ZKS (NIS2) AWARENESS

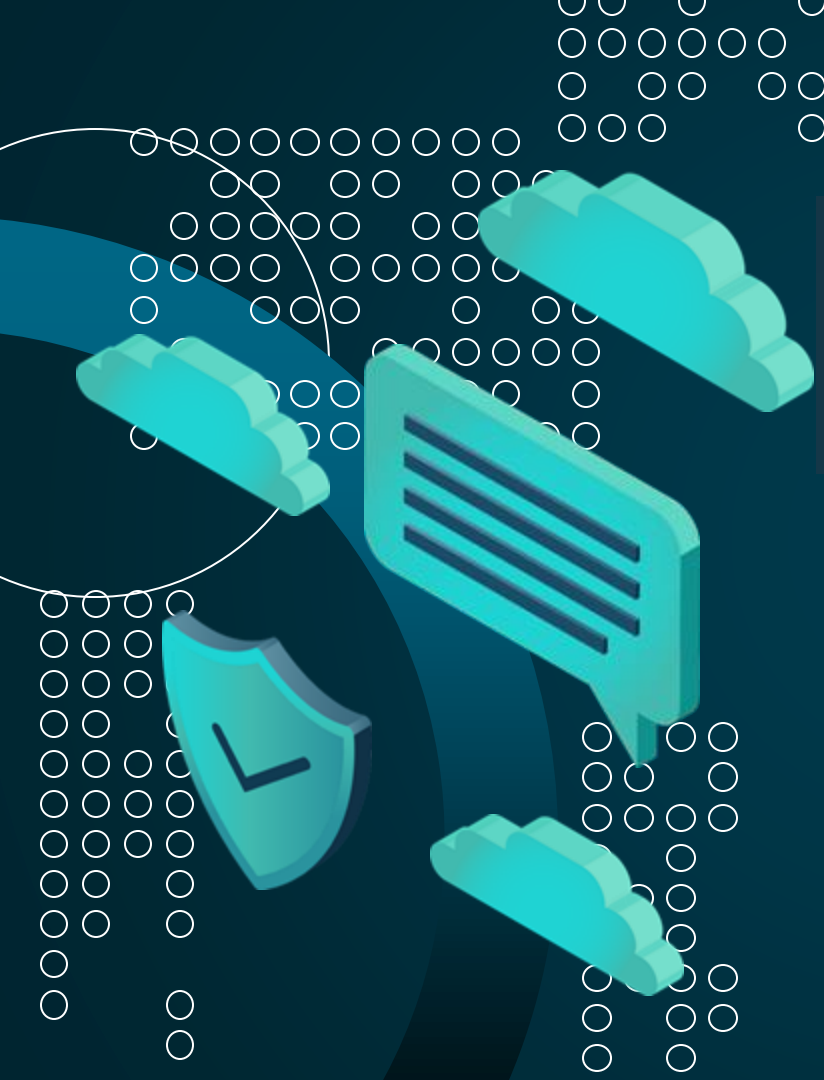
Edukacija o
Zakonu o kibernetičkoj sigurnosti

Daniel Bara

O predavaču

Daniel Bara, CISO
daniel@adventurespirit.hr

Sadržaj



It takes 20 years to build a reputation and five minutes to ruin it.

Warren Buffet

Flights canceled after IT outage grounds Alaska Airlines grounds flights nationwide

It's the second time this year an IT outage has grounded the airline's flights.

By Ayesha Ali
October 24, 2025, 4:55 AM

Alaska Airlines flight turns around due to severe turbulence Alaska Airlines Flight 309 made an emergency landing at Los Angeles International Airport after reporting an issue with one of its landing gears.

JLR hack is costliest cyber attack in UK history, say analysts

2 days ago

Share Save

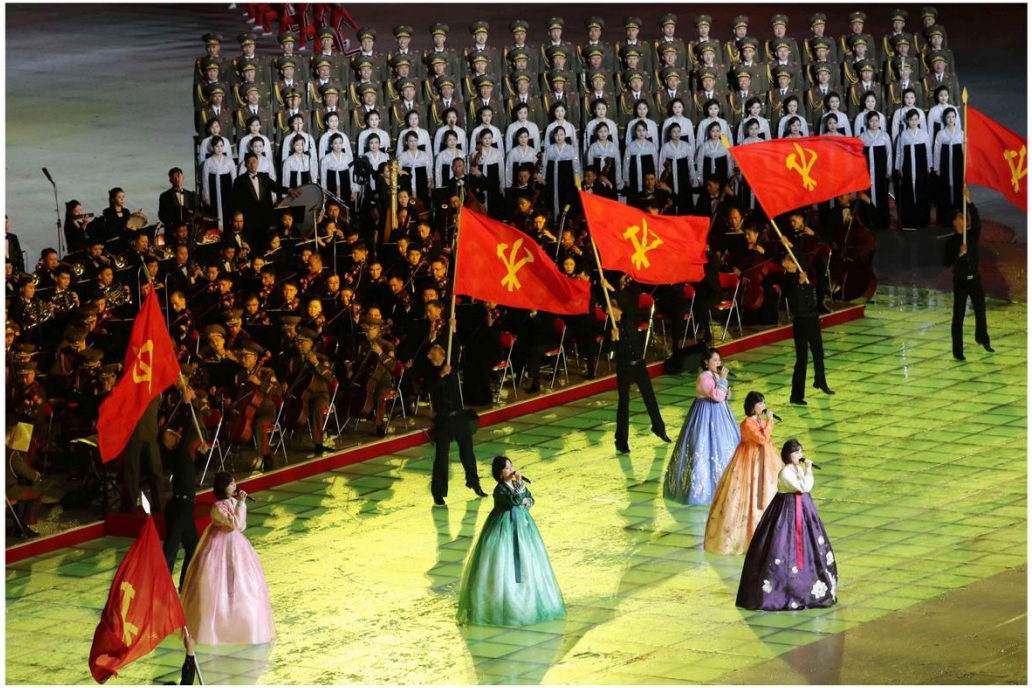
Joe Tidy
Cyber correspondent, BBC World Service

The cyber attack on Jaguar Land Rover (JLR) will cost an estimated £1.9bn and be the most economically damaging cyber event in UK history, according to researchers.

North Korea has stolen billions in cryptocurrency and tech firm salaries, report says

THE ASSOCIATED PRESS

October 23, 2025 at 12:15 JST



People perform during the ceremony marking the 80th anniversary of the founding of the ruling Workers' Party at the May Day Stadium in Pyongyang, North Korea, Oct. 9, 2025. (AP Photo)

1. UNFI cyberattack – disruptions to the food supply chain

In mid-June, United Natural Foods Inc. (UNFI), a major US grocery wholesaler and primary distributor for Whole Foods, fell victim to a crippling cyberattack. The incident crippled its electronic ordering systems, forcing temporary shutdown of automated ordering and delivery services, which in turn caused notable grocery shortages across North America. The attack, believed to have originated from unauthorised access, left UNFI scrambling to restore networked operations in coordination with partners .

Why it matters

- Highlighted the fragility of digital food supply systems and dependency on a single distributor.
- Forced many retailers to seek alternate wholesalers.

What businesses should do

- Vet third-party providers more thoroughly.
- Enhance disaster-recovery and business-continuity plans within supply chains.

Baking Manufacturer Suffers Cyberattack

JUN 16, 2025 | NEWS

By Gregory Hale
Chicago, Illinois-based Alpha Baking Co. suffered a cyberattack in January and is now letting victims know their personally identifiable information ended up stolen in the hack.

While the company said it has no evidence the stolen data is undergoing any kind of abuse at the moment, the company is issuing notices to victims.

"On January 23, 2025, we identified unusual activity on our computer network," the company said in a letter sent out to victims of the attack. "We immediately took steps to investigate. A forensic investigation conducted by external experts determined that an unauthorized third party obtained certain files stored on our network."

Alpha Baking then said it retained a team of forensic experts to review the contents of the documents it thought the attackers purloined.

RELATED STORIES

- Cyberattack Alters Food Distributor's Operations
- Second Attack in 2 Months for Clothing Maker
- First-Aid Product Maker Hit in Cyberattack
- Contract Driller Data Encrypted

ASTRAL FOODS, SOUTH AFRICA'S LARGEST POULTRY PRODUCER, LOST OVER $1M DUE TO A CYBERATTACK

Pierluigi Paganini March 25, 2025

Astral Foods, South Africa's largest poultry producer, lost over $1M due to a cyberattack disrupting deliveries and impacting operations.

