azop
Agencija za zaštitu osobnih podataka

Sufinancira
Europska unija

ARC
GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

Co-funded by the European Union

ARC

Croatian Personal Data Protection Agency
azop
Agencija za zaštitu osobnih podataka

OLIVIA

GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

foi
UNIVERSITY OF ZAGREB
FACULTY OF ORGANIZATION AND INFORMATICS
VARAŽDIN

UNIVERSITÀ DEGLI STUDI FIRENZE

VUB
VRIJE UNIVERSITEIT BRUSSEL

Olivia- virtual assistant for GDPR compliance

Glavni rezultat projekta ARC2 kojeg Agencija provodi s ciljem pružanja potpore prilikom usklađivanja s GDPR-om je online edukativni portal, web alat Olivia.

Olivia ima misiju pomoći poduzetnicima da svladaju osnove GDPR-a kroz kratke edukativne materijale, videozapise, kvizove, webinare i generiranje osnovne dokumenitacije za usklađivanje s GDPR-om.

15 tečajeva (svaki tečaj sastoji se o teorijskog i praktičnog modula):

1) Opća uredba o zaštiti podataka - osnove
2) Načela obrade osobnih podataka
3) Pravni temelji za obradu osobnih podataka
4) Politika privatnosti/izjava o obradi osobnih podataka
5) Službenik za zaštitu podataka
6) Procjena učinka na zaštitu podataka
7) Evidencija o aktivnostima obrade
8) Ugovor između voditelja obrade i izvršitelja obrade podataka
9) Organizacijske mjere
10) Tehničke mjere
11) Videonadzor
12) Kolačići
13) Prava ispitanika
14) Prijenos podataka u treće zemlje
15) Povrede podataka

https://olivia-gdpr-arc.eu/hr

KORACI ZA USKLAĐIVANJE S GDPR-om

TEHNIČKE I ORGANIZACIJSKE MJERE ZA ZAŠTITU PODATAKA

Članak 32. Opće uredba o zaštiti podataka "Sigurnost obrade"

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, **voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere** kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

(a) pseudonimizaciju i enkripciju osobnih podataka;

(b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;

(c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;

(d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Tehničke mjere odnose se na konkretna tehnološka rješenja i alate koji se koriste za zaštitu osobnih podataka. **To uključuje softverske i hardverske alate poput enkripcije, sustava za kontrolu pristupa, sigurnosnih sustava za prijavu i logiranja aktivnosti. Te mjere su usmjerene na sprječavanje neovlaštenog pristupa i osiguranje sigurnosti podataka putem tehnologije.**

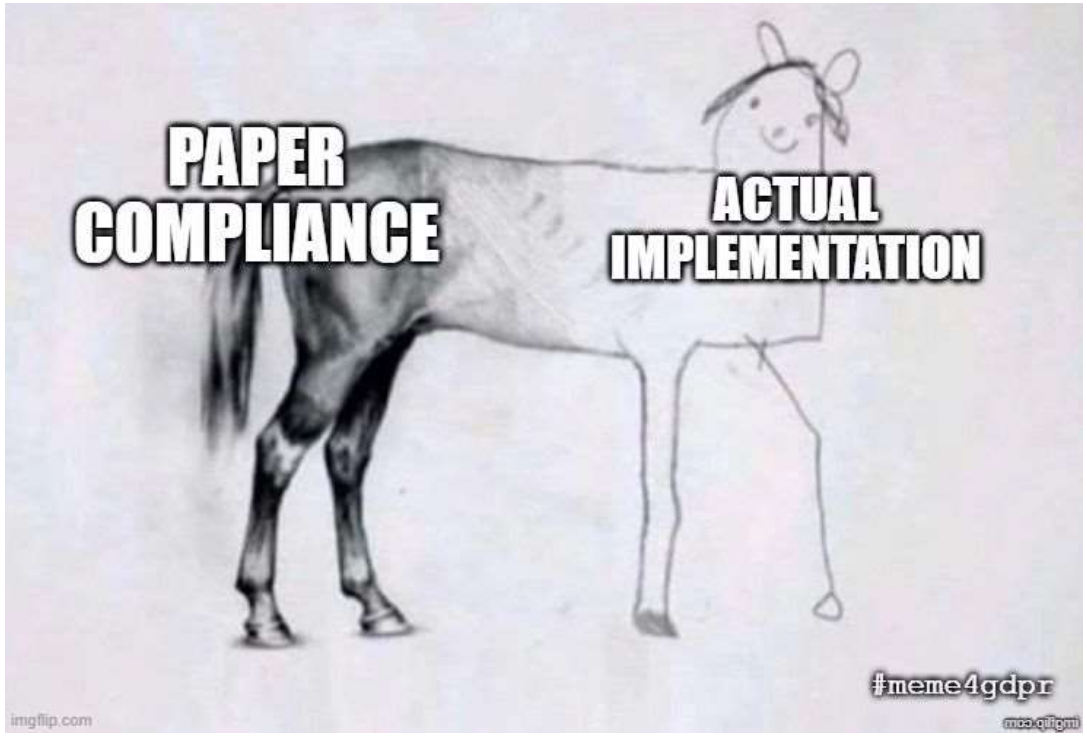
Tehničke mjere uključuju I :

