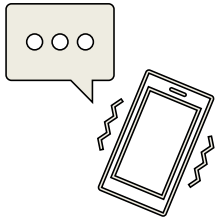
PHISHING NAPADI

Phishing email

COVID 19 vakcine

Vishing (Voice Phishing)

Lažno predstavljanje da je potrebno da se očisti virus na vašem računaru



Smishing (SMS Phishing)

Lažna poruka da vam račun ne bi bio blokiran traži se da kliknete na link

Department of Health impersonation email

Australian Government
Department of Health

Dear Recipient,

My colleague have contacted you earlier but there was no response from you.

There were three COVID-19 confirmed cases in your area earlier this week and one of the patients has listed you as one of her physical contacts within the last 14 days.

In line with the contact tracing modalities and within the laws on which we operate at the Department of Health, we strongly advice that you submit yourself for COVID-19 testing.

The neccessary details of your appointment with the Department of Health are contained in the attached document.

Read through the guidelines properly and ensure that you submit yourself for testing as failure to do so will result in arrest and prosecution.

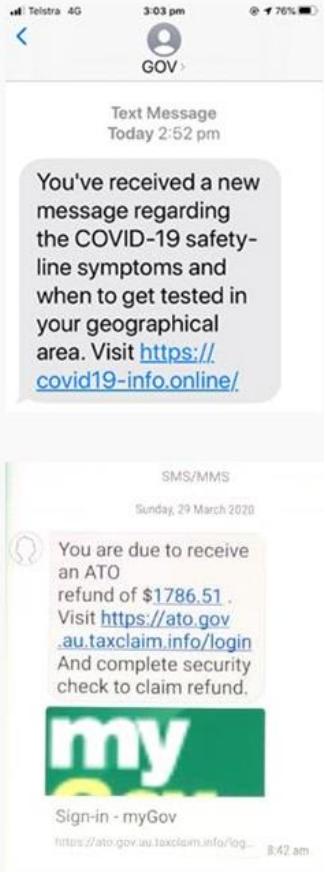
If you have any questions concerning this email, feel free to contact me anytime.

Regards.