Astral Foods is a South African integrated poultry producer and one of the country's largest food companies. It specializes in poultry production, animal feed, and related agricultural operations. The company supplies chicken products to retail, wholesale, and fast-food markets in South Africa and neighboring countries. Astral reported over $1 billion in annual revenue for 2024.

Cyberattacks on the food industry 2024

February

USA Feb 02
North East, PA
Juice producer

USA Feb 13
Horsham Townshi..., PA
Industrial bakery

AUS Feb 15
Mile End South, SA
Chain

IND Feb 27
India
Fast food chain

March

B Mar 06
Puurs-Sint-Amands
Brewery

USA Mar 06
Kansas City, MO
Brewery

B Mar 07
Puurs-Sint-Amands
Coffee roastery

USA Mar 10
Rosemead, CA
Restaurant chain

S March
Motala
Grocery chain

USA Mar 26
Sunset Hills, MO
Restaurant chain

April

USA Apr 05
Los Angeles, CA
Coffeehouse chain

S Apr 16
Umeå
Dairy

May

E May
Spain
Slaughterhouse

D May?
Aachen
Sweets manufacturer

June

CDN June?
Longueuil, QC
Dairy

USA Jun 30
Napa, CA
Wine producer

August

USA Aug 12
Seattle, WA
Company in the fish...

UK Aug 18
Attleborough
Poultry factory

USA Aug 23
Rockleigh, NJ
Food company

September

L Sep
Luxembourg
Alcoholic beverage ...

USA Sep
New York City, NY
Alcoholic beverage ...

October

USA Oct 18
Chino, CA
Food company

November

F Nov 12
Fontainebleau
Frozen food deliver...

D Nov 14
Ostbevern
Food company

USA Nov 21
Seattle, WA
Coffeehouse chain

USA Nov 29
Winston-Salem, NC
Doughnut chain

December

CDN Dec 12
Québec, QC
Retail chain

Total: 27

KonBriefing Research

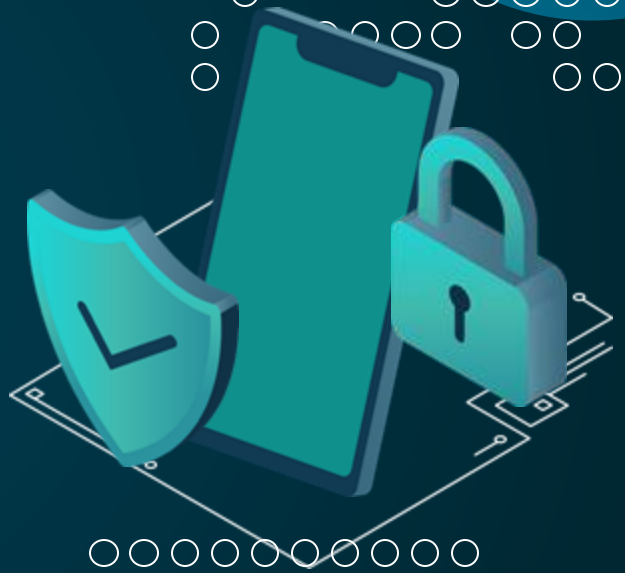
01

Uvod u ZKS

Zašto nova europska pravila znače i našu veću odgovornost za sigurnost poslovanja.

Što ćemo danas naučiti

- Što je ZKS i zašto se odnosi i na našu tvrtku
- Kako tvoj svakodnevni rad utječe na kibernetičku sigurnost
- Kako prepoznati sumnjive poruke, datoteke i ponašanja
- Što učiniti ako sumnjaš da se dogodio incident
- Kako funkcionira sigurnosna kopija (backup) i plan oporavka
- Zašto koristimo višefaktorsku autentikaciju (MFA)
- Kako svatko od nas može pomoći da posao teče bez prekida



Sigurnost počinje s tobom.

Što je Zakon o kibernetičkoj sigurnosti (ZKS)

Zakon o kibernetičkoj sigurnosti (ZKS) je hrvatski zakon koji prenosi u praksu europsku NIS2 direktivu – propis koji postavlja nova pravila za zaštitu mrežnih i informacijskih sustava.

Cilj ZKS-a je:

- Povećati otpornost tvrtki i institucija na kibernetičke prijetnje
- Osigurati kontinuitet poslovanja i zaštitu podataka
- Uspostaviti suradnju između privatnog i javnog sektora u slučaju incidenata

ZKS je naš domaći okvir za provedbu europskih pravila o kibernetičkoj sigurnosti – cilj nije birokracija, nego sigurnije i otpornije poslovanje

Koga se ZKS tiče

Zakon se odnosi na tzv. važne i ključne subjekte:

- energetike
- transporta
- prehrambene industrije
- financijskog sektora
- zdravstva i digitalnih usluga

Što ZKS zahtijeva

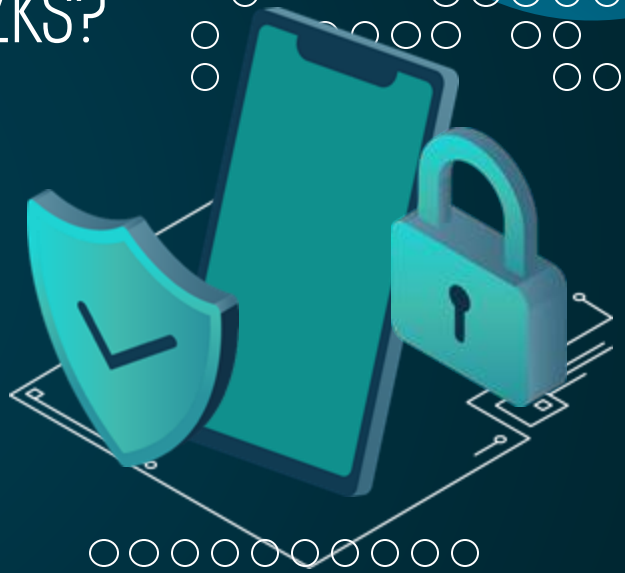
- Uspostavu organizacijskih i tehničkih mjera zaštite
- Procjenu rizika i upravljanje incidentima
- Edukaciju zaposlenika i uprave
- Prijavu kibernetičkih incidenata nadležnom tijelu
- Dokazivanje usklađenosti kroz nadzor ili inspekciju

Zašto pričamo o ZKS-u?

- **Zakon o kibernetičkoj sigurnosti obvezuje sve važne subjekte u Hrvatskoj – uključujući i prehrambenu industriju – da štite svoje informacijske sustave i poslovne procese od kibernetičkih prijetnji.**
- Cilj je osigurati neprekidnost poslovanja, zaštitu podataka, sustava i opskrbnih lanaca, te spriječiti prekide u proizvodnji.
- U današnjem digitalnom okruženju svaki klik, poruka ili propust može dovesti do zastoja, gubitka podataka ili financijske štete.
- Zato su zaposlenici prva linija obrane – njihova pažnja i odgovornost ključni su dio sigurnosnog sustava.

Tko spada u važne subjekte prema ZKS?

- "Važni subjekti" su organizacije koje pružaju **bitne usluge za društvo i gospodarstvo**.
- Prehrambena industrija je **dio lanca opskrbe hranom**, pa spada u taj okvir.
- Naša tvrtka mora dokazati da **štiti podatke, sustave i procese** od kibernetičkih rizika.
- Obveze vrijede **za sve zaposlenike**, ne samo za IT odjel.



ZKS se ne odnosi samo na tehnologiju — odnosi se na ljude i procese.