•Fizičke sigurnosne mjere poput vrata i brava

Organizacijske mjere odnose se na politike, procedure i prakse unutar organizacije koje osiguravaju zaštitu podataka.

To uključuje razvoj sigurnosnih politika, obuku zaposlenika o zaštiti podataka, jasno definirane procedure za upravljanje pristupnim pravima i redovite revizije sigurnosnih postupaka. Ove mjere su usmjerene na osiguranje da ljudi i procesi unutar organizacije pravilno upravljaju podacima.

TEHNIČKE I ORGANIZACIJSKE MJERE SE DOISTA MORAJU PRIMJENJIVATI U PRAKSI, A NE DA PREDSTAVLJAJU "MRTVO SLOVO NA PAPIRU"!



2. **Prilikom procjene odgovarajuće razine sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.**

1. KORAK PROCIJENITI RIZIKE AKTIVNOSTI OBRADE!

OSNOVNI KORACI ZA PROCJENU RIZIKA:

1) **Identificirajte sve aktivnosti obrade osobnih podataka u organizaciji, radi li se o automatiziranoj obradi osobnih podataka ili neautomatiziranoj, medije koje uključuje obrada osobnih podataka:**

- hardver (npr.: poslužitelji, prijenosna računala, tvrdi diskovi);
- softver (npr.: operativni sustavi, poslovni softver);
- resurse računalstva u oblaku (npr.: SaaS, PaaS, IaaS);
- logičke ili fizičke komunikacijske kanale (npr.: žičane veze, Wi-Fi, internet, usmene razmjene, kurirske službe);
- papirnate dokumente (npr.: tiskani dokumenti, preslike);
- fizičke prostorije i prostore u kojima se nalaze prethodno navedeni elementi (npr.: IT sobe, uredi).

2) Procijenite rizike koje nosi sa sobom svaka obrada podataka:

a. Identificirajte potencijalne učinke na prava i slobode ispitanika za sljedeća tri neželjena događaja:
– nezakonit pristup podacima (npr. krađa identiteta nakon otkrivanja platnih lista svih zaposlenika tvrtke neovlaštenoj trećoj strani);
– neželjena izmjena podataka (npr. pogrešna optužba za prekršaj nakon izmjene pristupnih zapisa);
– privremeni ili trajni gubitak podataka (npr. neotkrivanje interakcije između lijekova koje pacijent već uzima i novog lijeka zbog nemogućnosti pristupa elektroničkom kartonu pacijenta).

b. Identificirajte izvore rizika (tko ili što bi moglo biti uzrok svakog neželjenog događaja?), uzimajući u obzir unutarnje i vanjske ljudske izvore (npr. IT administrator, korisnik, vanjski napadač, konkurent) kao i unutarnje i vanjske ne-ljudske izvore (npr. voda, epidemija, opasni materijali, računalni virus).

c. Identificirajte moguće prijetnje (**što bi moglo omogućiti da se svaki od navedenih neželjenih događaj dogodi?).**

Te prijetnje se pojavljuju na prethodno identificiranim medijima (hardver, softver, komunikacijski kanali, papirnati dokumenti itd.), a ti mediji koji sadrže osobne podatke mogu:

– biti korišteni na neprimjeren način (npr. zloupotreba prava, pogreška u rukovanju);
– izmijenjeni (npr. zaraženi softver ili hardver - keylogger, instaliranje zlonamjernog softvera);
– izgubljeni (npr. krađa prijenosnog računala, gubitak USB sticka);
– "promatrani" (npr. promatranje ekrana laptopa u vlaku, geolokacija opreme);
– oštećeni (npr. vandalizam, degradacija zbog prirodnog trošenja);
– preopterećeni (npr. puna jedinica za pohranu, napad uskraćivanjem usluge).

d. **Identificirajte postojeće ili planirane mjere za smanjenje svakog rizika** (npr. kontrola pristupa, sigurnosne kopije, mogućnost ulaska u trag opremi, sigurnost prostora, enkripcija, anonimizacija).

e. **Procijenite ozbiljnost (utjecaj ili potencijalna šteta za ispitanike) i vjerojatnost (vjerojatnost pojave) rizika s obzirom na prethodne elemente). NIZAK, SREDNJI, VISOK, VRLO VISOK, BODOVANJE 1-4**

3) Provjeravajte učinkovitost implementiranih mjera.

PRIKUPLJANJE PRESLIKA BANKOVNIH KARTICA GOSTIJU HOTELA PUTEM MAILA, BODOVANJE **1-4,**

RAZINA RIZIKA: OZBILJNOST*VJEROJATNOST

NEŽELJENI DOGAĐAJ	UČINAK NA ISPITANIKA	GLAVNI IZVOR RIZIKA	GLAVNE PRIJETNJE	POSTOJEĆE ILI PLANIRANE MJERE	OZBILJNOST /UTJECAJ NA ISPITANIKA	VJEROJATNOST
NEOVLAŠTEN PRISTUP PODACIMA	VRLO VISOK	ZAPOSLENIK/NEOVLAŠTENA TREĆA STRANA	ZLOUPORABA OSOBNIH PODATAKA/KRAĐA IDENITETA	-	3	3
NEŽELJENA/ NEOVLAŠTENA IZMJENA PODATAKA	VRLO VISOK	ZAPOSLENIK/NEOVLAŠTENA TREĆA STRANA	ZLOUPORABA OSOBNIH PODATAKA/KRAĐA IDENITETA	-	3	2
GUBITAK PODATAKA	VRLO VISOK	ZAPOSLENIK/NEOVLAŠTENA TREĆA STRANA	ZLOUPORABA OSOBNIH PODATAKA/KRAĐA IDENITETA	-	3	3

Obrada rizika

Razina, Mjere, Prihvatljivost rizika - primjer

Razina rizika	Opis rizika	Prihvatljivost rizika
12,16	***Najviši rizik*** Vjerojatnost od ostvarenja rizika je iznimno visoka. Ostvarenje rizika može dovesti do katastrofalnih ili visoko štetnih posljedica za poslovanje ili postizanje poslovnih ciljeva, uzimajući u obzir financijske gubitke, gubitka povjerenja, kršenje zakonskih i regulatornih obaveza kao i gubitak kontrole nad ključnim poslovnim procesima i pružanju usluga korisnicima.	Neophodno je poduzeti hitne mjere za smanjivanje rizika na prihvatljivu razinu. Što prije definirati plan tretiranja rizika, prioritete i rok implementacije korektivnih mjera.
8,9	***Umjereno visoki rizik*** Vjerojatnost od ostvarenja rizika je umjereno visoka. Ostvarenje rizika može donijeti štetne posljedice za poslovanje ili postizanje poslovnih ciljeva.	Neophodno je poduzeti mjere za smanjivanje rizika što je prije moguće i postaviti prioritete i rokove implementacije korektivnih mjera.

Razina rizika	Opis rizika	Prihvatljivost rizika
6	***Srednji rizik*** Vjerojatnost ostvarenja rizika je srednje razine.	Neophodno je poduzeti mjere za smanjivanje rizika u razumnom roku.
3,4	***Niži srednji rizik*** Vjerojatnost ostvarenja rizika je niže srednje razine.	Neophodno je, od slučaja do slučaja, poduzeti mjere za smanjivanje rizika ili rizik može biti prihvaćen uzimajući u obzir kriterije za prihvaćanje rizika.
1,2	***Nizak rizik*** Učinak na poslovanje ako se rizik ostvari je zanemariv.	Rizik je prihvatljiv i može ga se tretirati u redovitoj proceduri.