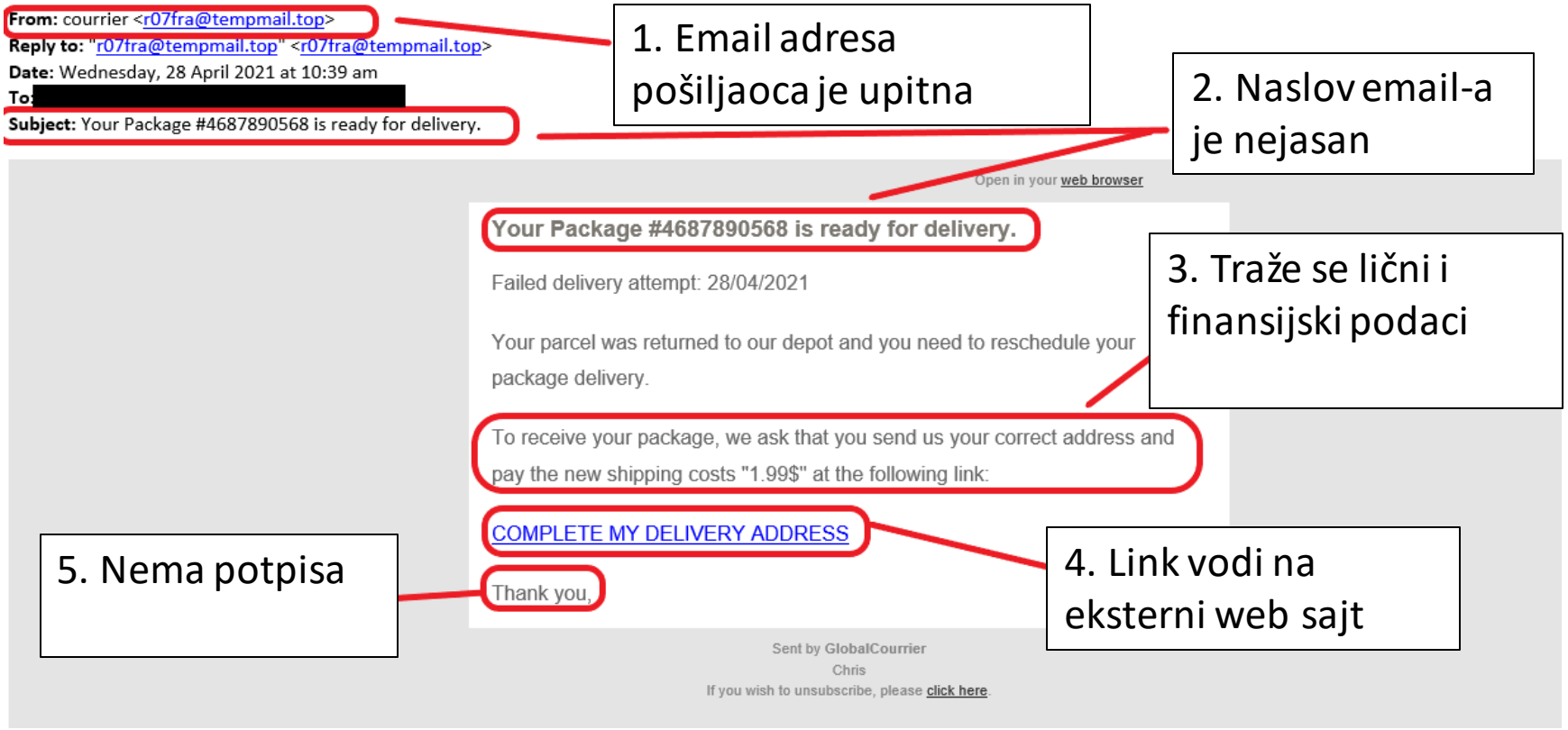
Greg Hunt MP

Department of Health
GPO Box 9848
Canberra ACT 2601
Australia

Fake myGov texts



PRIMER ZA PHISHING NAPAD



RANSOMWARE

Ransomware je vrsta malicioznog softvera (malware-a) koji šifrira podatke na računaru ili mreži i zahteva otkup (ransom) od žrtve kako bi se dešifrirali podaci.

Kako?

Email attachments

Website downloads

Email links

Website links

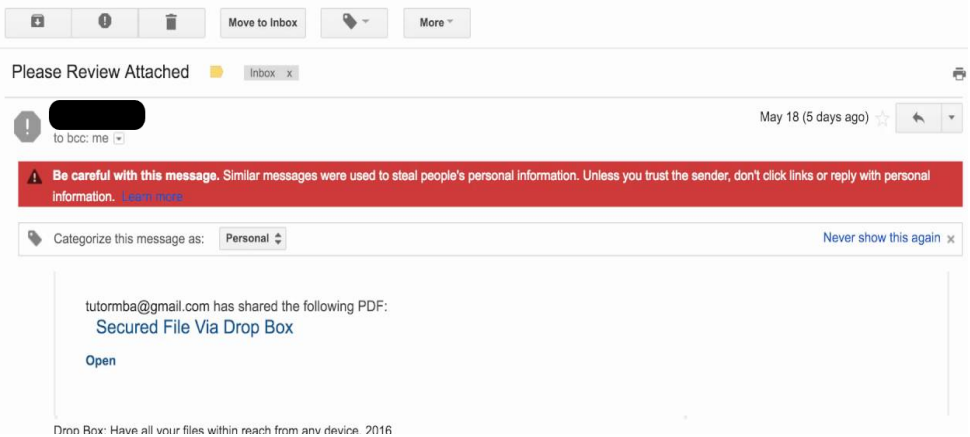
Zaštita

Redovni backup

Updates

Verifikacija email-ova

Ne PLAĆAJ!

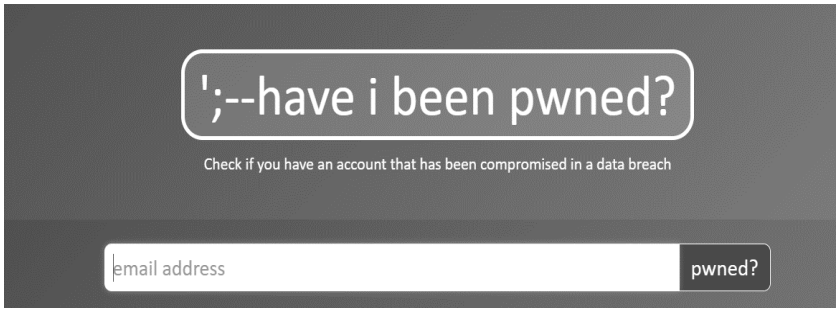


ZAŠTO JE SVEST O SAJBER BEZBEDNOSTI BITNA?