Što ZKS traži od tvrtki i zaposlenika

Tvrtka mora:

- Osigurati zaštitu svojih sustava, mreža i podataka
- Imati planove za oporavak u slučaju kibernetičkog incidenta
- Redovito provoditi sigurnosne kopije (backup)
- Prijavljivati incidente nadležnim tijelima u roku od 24 sata
- Provoditi edukaciju i testiranja zaposlenika

Zaposlenici moraju:

- Pažljivo rukovati poslovnim podacima
- Koristiti lozinke i MFA po pravilima
- Prijaviti svaku sumnjivu poruku, grešku ili incident
- Poštivati interne politike i procedure sigurnosti

02

Osnove ZKS

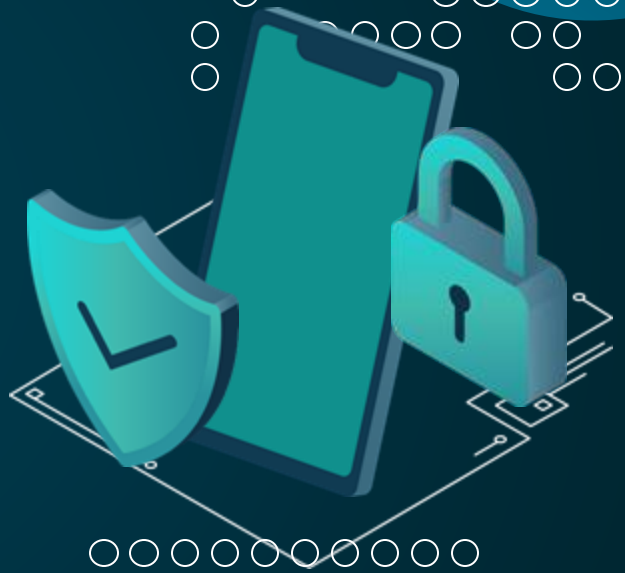
Važni apsketi direktive

Pregled glavnih aspekata

Područje	Tema	Šta to znači za nas
1	Odgovornost Uprave	Uprava mora osigurati da postoji sustav upravljanja sigurnošću – edukacija, politike, planovi i resursi.
1	Sigurnosne mjere	Tvrtka mora imati provedene tehničke i organizacijske mjere (npr. backup, MFA, plan kontinuiteta poslovanja, prijava incidenata).
32	Prijava incidenata	Ozbiljni sigurnosni incidenti moraju se prijaviti Nacionalnom centru za kibernetičku sigurnost (NCSC) u roku od 24 sata od saznanja.
43	Nadzor i sankcije	Nadležna tijela mogu provjeravati provedbu mjera i izreći kazne ako se obveze ne poštuju (do 10 mil. € ili 2 % prihoda).

Obveze uprave prema ZKS-u

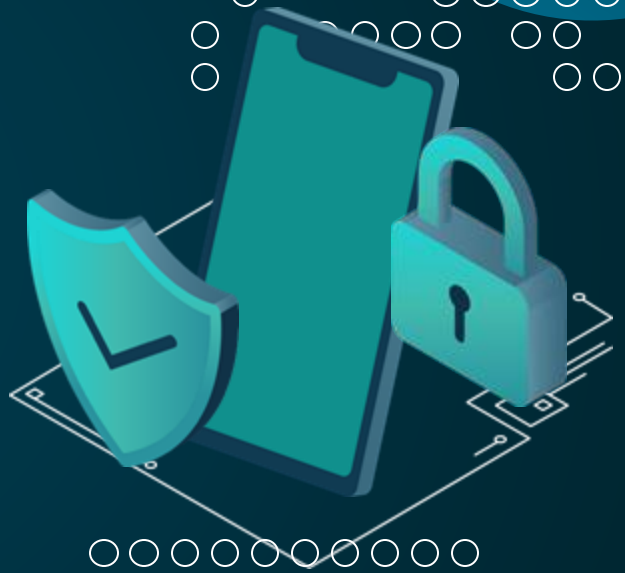
- Uprava i menadžment odgovorni su za uspostavu i provedbu sustava kibernetičke sigurnosti u tvrtki.
- Moraju osigurati resurse, osoblje i procese potrebne za zaštitu poslovnih sustava, mreža i podataka.
- Dužni su odobriti politike sigurnosti, redovito procjenjivati rizike i donositi odluke na temelju tih procjena.
- Obvezni su proći edukaciju o kibernetičkoj sigurnosti i promicati kulturu sigurnosti među zaposlenicima.
- U slučaju neprovođenja mjera ili propusta u nadzoru, odgovorne osobe mogu snositi osobnu prekršajnu i financijsku odgovornost.



Liderstvo u kibernetičkoj sigurnosti počinje primjerom – ne samo politikom

Sigurnosne mjere prema ZKS-u

- 🔐 Upravljanje rizicima – procjena prijetnji, planiranje zaštite i redovita kontrola rizika
- 💾 Backup i oporavak – izrada sigurnosnih kopija i test vraćanja podataka
- ⚙️ Postupanje s incidentima – definirani proces prijave i rješavanja sigurnosnih incidenata
- 🧩 Kontinuitet poslovanja (BCP/DR) – plan za nastavak rada u slučaju napada, kvara ili prekida
- 🧠 Edukacija zaposlenika – redovite obuke, provjere i podizanje svijesti o sigurnosti
- 🔑 Kontrola pristupa i MFA – zaštita korisničkih računa i višefaktorska autentikacija
- 🔍 Praćenje i otkrivanje prijetnji – detekcija sumnjivih aktivnosti i neovlaštenih pristupa
- 📈 Procjena učinkovitosti mjera – redovite interne provjere i poboljšanja sigurnosnog sustava



Tehničke i organizacijske mjere

Tehnilčke mjere:

- Sigurnosni softver (antivirus, firewall, nadzor mreže i sustava)
- Višefaktorska autentikacija (MFA) za zaštitu korisničkih računa
- Redoviti backup podataka i test vraćanja iz sigurnosnih kopija
- Kontrola pristupa sustavima i praćenje aktivnosti korisnika
- Šifriranje osjetljivih podataka i sigurna pohrana datoteka
- Ažuriranje operacijskih sustava i aplikacija radi zatvaranja ranjivosti

Organizacijske mjere::

- Politike i procedure sigurnosti informacija
- Plan kontinuiteta poslovanja (BCP/DRP) i plan oporavka nakon incidenata
- Obuka i podizanje svijesti zaposlenika o sigurnosnim pravilima
- Postupci prijave i rješavanja incidenata
- Redovite interne provjere, testiranja i revizije učinkovitosti mjera
- Ugovori i sigurnosne klauzule s partnerima i dobavljačima

Prava sigurnost nastaje tek kad se tehnologija i ljudi usklade.

Povezanost ZKS s ISO 27001 i GDPR-om

Standard / Direktiva	Glavni cilj	Kako se povezuje
ZKS	Jačanje kibernetičke otpornosti organizacija i opskrbnih lanaca	Propisuje obvezne sigurnosne mjere, planove oporavka i pravovremenu prijavu incidenata Nacionalnom centru za kibernetičku sigurnost (NCSC).
ISO27001	Uspostava Sustava upravljanja sigurnošću informacija (ISMS)	Pruža strukturu, procedure i kontrolne mjere koje pomažu organizaciji dokazati usklađenost sa ZKS-om i održavati stalno poboljšanje.
GDPR	Zaštita osobnih podataka fizičkih osoba	Djelomično se preklapa – i ZKS i GDPR zahtijevaju sigurnost podataka, prijavu incidenata i odgovornost uprave za zaštitu informacija.

Nadzor, inspekcije i kazne.

Nadzor:

- Nadzor nad provedbom Zakona provodi Nacionalni centar za kibernetičku sigurnost (NCSC) i druga nadležna tijela.
- Tijela mogu zatražiti dokumentaciju i dokaze o provedbi mjera (planovi, politike, evidencije incidenata, zapisi o edukacijama).
- Provode se redoviti i izvanredni nadzori radi provjere stvarne primjene sigurnosnih mjera, a ne samo formalne usklađenosti.
- Tvrtka mora surađivati s nadležnim tijelima i omogućiti pristup traženim podacima.

Inspekcije i sankcije::

- Ako se utvrdi da obveze nisu ispunjene, tijela mogu izdati:
  - Nalog za usklađivanje (rok za otklanjanje nepravilnosti)
  - Prekršajni nalog ili novčanu kaznu
- Kazne mogu iznositi do 10 milijuna eura ili 2 % godišnjeg prometa – ovisno što je veće.
- Odgovorne osobe u upravi mogu snositi i osobnu prekršajnu odgovornost, ako nisu osigurale provođenje mjera.

Cilj nadzora nije kažnjavanje, nego jačanje otpornosti i povjerenja u sustav.

03

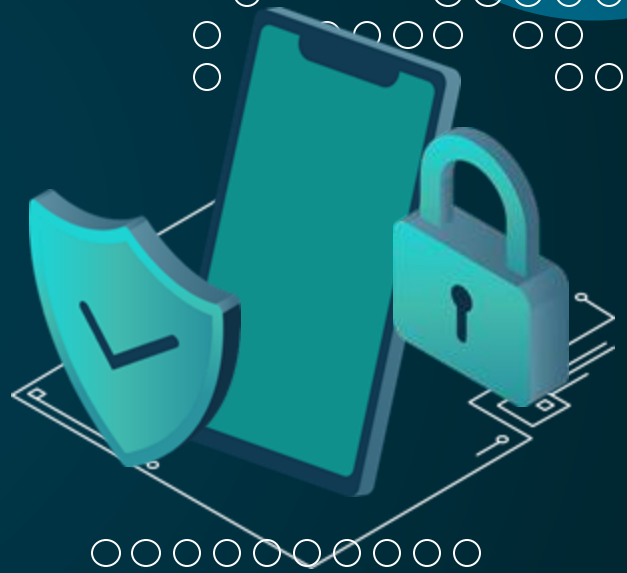
Cyber higijena

Male svakodnevne navike koje sprječavaju velike sigurnosne incidente

Što znači *cyber higijena*

Cyber higijena znači **svakodnevne navike i ponašanja** koja pomažu u zaštiti računala, podataka i sustava – isto kao što osobna higijena čuva zdravlje.