RAZINA učinka	Opis
Niska	Pojedinci se mogu susresti s manjim neugodnostima, koje mogu savladati bez ikakvog problema (vrijeme provedeno na ponovni unos podataka, "gnjavaža", nelagoda itd.
Srednja	Pojedinci se mogu susresti sa značajnim neugodnostima, koje će uspjeti savladati usprkos nekim poteškoćama (dodatni troškovi, uskrata pristupa poslovnim uslugama, strah, manjak razumijevanja, stres, manji fizički nedostaci itd.).
Visoka	Pojedinci se mogu suočiti sa značajnim posljedicama, koje bi trebali moći savladati usprkos ozbiljnim poteškoćama (zlouporaba novčanih sredstava, stavljanje na crnu listu od strane financijskih institucija, štete na imovini, gubitak zaposlenja, poziv na sud, pogoršanje zdravlja itd.).
Vrlo visoka	Pojedinci koji se mogu susresti sa značajnim, ili čak nepovratnim posljedicama, koje ne mogu savladati (nemogućnost rada, dugotrajne psihološke ili fizičke bolesti, smrt itd.).

Tehničke mjere

Postavljanje zaporki za pristup podacima, programima i opremi

Zaporka se koristi kao mjera zaštite od neovlaštenog pristupa opremi, računalnim programima, elektroničkoj pošti i datotekama s podacima.

Snažna sigurnosna zaporka sadrži:
•16 ili više znakova, što više to bolje,
•velika slova (ABCDEFGH…),
•mala slova (abcdefgh…),
•brojke (123456…),
•simbole (@#$%{ } [ ] ( ) / ' " , ; : . < >…).

Snažne zaporke nije potrebno periodično mijenjati, kako su do sad bile sigurnosne preporuke. Snažnu zaporku je potrebno promijeniti na uređaju ili u programu u slučaju sumnje kako je ista kompromitirana od strane neovlaštenog korisnika i omogućuje neovlašten pristup.

Svaki zaposlenik treba imati jedinstveno korisničko ime i zaporku radi zaštite od neovlaštenog pristupa za:
- **računalo na kojem radi (stolno ili prijenosno),**
- **poslovne programe koje koristi u poslovne svrhe,**
- **adrese elektroničke pošte (e-mail) koje koristi u poslovne svrhe.**

Redovita nadogradnja operativnog sustava i računalnih programa

- ✓ **Nadogradnje često uključuju ispravke sigurnosnih ranjivosti koje su otkrivene nakon izdavanja prethodnih verzija. Bez redovitih nadogradnji, sustavi su izloženi riziku od napada i zloupotreba**

- ✓ OWASP (Open Web Application Security Project) Top Ten: ključne ranjivosti u web aplikacijama: https://owasp.org/www-project-top-ten/

- ✓ **potrebno je redovito instalirati zakrpe za sve instalirane softvere u sustavu**

Kontrola pristupa

Voditelj obrade podataka ima dužnost ograničiti pristup osobnim podacima. Veća ograničenja pristupa ili kontrole trebale bi se primijeniti na osjetljivije podatke. Voditelj obrade podataka mora biti svjestan različitih korisnika koji pristupaju njihovim sustavima/zapisima.

Različite vrste korisnika mogu uključivati:
- zaposlenike na različitim razinama;
- treće strane / izvršitelji obrade;
- kupci;
- poslovni partneri.