- Sve je UMREŽENO!
- Lični dokumenti
- Identitet
- Finansije
- Digitalni footprint (otisak).

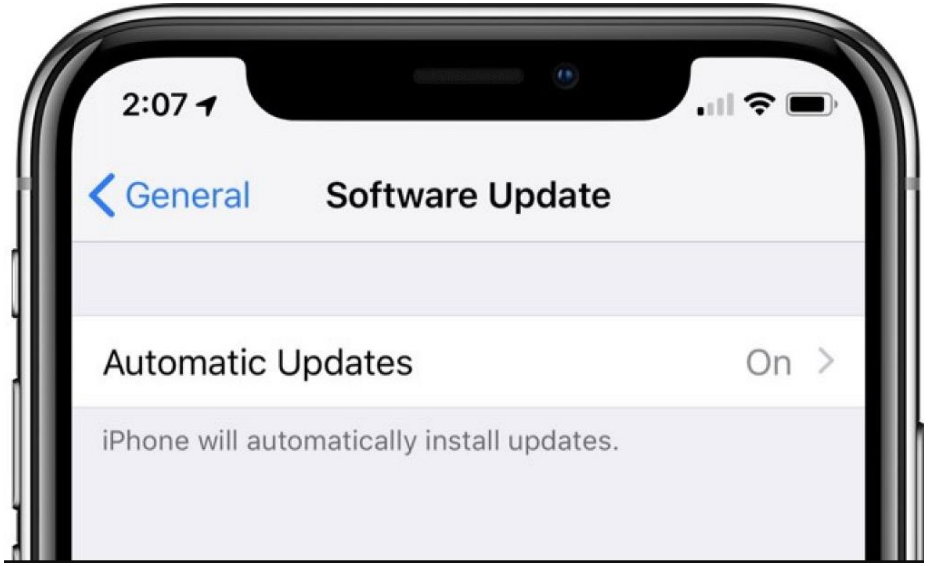
LOZINKE

- Duga i jaka.
- Omogućiti 2FA uvek kad je moguće
- Promena default lozinke
- Ne koristiti istu lozinku na različitim nalozima
- **Koristi Password manager (LastPass je Besplatan)**



UPDATES

- Obezbediti da svi uređaji imaju najnoviji update
- Uključiti AUTOMATIC UPDATES
- Odvoji vreže za update
- Redovno čistiti aplikacije



OPREZNOST OD PREVARA

1. Phishing - email
2. Vishing – telefonski pozivi
3. Smishing – SMS poruke

Obratiti pažnju na:

1. Hitnost
2. Traženje ličnih/finansijskih informacija
3. Sadrži link i (downloadable) fajl
4. Gramatičke greške
5. Isuviše dobro da bi bilo istinito

DIGITALNI POTPIS

Digitalni trag koji ostavljamo dok koristimo internet ili digitalne tehnologije.

Uključuje sve što ostavljamo iza sebe dok pretražujemo internet, koristimo društvene mreže, šaljemo e-mailove, kupujemo online ili koristimo mobilne aplikacije.

Kontrola privatnosti

Budite mudri šta delite

Pregledati app privacy kolekciju

CYBER SECURITY CHECK LISTA

Da li su moji uređaji bezbedni?

Koristi *VPN* za pristup udaljenim resursima?

Budi oprezan korišćenjem *FREE Wi-Fi*

Da li je instaliran antivirus?

Da li imam back up bitnih podataka? *Cloud & Lokal*

Da li su uređaji up to date?

Omogući *two-factor* authentifikaciju *(2FA)* gde je moguće

STOP.

THINK BEFORE YOU CLICK.

SYBER BEZBEDNOST - ODGOVORNOST

Skoro sve organizacije zavise od digitalne tehnologije da bi funkcionisale.