- 🔐 Korištenje jakih lozinki i višefaktorske autentikacije (MFA)
- 📩 Pažljivo otvaranje e-mailova i izbjegavanje sumnjivih linkova
- 💾 Redovito spremanje i sigurnosne kopije podataka
- 💻 Ažuriranje sustava i programa
- 🚫 Ne korištenje privatnih uređaja na poslovnim mrežama
- 🧠 Razmišljanje prije klika – svaka radnja može imati posljedice



Male navike – velika zaštita.

Pravila za lozinke i MFA

Dobra lozinka = najbolja zaštita!
Lozinka štiti tvoje korisničke podatke i poslovne informacije.
Slaba lozinka = otvorena vrata napadaču.
Preporučuje se:

- Koristi barem 12 znakova (slova, brojevi, simboli).
- Nemoj koristiti osobne podatke (ime, datum rođenja, naziv firme).
- Redovito mijenjaj lozinku – posebno nakon sumnjivih aktivnosti.
- Koristi različite lozinke za različite sustave.
- Po mogućnosti koristi password manager (alat za sigurno čuvanje lozinki).

Višefaktorska autentikacija (MFA)

MFA znači da osim lozinke koristiš još jedan dokaz da si to stvarno ti —
npr. SMS kod, aplikaciju (Microsoft Authenticator, Google Authenticator) ili fizički token.

Zašto je važna?
Čak i ako netko sazna tvoju lozinku, bez drugog faktora ne može pristupiti sustavu..

Cilj Lozinka je ključ – MFA je lokot.

Primjer kreiranja jake lozinke

Lukovnjak - otok pored Primoštena

www.facebook.com - stranica na koju se logiram

bara.daniel777@gmail.com - email s kojim se logiram

kajnvokuL - otok napisan unatrag

kajfcnvokuL - nakon trećeg slova dodajem prva dva suglasnika stranice na koju se logiram

k1jfcnv0kuL - prvi samoglasnik zamjenim brojem (a-1,e-2,i-3,o-4,u-5), ako je prvi samoglasnik o stavljam broj 4, a ako postoji bilo gjde u tekstu stavljam broj 0

k1jfc.nvokuL - nakon 5 znaka stavljam .**(točka)**
k1jfc.nvokuL-bd - na kraju dodajem -bd što mi je oznaka e-maila s kojim se logiram,

sve zajedno 15 znakova

Prepoznavanje phishinga

Što je phishing?

Phishing je pokušaj prijevare putem e-pošte, poruka ili lažnih web stranica kojima napadači žele:

- ukrasti lozinke ili podatke,
- instalirati zlonamjerni softver,
- ili navesti zaposlenika da napravi neku pogrešnu radnju (npr. uplatu, klik, slanje datoteke).

Kako prepoznati sumnjiv e-mail
Obrati pažnju na:

1. Pošiljatelja – adresa izgleda slično, ali nije prava npr. info@pan-pek.hr umjesto info@panpek.hr
2. Linkove i privitke – neočekivani dokumenti, "računi", "nove cijene" ili "sigurnosne obavijesti"
3. Hitnost i prijetnje – "Odmah otvorite!", "Vaš račun će biti blokiran!"
4. Greške u jeziku – pravopisne pogreške, neobičan ton, loš hrvatski prijevod
5. Previše dobro da bi bilo istinito – "Osvojili ste nagradu!", "Dodatak plaći – otvorite privitak"

Ako nešto izgleda čudno – vjerojatno i jest. Bolje prijaviti nego riskirati.

REPUBLIKA HRVATSKA
Ministarstvo pravosuđa

RAVNATELJSTVO DRŽAVNE POLICIJE

PRAVNI PODNESAK

Za potrebe pravne istrage

Ja sam DALIBOR JURIĆ, načelnik Ureda kriminalističke policije RH i voditelj Odjela za međunarodnu policijsku suradnju (INTERPOL)

Nakon zapljene kibernetičkog kriminalca, kontaktirao sam vas u suradnji s Nacionalnim centrom za analizu pornografije, dječje pornografije i kibernetičkih slika (CNAIP) i Službom za analizu Međunarodne organizacije kriminalističke policije (INTERPOL) kako bih vas obavijestio da je poduzeto nekoliko pravnih radnji protiv vas, uključujući:

***PEDO PORNOGRAFIJA**
***PORNO GRAFIČKE WEB STRANICE**
***CYBER PORNOGRAFIJA**
***PEDOFILIJA**
***EGZIBIONIZAM**

Željeli bismo čuti od vas putem e-pošte. poštom na ovu adresu, navodeći svoje razloge kako bi se mogli ispitatii provjeriti za odmjeravanje sankcija; to je unutar strogog vremenskog ograničenja od 72 sata.

Nakon tog razdoblja, proslijedit ćemo vaš dosje tužitelju koji vodi vaš slučaj kako bi izdali nalog za vaše uhićenje.

Stoga ćete biti registrirani kao seksualni prijestupnik, a vaši podaci također će biti objavljeni medijima kako bi se objavili vaši postupci za sprječavanje recidivizma i na taj način odvratili druge podnositelje zahtjeva od takvih aktivnosti.

Sada ste upozoreni.

DALIBOR JURIĆ
načelnik Uprave kriminalističke policije RH
Voditelj a Međunarodne policijske suradnje
Ravnatelstvo policije

Dropbox - Password Reset Link

Message

Delete | Reply | Reply All | Forward | Move | Junk | Rules | Read/Unread | Categorize | Follow Up

Dropbox - Password Reset Link

D

• **Dropbox <dropbox@shared-document.com>**

Friday, 27 September 2019 at 08:46

Show Details

Hi Tino,

Someone recently requested a password change for your Dropbox account. If this was you, you can set a new password here:

If you don't want to change your password or didn't request this, secure your account Click Here immediately.

To keep your account secure, please don't forward this email to anyone. See our Help Center for more security tips.

Happy Dropboxing!

Pošiljatelj: Olt Director <Olt.Director@tgie.ro>
Poslano: 20. veljače 2020. 10:44
Primatelj: no-reply@microsoft.net
Predmet: Vaš račun za e-poštu treba odmah potvrditi

MICROSOFT VAŽNA OBAVIJEST

Vaš račun za e-poštu treba odmah **potvrditi** ili će vaš račun za e-poštu biti obustavljen ako nije potvrđen sada.

https://ismcadmissions.wixsite.com/mysite

Hvala na razumijevanju

Microsoftov tim za provjeru

Pošiljatelj: XBanka info@hr-xbanka.com → usporedite e-mail adresu pošiljatelja sa službenom e-mail adresom banke

Primatelj (To):

Predmet: VAŽNO → obratite pažnju na predmet e-poruke, najčešće se navodi primatelja da je riječ o hitnoj/važnoj poruci

Dragi klijent, → generički pozdrav

→ izlika da je račun ugrožen što izaziva reakciju primatelja

Vaš račun je blokiran jer sumnjamo da je neovlaštenoj trećoj strani pristupio vašoj kreditnoj kartici.

Kliknite ovdje poveznica u roku od 24 sata da biste ponovno aktivirali svoj račun. → traži se hitna reakcija

→ sumnjiva poveznica

Iskreno,

Xbanka

smishing

Što je smishing?

pokušaj prijevare putem SMS poruka ili mobilnih aplikacija za razmjenu poruka (npr. WhatsApp, Viber, Telegram).

Kako izgleda smishing napad
Napadač šalje poruku koja izgleda kao da dolazi od:

- banke, dostavne službe, teleoperatera,
- porezne uprave,
- ili čak od vašeg poslodavca ili kolege.