- ✓ **Trebale bi postojati stroge kontrole mogućnosti preuzimanja osobnih podataka iz sustava organizacije. Takvo preuzimanje može se blokirati tehničkim sredstvima (onemogućavanje pogona itd.)**

- ✓ **Mnoge su organizacije donijele odluku da blokiraju pristup USB priključcima nakon što su ispitale rizike vezane za ostavljanje takvih priključaka otvorenim prema zadanim postavkama za sve korisnike**

- ✓ **Data protection loss softver, ili softver za zaštitu podataka od gubitka,** je program koji pomaže u sprečavanju gubitka, oštećenja ili neovlaštenog pristupa podacima:

- ✓ Šifriranje podataka kako bi se zaštitili od neovlaštenog pristupa,
- ✓ Praćenje aktivnosti na mreži i otkrivanje sumnjivih ponašanja koja mogu ukazivati na pokušaj gubitka podataka,
- ✓ Ograničavanje pristupa podacima samo ovlaštenim korisnicima

```
{
   "timestamp": "2024-11-10T10:21:35Z",
   "event": "UserLogin",
   "database": "employee_db",
   "user": "employee123",
   "host": "192.168.1.30",
   "status": "Success",
   "details": {
      "client_application": "SQL Workbench",
      "session_id": "abc123xyz456",
      "login_method": "PasswordAuthentication"
   }
}
```


Log prijave u bazu podataka (u JSON formatu)
json

Vođenje evidencije pristupa osobnim podacima (LOGOVI): vode se kako bi pratili događaje, operacije i aktivnosti unutar sustava.

- služe za identifikaciju potencijalnih problema, praćenje sigurnosnih prijetnji, analizu performansi te osiguravanje usklađenosti s GDPR-om

Višefaktorska autentifikacija **(za provjeru autentičnosti pristupa koristi više od jednog faktora identiteta)**

- ✓ Kada korisnici pristupaju povjerljivim informacijama, kao što su financijski podaci, osobni identifikacijski podaci ili zdravstvene informacije
- ✓ Rad na daljinu
- ✓ Administratorski pristup: Kada administratori ili IT osoblje pristupaju sustavima sa višim privilegijama, gdje bi potencijalni kompromitirani računi mogli izazvati veće štete
- ✓ Kada se vrše promjene na sigurnosnim postavkama ili konfiguracijama sustava
- ✓ Kada korisnici pristupaju aplikacijama koje su ključno važne za poslovanje ili sigurnost organizacije
- ✓ Kada se koristi cloud usluge ili vanjski resursi, gdje je sigurnost podataka posebno važna

ENKRIPCIJA

Kriptirati se mogu:

- **mediji za pohranu podataka (USB stik, disk, prijenosni disk),**
- **dijelovi medija za pohranu,**
- **datoteke u kojima su pohranjeni podaci,**
- **sami podaci pohranjeni u bazama podataka.**

Enkripcija medija za pohranu ili samo dijela medija za pohranu u kom se čuvaju podaci radi se pomoću posebnih programa za kriptiranje.

Enkripcije i hash funkcije

Enkripcija je pretvaranje podataka pomoću šifre iz čitljivog oblika u nečitljiv (šifriran) oblik, koji je nečitljiv svima onima koji nemaju šifru (ključ) kojim se podaci mogu vratiti u čitljivi oblik.

Hash funkcije osiguravaju integritet podataka, što znači da podaci nisu izmijenjeni tijekom prijenosa ili pohrane.

Enkripcija osigurava povjerljivost poruka, štiteći informacije od neovlaštenog pristupa.

VAŽNO: Hashiranje pohranjenih lozinki u poslovnim sustavima je svakako obvezno, jer se time značajno smanjuje rizik od zloupotrebe lozinki od strane zaposlenika s pravima pristupa, a još više štiti podatke od potencijalnih hakera i cyber napada

Koristite priznate i sigurne algoritme:

•**SHA-2 ili SHA-3:** kriptografski hash algoritmi koji se koriste za generiranje jedinstvenih otisaka podataka;

•**bcrypt, scrypt, Argon2 ili PBKDF2 za pohranu lozinki:** algoritmi dizajnirani za sigurnu pohranu lozinki. Oni se koriste za hashiranje lozinki na način koji otežava napadačima da ih povrate, čak i ako dobiju pristup hashiranim lozinkama;

•**AES s odgovarajućim načinom konstrukcije (CCM, GCM ili EAX) ili ChaCha20 (s Poly1305) za simetričnu enkripciju;**

•**RSA-OAEP, ECIES-KEM ili DLIES-KEM za asimetričnu enkripciju**;

•**RSA-SSA-PSS ili ECDSA: kriptografski algoritmi koji se koriste za digitalne potpise**

Koristite dovoljno duge ključeve:

•za AES, 128, 192 ili 256-bitni ključevi se smatraju dovoljnima, a **256-bitni ključ nudi** najvišu razinu sigurnosti i potrebno ga je koristiti situacijama gdje je potrebna maksimalna zaštita;

•za RSA-bazirane algoritme, preporučuje se koristiti tajni modul i eksponente od najmanje 2048 bita ili 3072 bita, s javnim eksponentima, za enkripciju veću od 65536 bita.