Potencijalni trošak otklanjanja sajber incidenta može biti značajan.

Rizik od gubitka reputacije.

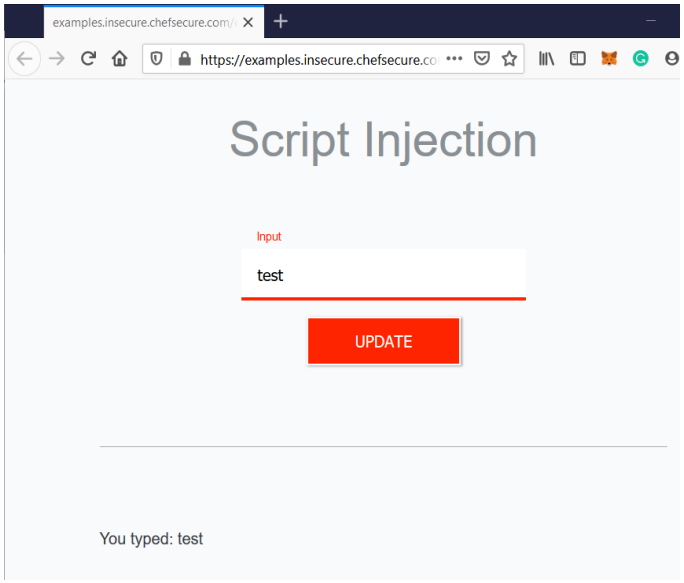
Sajber bezbednost je od suštinskog značaja i treba je shvatiti kao naizbežan faktor.

PRIMER SIMULACIJE
CROSS SITE SCRIPTING NAPADA

Test sajt:

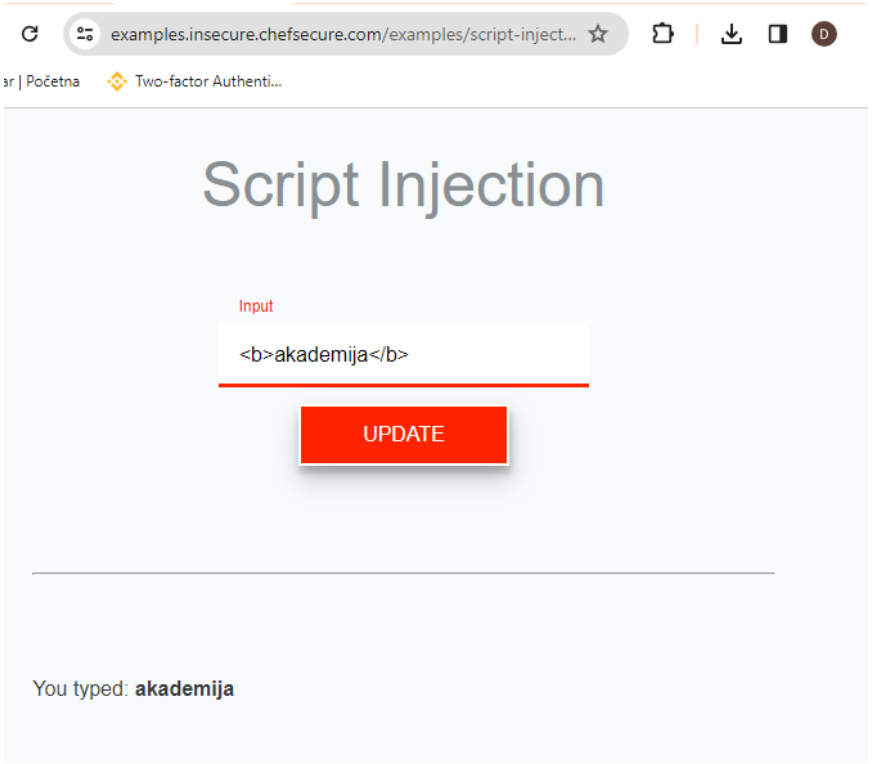
https://examples.insecure.chefsecure.com/examples/script-injection

Otvoriti web stranicu i uneti proizvoljan tekst a zatim kliknuti na update.