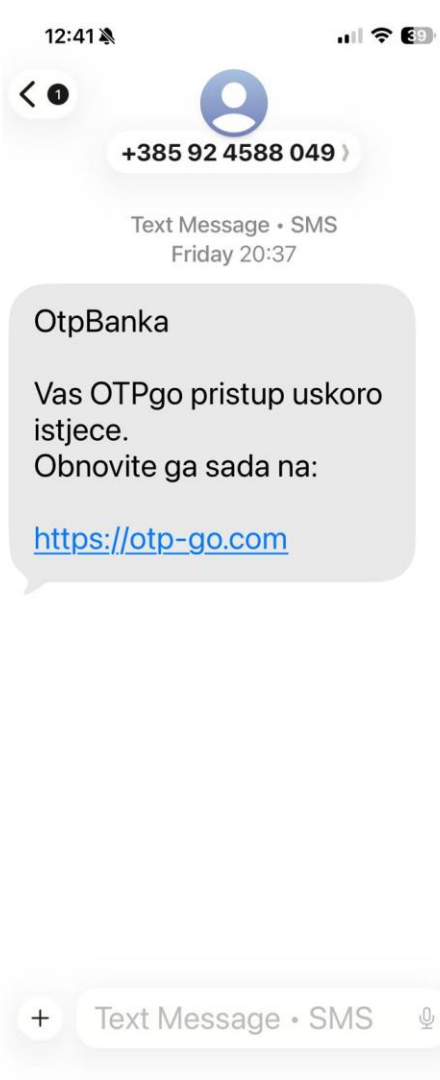
Poruka obično sadrži link koji vodi na lažnu stranicu ili traži brzu akciju.

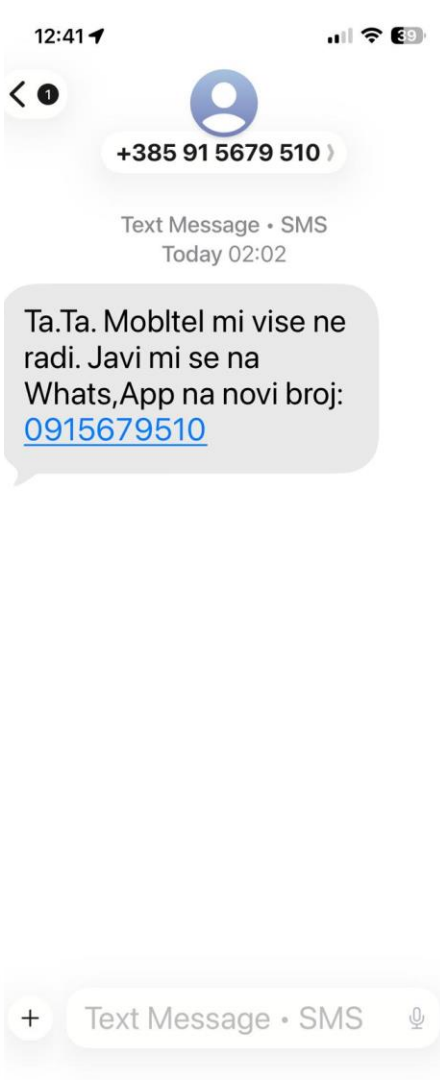
Kako se zaštititi

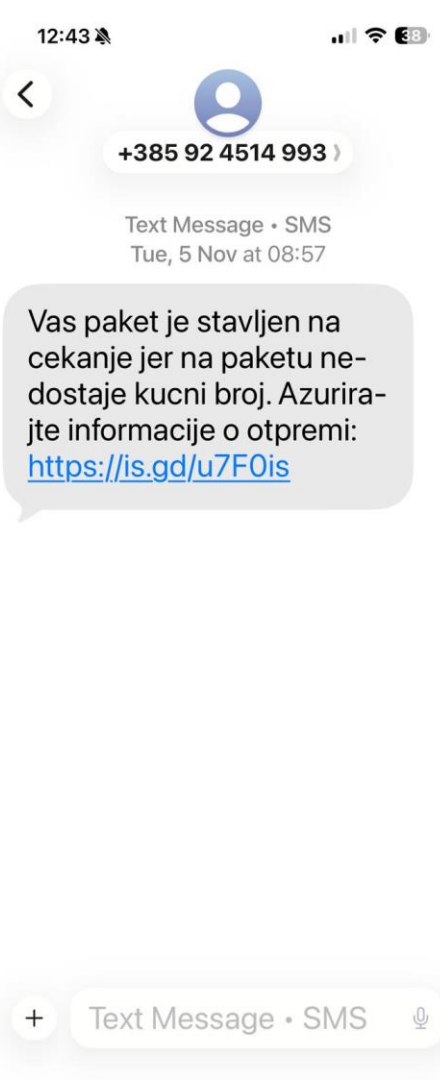
- Nikad ne otvaraj linkove iz sumnjivih SMS-ova.
- Ne preuzimaj aplikacije iz linkova – koristi samo Google Play / App Store.
- Ako poruka tvrdi da dolazi iz banke, provjeri službenu aplikaciju ili nazovi kontakt centar.
- Obriši poruku i obavijesti IT ako se radi o poslovnom telefonu.

Phishing koristi e-mail.
Smishing koristi SMS.
Cishing (ili voice phishing) koristi poziv.


12:42
+385 92 4530 120
Text Message • SMS
Tue, 8 Apr at 04:04
maamaa..mobitel mi je pokvaren..Pisi mi na WhatsApa..novi broj: +385917286748 ovaj
Text Message • SMS


12:41
+385 92 4588 049
Text Message • SMS
Friday 20:37
OtpBanka
Vas OTPgo pristup uskoro istjece.
Obnovite ga sada na:
https://otp-go.com
Text Message • SMS


12:41
+385 91 5679 510
Text Message • SMS
Today 02:02
Ta.Ta. Mobltel mi vise ne radi. Javi mi se na Whats,App na novi broj: 0915679510
Text Message • SMS


12:43
+385 92 4514 993
Text Message • SMS
Tue, 5 Nov at 08:57
Vas paket je stavljen na cekanje jer na paketu nedostaje kucni broj. Azurirajte informacije o otpremi: https://is.gd/u7F0is
Text Message • SMS

Ažuriranja i sigurni USB uređaji

Ažuriranja (Updateovi)
Redovita ažuriranja sustava i programa nisu gnjavaža – to su popravci sigurnosnih rupa koje napadači najčešće iskorištavaju.

Zapamti:
- Kad računalo traži ažuriranje – odmah dopusti instalaciju.
- Ne odgađaj "kasnije" – to "kasnije" često znači nikad.
- Ažuriranja uključuju antivirus, operacijski sustav, Office, ERP aplikacije i preglednike.
- IT odjel povremeno može pokretati automatska ažuriranja – ne prekidaj proces.

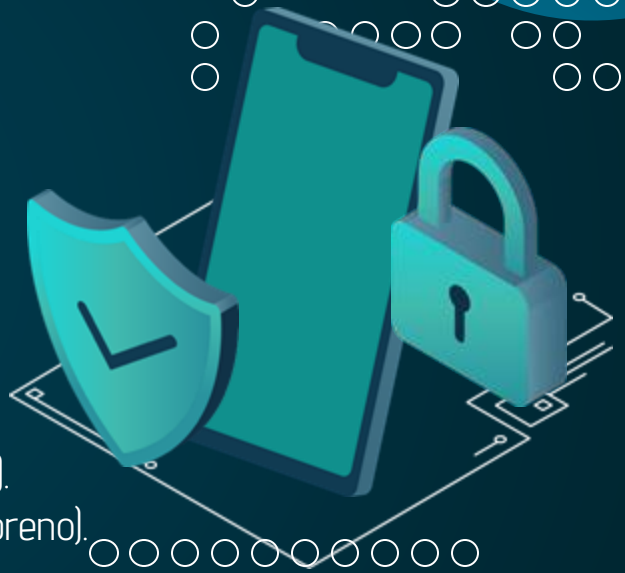
Sigurna upotreba USB uređaja
USB-ovi su praktični, ali mogu biti "Trojanac na ključu" – lako prenose viruse i ransomware.

Nikad nemoj:
- koristiti nepoznate USB stickove ili one pronađene "slučajno";
- spajati privatni USB na službeno računalo;
- koristiti USB za prijenos podataka između poslovnih i osobnih uređaja.

Uvijek:
- koristi odobrene i označene USB uređaje koje je odobrio IT;
- prije upotrebe, USB treba proći antivirusnu provjeru;
- po završetku posla, izbriši osjetljive podatke i sigurno izbaci uređaj.

Sigurnost mobilnih uređaja

Mobilni telefoni danas sadrže poslovne e-mailove, kontakte, aplikacije, dokumente i lozinke. Gubitak, krađa ili zlonamjerna aplikacija može značiti curenje poslovnih podataka ili neovlašteni pristup sustavima.