PSEUDONIMIZACIJA I ANONIMIZACIJA

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Pseudonimizacija je proces zamjene osobnih podataka s alternativnim oznakama ili pseudonimima: i dalje se radi o osobnim podacima na koje se primjenuje GDPR.

Anonimizacija je proces uklanjanja svih identifikacijskih informacija iz skupa podataka tako da se ne može utvrditi identitet osobe- više nisu osobnih podaci, GDPR se ne primjenjuje.

- *Health care*

1. Name, address date of birth	2. Period of Special Assistance Benefit.	3. Body mass index	6. Research cohort reference no.
[redacted]	< 2 years	15	QA5FRD4
	> 5 years	14	2B48HFG
	< 2 years	16	RC3URPQ
	> 5 years	18	SD289K9
	< 2 years	20	5E1FL7Q

Table 5. An example of pseudonymisation by hashing (name, address date of birth) which can be easily reversed

Last Name	First Name	e-mail Address	Title	Department	Salary	Holidays Available (Days)
x	x	x	x	HQ	25.000,00 €	11
x	x	x	x	IT	17.000,00 €	5
x	x	x	x	Engineering	18.000,00 €	14
x	x	x	x	Sales	16.000,00 €	11
x	x	x	x	HQ	6.000,00 €	6

Enkripcija – BitLocker, https i slični protokoli, VPN

Pseudonimizacija i anonimizacija – ručno ili softverski

Softverski:

- **Data Masking Software**: IBM InfoSphere Optim, Oracle Data Masking and Subsetting i Informatica Dynamic Data Masking
- **Database Management Systems (DBMS)** i ugrađene funkcije za pseudonimizaciju ili maskiranje podataka: Microsoft SQL Server Dynamic Data Masking ili MySQL Data Masking
- **Data Anonymization Tools** i **ETL (Extract, Transform, Load) Tools**
- *custom* skripte i algoritmi u Pythonu, R ili Javi i drugi

Enkripcija 'in transit':

• TLS (Transport Layer Security) enkripcija komunikacije između računala, komunikacija porukama

• HTTPS (Hypertext Transfer Protocol Secure) – zaštita web sučelja i kontakt formi

• IPSec VPN (Virtual Private Network) - zaštićena komunikacija između mrežnih točaka

• SFTP (Secure File Transfer Protocol) – prijenos datoteka

Enkripcija 'at rest' :

• Advanced Encryption Standard (AES): AES-256

Firewalli
Hardverski Firewalli: Cisco ASA, Fortinet FortiGate, Palo Alto Networks Firewall
Softverski Firewalli: pfSense, Windows Firewall, iptables (Linux)

Intrusion Detection and Prevention Systems (IDPS)
Network-based: Snort, Suricata
Host-based: OSSEC, McAfee Host Intrusion Prevention

Antivirus i Anti-Malware Softver
Symantec Endpoint Protection
Kaspersky Endpoint Security
Malwarebytes

Virtual Private Networks (VPNs)
OpenVPN
NordVPN
Cisco AnyConnect

Data Loss Prevention (DLP) Alati
Symantec Data Loss Prevention
Digital Guardian
Forcepoint DLP

Sigurnosne informacije i upravljanje događajima (SIEM)
Splunk
IBM QRadar
LogRhythm

Sigurnosne analize podataka
Rapid7
Varonis
AlienVault

Upravljanje identitetima i pristupom (IAM)
Microsoft Active Directory
Okta
OneLogin

Alati za šifriranje
BitLocker (za šifriranje diska)
VeraCrypt
GnuPG (za šifriranje e-maila i datoteka)