PRIMER SIMULACIJE
CROSS SITE SCRIPTING NAPADA

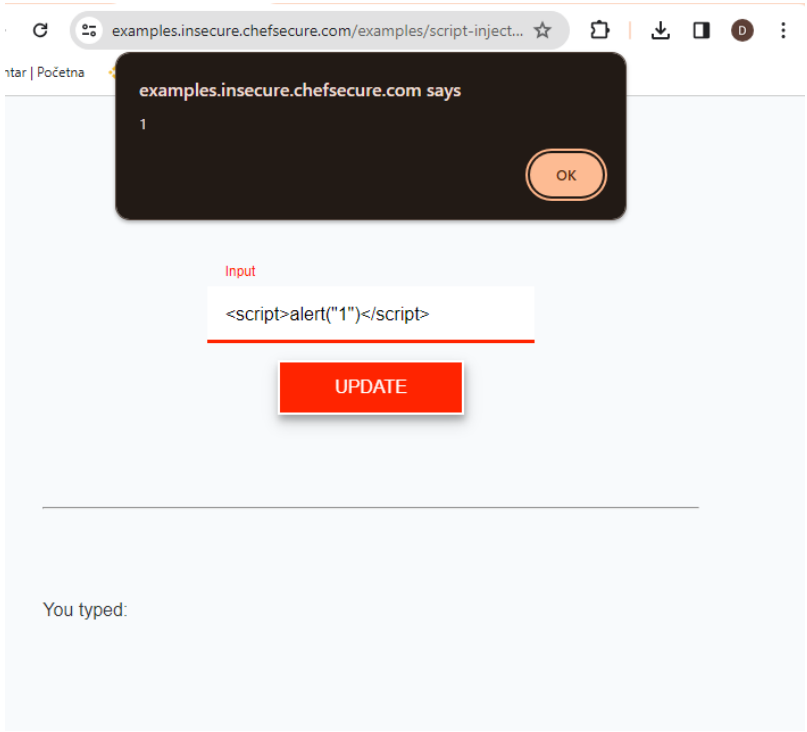
Forma dozvoljava izvršavanje HTML koda.



PRIMER SIMULACIJE

CROSS SITE SCRIPTING NAPADA

Forma dozvoljava izvršavanje Java script koda.



PRIMER SIMULACIJE
CROSS SITE SCRIPTING NAPADA

Forma dozvoljava izvršavanje Java script koda koji čisti web stranu

<script>document.documentElement.innerHTML=“”</script>

```
<html>
<head>
  <meta charset="utf-8">
  <meta name="robots" content="noindex">
  <meta name="domain" content="chefsecure.com">
  <link rel="stylesheet" media="screen" href="https://examples.insecure.chefsecure.com/assets/insecu
  <script src="https://examples.insecure.chefsecure.com/assets/insecure/examples_init-68be104777c4cf
</head>
<body>
  <h1 class="title">Script&#x20;Injection</h1>
  <div class="styled-input">
  <input id="input" type="text" required>
  <label>Input</label>
  <span></span>
</div>
<div class="btn-wrap">
  <button id="update">Update</button>
</div>
<hr>
<p>You typed: <span id="value"></span></p>
<script>
  /* Mimic a server response since innerHTML won't run scripts.
   * code from https://stackoverflow.com/a/20584396 */
  function nodeScriptReplace(node) {
    if ( nodeScriptIs(node) === true ) {
      node.parentNode.replaceChild( nodeScriptClone(node) , node );
    }
    else {
      var i = 0;
      var children = node.childNodes;
      while ( i < children.length ) {
        nodeScriptReplace( children[i++] );
      }
    }

    return node;
  }
  function nodeScriptIs(node) {
    return node.tagName === 'SCRIPT';
  }
  function nodeScriptClone(node){
    var script  = document.createElement("script");
    script.text = node.innerHTML;
    for( var i = node.attributes.length-1; i >= 0; i-- ) {
      script.setAttribute( node.attributes[i].name, node.attributes[i].value );
    }
    return script;
  }
  function inputUpdated() {
    let value = document.getElementById('value')

    value.innerHTML = document.getElementById('input').value
    nodeScriptReplace(value)
    sendHeight()
  }

  document.getElementById('update').addEventListener('click', inputUpdated)
</script>

</body>
```