Preporučene sigurnosne navike

- Zaključavaj zaslon PIN-om, otiskom prsta ili prepoznavanjem lica.
- Instaliraj samo provjerene aplikacije (Google Play / App Store).
- Ukloni nepotrebne aplikacije koje ne koristiš.
- Redovito ažuriraj sustav i aplikacije.
- Ne spajaj se na otvorene Wi-Fi mreže (kafići, benzinske, javni prostori).
- Ne koristi poslovne aplikacije na privatnim uređajima (osim ako je odobreno).
- Šifriraj memoriju uređaja i koristi službeni alat za sigurnosne kopije.
- Nikad ne pohranjuj lozinke u bilješkama, galeriji ili chatovima.

Tvoj mobitel je tvoja poslovna iskaznica – čuvaj ga kao sef

Sigurna upotreba mreže i Wi-Fija

Mreža je "krvotok" poslovanja — kroz nju prolaze svi podaci, od e-maila do sustava za naručivanje i ERP-a. Ako napadač dođe do mreže, može doći i do poslovnih informacija, lozinki ili financijskih podataka..

Sigurnosne korištenje mreže:

- Koristi samo službene mreže u tvrtki ili poslovnim prostorima.
- Nikad se ne spajaj na nepoznate ili otvorene Wi-Fi mreže (kafići, hoteli, kolodvori).
- Ako radiš od kuće, koristi sigurnu kućnu mrežu s lozinkom (ne "default password").
- Ne dijeli hotspot sa službenog mobitela bez odobrenja IT-a.
- VPN (Virtual Private Network) koristi kad se spajaš na interne sustave izvan firme.
- Ne koristi dijeljenje datoteka (file sharing) ili peer-to-peer aplikacije na poslovnoj mreži.
- Ne koristi poslovnu opremu (npr. laptop) za privatno surfanje, streaming ili društvene mreže

Ne vidiš tko je na Wi-Fiju — ali on možda vidi tebe

Vijesti

Haker iz Italije pokazao u Zagrebu kako ljudima krade podatke: 'Pogledaj što ću uzeti ovom tipu, ima erotske fotke'

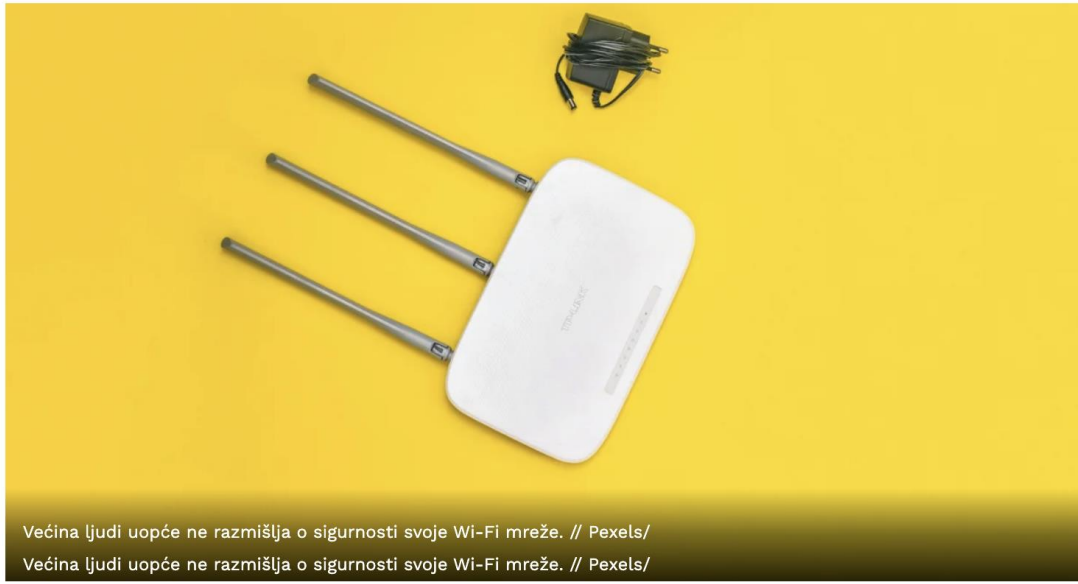
Talijanski novinar s hakerom je odlučio pokazati koliko je lako doći do tuđih podataka

FOTO: SCREENSHOT / LE IENE

VALENTINA PAVLICA 08. 06. 2024. 72 PREPORUKA

Talijanski novinar **Luigi Pelazza** istraživački serijal "Le Iene" doveo je u Zagreb gdje je s talijanskim hakerom, čiji je identitet u emisiji skriven, pokazao kakve sve opasnosti vrebaju i kojih se sve podataka i informacija hakeri bez ikakvih problema mogu domoći, piše Jutarnji list.

Sa velikom lakoćom hakeri mogu "provaliti" u vaš Wi-Fi: Evo kako da se zaštitite



Većina ljudi uopće ne razmišlja o sigurnosti svoje Wi-Fi mreže. // Pexels/

Većina ljudi uopće ne razmišlja o sigurnosti svoje Wi-Fi mreže. // Pexels/

Piše: B. A. | 27.09.2023. (16:15)

Wi-Fi ili bežični internet je nešto što većina ljudi postavi i zaboravi. Nedovoljno zaštićene mreže laka su meta za hakere, a s njima - baš sve vaše informacije!

Sigurno ponašanje u proizvodnji i prodaji

U proizvodnji i prodaji koristi se sve više pametnih uređaja, digitalnih vaga, blagajni, tableta i sustava naručivanja. Svaki od njih može postati ulazna točka ako nije pravilno korišten. Zato svaka osoba u lancu – od pekare do uprave – ima ulogu u kibernetičkoj zaštiti.

Preporučene prakse u svakodnevnom radu:

- Ne ostavljaj prijavljene uređaje bez nadzora (računalo, blagajna, tablet).
- Zaključaj ekran kad odlaziš od radnog mjesta.
- Ne dijeli svoje korisničke podatke s kolegama – svatko mora koristiti svoj račun.
- Ne koristi neodobrene USB uređaje za prijenos HACCP, skladišnih ili narudžbenih podataka.
- Ne mijenjaj postavke uređaja bez znanja IT odjela (posebno mrežne postavke).
- Koristi službene kanale komunikacije (e-mail, Teams, poslovni chat), ne privatne WhatsApp grupe.
- Čuvaj poslovne dokumente – nemoj ih fotografirati, dijeliti ni slati privatno.

Sigurnost ne ovisi o tehnologiji – nego o našim navikama

04

Incidenti

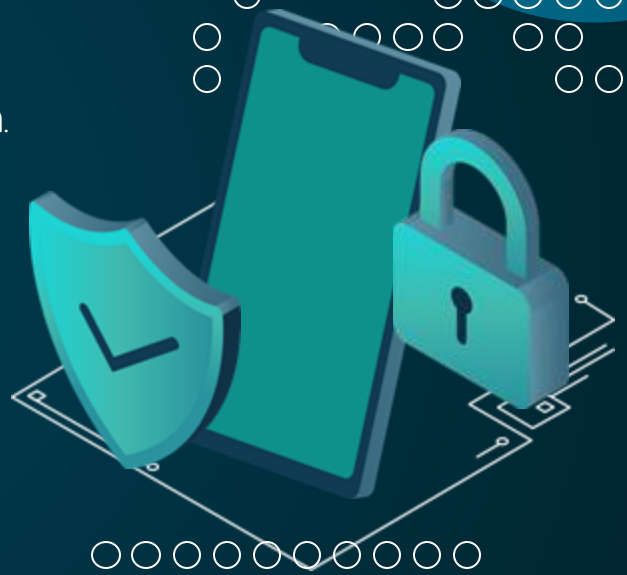
Kako prepoznati, prijaviti i reagirati kad nešto krene po zlu

Sigurnosni incident je svaki događaj koji ugrožava ili može ugroziti sigurnost informacija, sustava ili poslovanja.

To može biti namjerno djelovanje (napad) ili slučajna pogreška.

Primjeri sigurnosnih incidenata

- Računalo se iznenada zaključalo ili prikazuje poruku o šifriranju (ransomware).
- Otvoren je e-mail sumnjivog sadržaja ili privitak nepoznatog pošiljatelja.
- Lozinka ili korisnički račun kompromitirani su (netko drugi se prijavio u tvoje ime).
- USB uređaj, laptop ili mobitel s poslovnim podacima je izgubljen ili ukraden.
- Povjerljivi dokument (HACCP, popis zaposlenika, ugovori) poslan je pogrešnoj osobi.
- Sustav radi neuobičajeno sporo ili pokazuje znakove manipulacije.
- Netko traži osjetljive informacije koje ne bi trebao imati (npr. "kolega iz IT-a" preko e-maila).