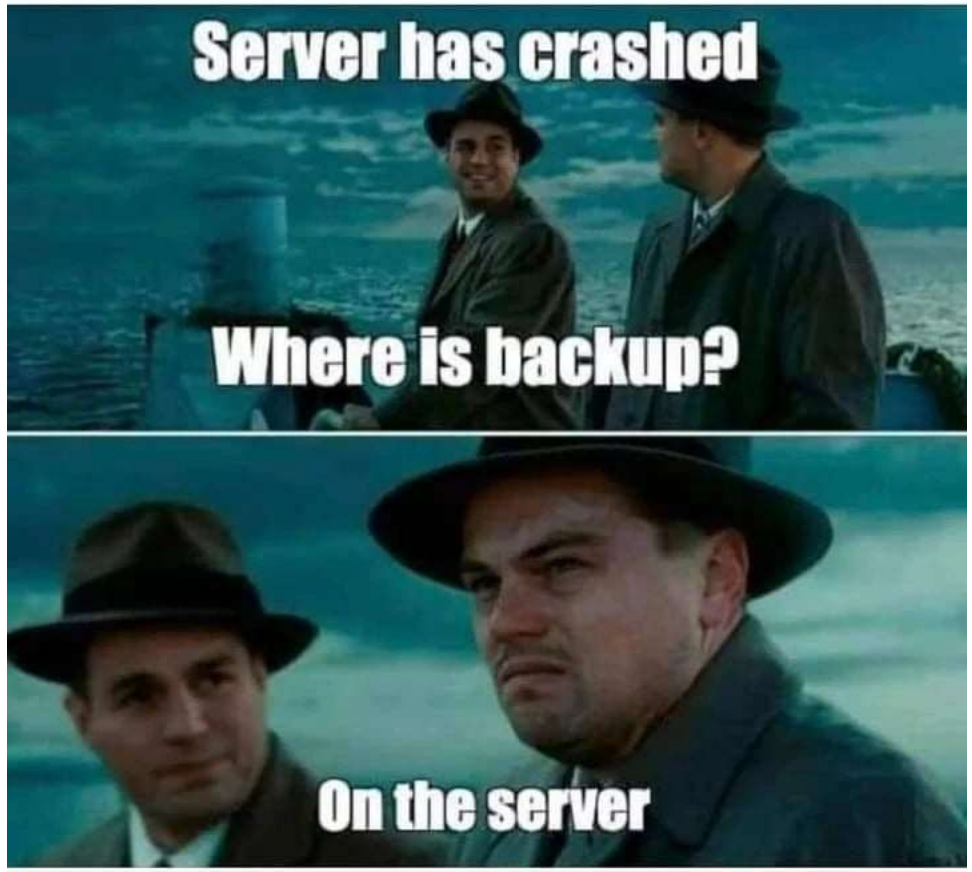
Mrežni skeneri ranjivosti
Nessus
Qualys
OpenVAS

Alati za upravljanje konfiguracijom
Ansible
Chef
Puppet

Multi-Faktorska Autentifikacija (MFA)
Google Authenticator
Authy
Duo Security

- ✓ **Instaliranje antivirusnog programa na uređaje, instaliranje vatrozida**
- ✓ **Sigurnosne kopije podataka (Backup)**

- **Redovitost: Backup podataka treba biti redovito proveden kako bi se osiguralo da su najnoviji podaci zaštićeni. Učestalost backupa ovisi o važnosti podataka i učestalosti njihovih promjena (npr. dnevni, tjedni ili mjesečni backup)**
- **Višestruke kopije: Čuvanje višestrukih kopija backup podataka na različitim mjestima**
- **Testiranje i verifikacija: Redovito testiranje procesa oporavka iz backupa ključno je za osiguravanje da su backup podaci ispravni i da se mogu uspješno obnoviti kada je to potrebno.**



Ukoliko voditelj obrade angažira IT poduzeće pružatelja usluge za izradu i čuvanja sigurnosnih kopija u oblaku (cloud backup), potrebno je voditi računa da li pružatelj usluge pruža i jamči dovoljno visoku razinu sigurnosti za tako pohranjene podatke! UGOVOR VODITELJ-IZVRŠITELJ, ČLANAK 28. GDPR-A.