Uoči – prijavi – zaštiti.

Kako prepoznati da nešto nije u redu

Računalo ili sustav

- Uređaj radi sporije nego inače, "smrzava se" ili se sam gasi.
- Na ekranu se pojavljuju čudne poruke, skočni prozori ili reklame.
- Programi se otvaraju ili zatvaraju sami od sebe.
- Antivirusi su isključeni ili javlja da "nema zaštite".
- Datoteke su nestale, preimenovane ili imaju čudne nastavke (.locked, .enc).

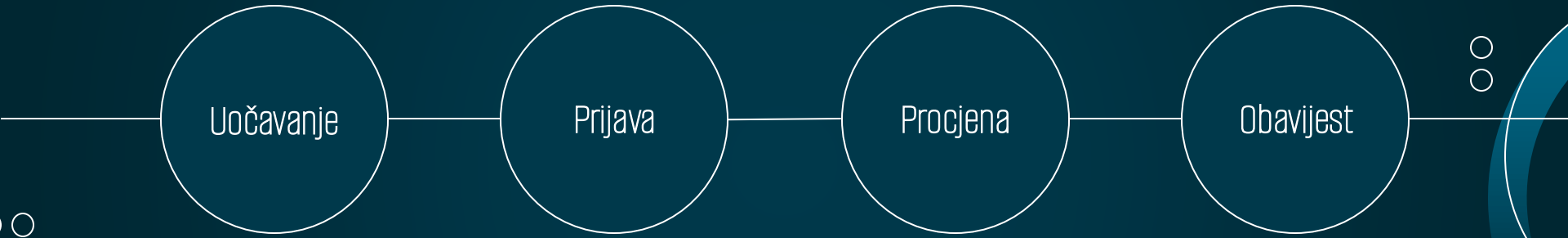
E-mail i komunikacija

- Dobivaš e-mailove koji traže brzu reakciju ili unos lozinke.
- Poruke dolaze s neobičnih adresa ili imaju pravopisne pogreške.
- Kolega "traži" osjetljive podatke koje inače ne bi trebao tražiti.
- Netko iz "IT-a" traži da "hitno klikneš ovdje" – a poruka nije iz službene adrese.

Mreža i sustavi

- Pojavljuju se neobične prijave u sustav iz nepoznatih lokacija.
- ERP ili POS sustav ne reagira ispravno ili prikazuje netočne podatke.
- Ne možeš pristupiti dijeljenim mapama ili diskovima koji su inače dostupni.

Prijava incidenta.



Zaposlenik

Primijetiš sumnjivo ponašanje (čudan e-mail, šifrirane datoteke, neobične prijave). Ne pokušavaš "popraviti" sam

Zaposlenik

Odmah dojavi kroz službeni kanal (helpdesk/telefon/obrazac) IT-u ili sigurnosnom službeniku.

IT

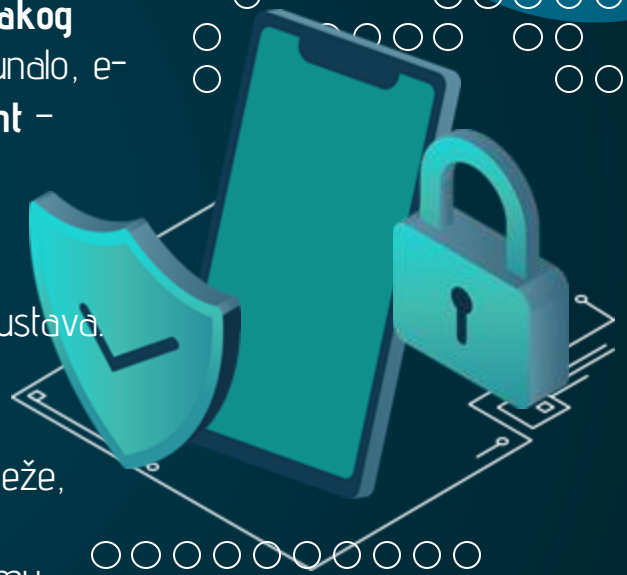
Izolira zahvaćeni uređaj/sustav, utvrđuje ozbiljnost, prikuplja dokaze i odlučuje o daljnjim koracima.

CISO

Ako je incident značajan, prijavljuje ga NKSC u roku od 24 sata te koordinira komunikaciju i oporavak.

Uloga svakog zaposlenika

Kibernetička sigurnost nije samo posao IT odjela – to je **odgovornost svakog zaposlenika**, bez obzira na radno mjesto. Svaka osoba koja koristi računalo, e-mail, mobitel ili bilo koji digitalni sustav **može spriječiti ili izazvati incident** – ovisno o tome koliko pažljivo postupa.



Tvoja uloga u zaštiti tvrtke

- **Budi oprezan** – prepoznaj sumnjive poruke, datoteke i ponašanja sustava.
- **Prijavi sve sumnje** odmah – nema "malih" incidenata.
- **Čuvaj lozinke i uređaje** – nikad ih ne dijeli s drugima.
- **Primjenjuj pravila cyber higijene** – redovita ažuriranja, sigurne mreže, provjereni USB-ovi.
- **Podrži kolege** – ako netko nije siguran, pomogni mu ili ga uputi IT timu.
- **Sudjeluj u edukacijama** – znanje je najbolja zaštita.

Zajedno gradimo kulturu sigurnosti

05

Backup

Sigurnosna kopija podataka –
naš štit protiv gubitka informacija

Što je *backup* i zašto je bitan

Backup (sigurnosna kopija) znači spremanje kopije važnih podataka na drugo, sigurno mjesto – kako bi se podaci mogli vratiti ako original bude izgubljen, izbrisan ili oštećen.

Zašto je važan

- Štiti od gubitka podataka zbog grešaka, kvarova ili napada (npr. ransomware).
- Omogućuje brz oporavak poslovanja – bez backupa, zastoji mogu trajati danima.
- Spašava od posljedica virusa i šifriranja podataka.
- Pomaže dokazati usklađenost sa Zakonom o kibernetičkoj sigurnosti i internim politikama.
- Smanjuje trošak i stres u slučaju incidenta – obnova iz kopije je brža i jeftinija od ponovne izrade podataka.

Kako se radi backup

- **Automatski** – IT sustav svakodnevno radi sigurnosne kopije.
- **Na više lokacija** – u tvrtki i izvan nje (off-site ili u oblaku).
- **Redovito testiranje vraćanja** – da se provjeri radi li backup ispravno.
- Zaposlenici ne moraju ručno spremati, ali moraju paziti da datoteke ne drže samo lokalno (npr. na Desktopu).

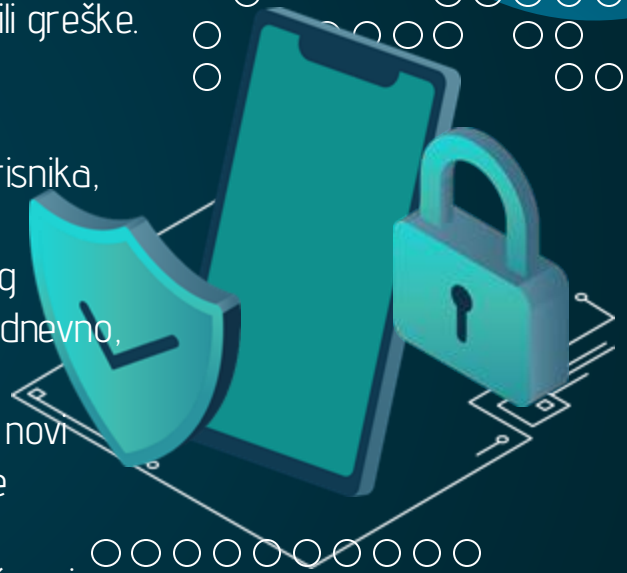
Svi griješimo. Backup postoji da te pogreške ne koštaju tvrtku

Kako se podaci vraćaju nakon kvara

Oporavak podataka (recovery) je proces vraćanja izgubljenih, oštećenih ili šifriranih datoteka iz sigurnosnih kopija (backupa) nakon tehničkog kvara, napada ili greške.

Procesu praksi

1) Utvrđivanje problema – IT provjerava što je uzrok kvara: greška korisnika, oštećenje diska, virus, nestanak struje, ransomware ili drugi napad.
2) Pronalaženje sigurnosne kopije –Podaci se preuzimaju iz posljednjeg dostupnog backupa – lokalnog ili oblaka. Ako je backup rađen svakodnevno, gubitak podataka najčešće je manji od 24 sata.
3) Vraćanje datoteka i testiranje – Kopija se vraća na izvorno mjesto ili novi uređaj. IT provjerava da su datoteke cjelovite i da sve aplikacije rade ispravno
4) Analiza i prevencija Nakon oporavka, IT dokumentira uzrok i predlaže mjere da se sličan problem više ne ponovi (npr. ažuriranja, bolji backup ciklus, edukacija korisnika).



06

BCP / DRP i rizici

Kako osigurati da posao ne stane – čak i kad sustavi zakažu.

Što je *Business Continuity Plan* (BCP)

Backup (sigurnosna kopija) znači spremanje kopije važnih podataka na drugo, sigurno mjesto – kako bi se podaci mogli vratiti ako original bude izgubljen, izbrisan ili oštećen.

Što BCP obuhvaća

- Informacijske sustave (ERP, e-mail, POS, dokumentacija)
- Proizvodnju i distribuciju
- Zaposlenike i komunikaciju
- Dobavljače i opskrbne lance
- Prostore, opremu i dokumente.

Glavni ciljevi BCP-a

- Održati kritične procese i spriječiti prekid poslovanja.
- Osigurati dostupnost podataka i resursa.
- Jasno definirati uloge i odgovornosti tijekom krize.
- Smanjiti financijsku i reputacijsku štetu.
- Povećati povjerenje klijenata, partnera i nadležnih tijela.

BCP = plan koji čuva ritam poslovanja.

Što je *Disaster Recovery Plan* (DRP)

Disaster Recovery Plan (DRP) je tehnički plan koji definira kako se informacijski sustavi i podaci vraćaju u funkciju nakon ozbiljnog incidenta ili katastrofe..

Što DRP uključuje:

- Sigurnosne kopije (backup) i procedure vraćanja podataka.
- Rezervne poslužitelje i lokacije spremne za aktivaciju.
- Uloge IT osoblja – tko reagira, kako i kojim redoslijedom.
- Vrijeme oporavka (RTO) – koliko brzo sustav mora proraditi.
- Prihvatljiv gubitak podataka (RPO) – koliko se podataka može izgubiti bez štete.
- Testiranje oporavka – redovite vježbe vraćanja sustava.

DRP je "tehnički brat" Business Continuity Plana (BCP):

- BCP osigurava da posao ne stane.
- DRP osigurava da IT sustavi ponovno rade.

BCP + DRP = otpornost poslovanja

Što je rizik u kibernetičkoj sigurnosti

Rizik znači mogućnost da se dogodi događaj koji će negativno utjecati na poslovanje, podatke ili sustave.

U kibernetičkoj sigurnosti rizik nastaje kada postoji:

- prijetnja (npr. napad, kvar, pogreška zaposlenika)
- i ranjivost (npr. zastarjeli sustav, slaba lozinka, nepažnja).

Vrsta rizika	Primjer u prehrambenoj industriji	Moguće posljedice
Tehnički	Zastarjeli antivirus, nezaštićeni server	Gubitak podataka, šifriranje sustava
Ljudski	Zaposlenik otvara phishing e-mail	Kompromitacija korisničkih računa
Operativni	Neuspješan backup ili greška u ERP-u	Zastoj u proizvodnji i isporuci
Opskrbni	Napad na IT sustav dobavljača	Kašnjenje sirovina, prekid lanca
Reputacijski	Incident dospije u medije	Gubitak povjerenja kupaca i partnera

Kako smanjujemo rizike

Na razini tvrtke

- Provedba tehničkih i organizacijskih mjera (kontrole pristupa, backup, antivirus).
- Edukacija zaposlenika – svi znaju prepoznati i prijaviti sumnju.
- Procjena rizika – redovito analiziranje prijetnji i slabih točaka.
- Politike i procedure – jasna pravila za ponašanje i odgovornosti.
- Planovi BCP i DRP – priprema za oporavak ako nešto pođe po zlu.

Na razini zaposlenika

- Pažljivo koristi e-mail i USB uređaje.
- Čuvaj lozinke i ne dijeli pristupne podatke.
- Odmah prijavi sve sumnje ili neobične pojave.
- Ažuriraj uređaje i ne koristi nepoznate mreže.
- Budi primjer drugima u sigurnom ponašanju.

Rizike ne možemo ukloniti, ali ih možemo kontrolirati – zajedno

07

MFA

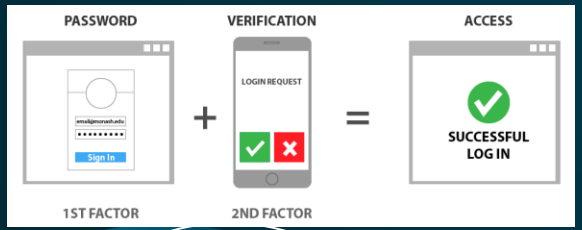
Dodatni sloj zaštite koji čini razliku između sigurnosti i kompromitacije

Što je *MFA*

MFA (Multi-Factor Authentication) znači da se prilikom prijave u sustav ne koristi samo lozinka, nego se mora dati dodatni dokaz identiteta – drugi "ključ" koji potvrđuje da ste to zaista vi.

MFA kombinira barem dva od tri elementa:

- **Nešto što znaš** – lozinka ili PIN
- **Nešto što imaš** – mobitel, token, aplikacija (npr. Microsoft Authenticator)
- **Nešto što jesi** – otisak prsta, lice ili prepoznavanje glasa



Kako to štiti korisnički račun

- Ako netko ukrade lozinku, ne može se prijaviti bez drugog faktora (npr. koda iz aplikacije).
- Kod se stalno mijenja – obično svakih 30 sekundi.
- Napadač ne može "pogoditi" ili ponoviti taj kod.
- MFA sprječava najčešće oblike napada: phishing, brute-force, krađu lozinki.
- Značajno smanjuje rizik neovlaštenog pristupa sustavima – čak i ako korisnik pogriješi.

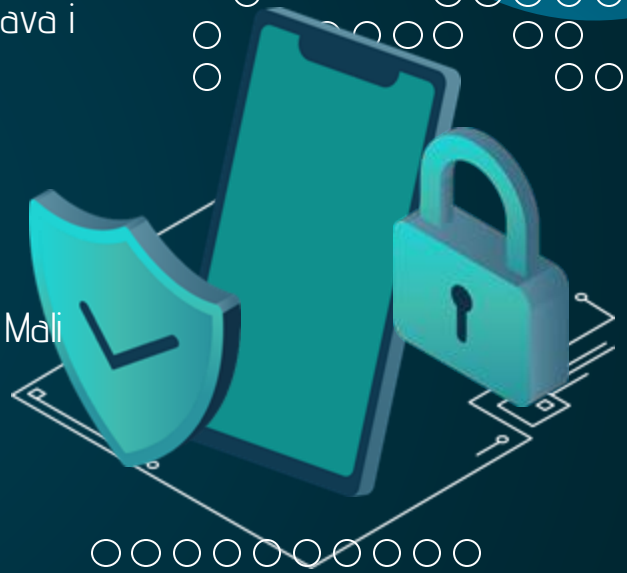
08

Summary

Kibernetička sigurnost počinje sa svakim od nas

Što smo danas naučili

Kibernetička sigurnost je zajednička odgovornost.
Nije posao samo IT-a – svatko od nas ima ulogu u zaštiti podataka, sustava i poslovanja.
Prepoznaj sumnjivo ponašanje.
Ako ti nešto izgleda čudno – prijavi odmah. Brza reakcija sprječava veće probleme.
Pridržavaj se pravila cyber higijene.
Ažuriraj uređaje, koristi sigurne lozinke, provjerene mreže i MFA zaštitu. Mali postupci čine veliku razliku.
Backup i plan kontinuiteta čuvaju poslovanje.
Backup vraća podatke, BCP i DRP vraćaju sustave i ritam rada.
Edukacija je najbolja zaštita.
Što više znaš, to bolje prepoznaješ rizike.
Zato redovita obuka nije formalnost – nego ulaganje u sigurnost svih nas.



Sigurnost počinje s tobom – svaki klik, svaka odluka, svaki dan.

Hvala!

Pitanja?

daniel@adventurespirit.hr
+385 94 5041 496
www.adventurespirit.hr