Zaštita pristupa mrežnoj infrastrukturi

- ✓ Ovisno o veličini poslovnog subjekta i količini poslovne opreme (računala, prijenosnih računala, printera, mrežnih kopirki itd.) te poslovnim procesima, postoji potreba **međusobnog povezivanja navedene opreme u lokalnu mrežu kako bi međusobno mogla komunicirati i razmjenjivati podatke. Za povezivanje opreme koriste se mrežni preklopnici (eng. switch)**

- ✓ Koristite mrežne preklopnike koji imaju mogućnost konfiguriranja i zaštite pristupa konfiguraciji putem zaporke

Zaštita internetskog usmjerivača (eng. Internet router) od neovlaštenog pristupa

- ✓ Internet usmjerivač je uređaj koji omogućuje spajanje računala i ostale opreme na internet i dobili ste ga od svog pružatelja internet usluge (eng. Internet provider) kao opremu za pristup internetu

- ✓ Postoji nekoliko jednostavnih koraka za zaštitu usmjerivača, uključujući promjenu zadane lozinke, ažuriranje firmvera i omogućavanje enkripcije (npr. WPA3-najnoviji sigurnosni protokol za bežične mreže). Upute specifične za model usmjerivača obično se nalaze u priručniku koji ste dobili uz uređaj

Zaštita pristupa podacima s udaljenih lokacija od neovlaštenog pristupa

- ✓ Ukoliko poslovni subjekt ima izdvojene lokacije i međusobno ih treba povezati (umrežiti) da svi zaposlenici mogu komunicirati kao da su na jednoj lokaciji, ili zaposlenik samostalno ima potrebu raditi s udaljenog mjesta i koristiti resurse poslovnog subjekta, tada je potrebno između lokacija uspostaviti **tzv. virtualnu privatnu mrežu (VPN) (eng. Virtual Private Network)**

Zaštita podataka pohranjenih u papirnatom obliku

- ✓ podatke u papirnatom obliku potrebno je nakon korištenja pohraniti adekvatan prostor i u adekvatan uredski namještaj (ladica, ormar, vatronepropusni ormar i sl.) koji su od neovlaštenog pristupa zaštićeni ključem ili na neki drugi sigurnosni način (npr. putem kartica s čipom i čitača kartica), a ne ih držati na otvorenom poslovnom prostoru (npr. na radnom stolu, na pultu i sl.)

- ✓ **Politika čistog stola, rezač papira**

Fizička zaštita od neovlaštenog pristupa

✓ Prilikom uspostavljanja zaštitnih mjera u poslovnom subjektu, potrebno je voditi računa i o uspostavljanju odgovarajućih fizičkih mjera zaštite od nedozvoljenog pristupa kako prostorijama unutar poslovnog subjekta tako i opremi koja se koristi u poslovnom subjektu

✓ Potrebno je:

•Osigurati da se prostor zgrade osiguran od neovlaštenog pristupa na adekvatan način van radnog vremena poslovnog subjekta

•Ograničiti pristup uredskom namještaju i prostorijama u kojima se pohranjuju osobni i drugi povjerljivi podaci

•Ograničiti pristup opremi na koju se pohranjuju podaci (računalni serveri, diskovni sustavi, vanjski diskovi itd.)

Sigurnost osobnih podataka na web stranicama

Svaka web stranica mora jamčiti svoj identitet terminalima koji se povezuju s njom i povjerljivost prenesenih informacija.

• Osigurati protok razmjene podataka korištenjem TLS-a:
– implementirati **TLS (umjesto SSL) protokol na svim web stranicama**, koristeći samo najnovije verzije i provjeravajući njegovu ispravnu implementaciju;
– **učiniti korištenje TLS-a obaveznim za sve stranice za autentifikaciju ili stranice na kojima se prikazuju ili prenose osobni podaci**.

• Ograničiti komunikacijske portove na one koji su strogo potrebni za ispravno funkcioniranje instaliranih aplikacija. Ako je pristup web poslužitelju moguć samo putem HTTPS-a, trebate dozvoliti samo dolazni IP mrežni promet na portu 443 i blokirati sve ostale portove

• Ograničiti pristup administrativnim alatima i sučeljima samo ovlaštenom osoblju. Osobito, ograničiti korištenje administratorskih računa na unutarnje IT timove, i to samo za administrativne radnje koje to zahtijevaju

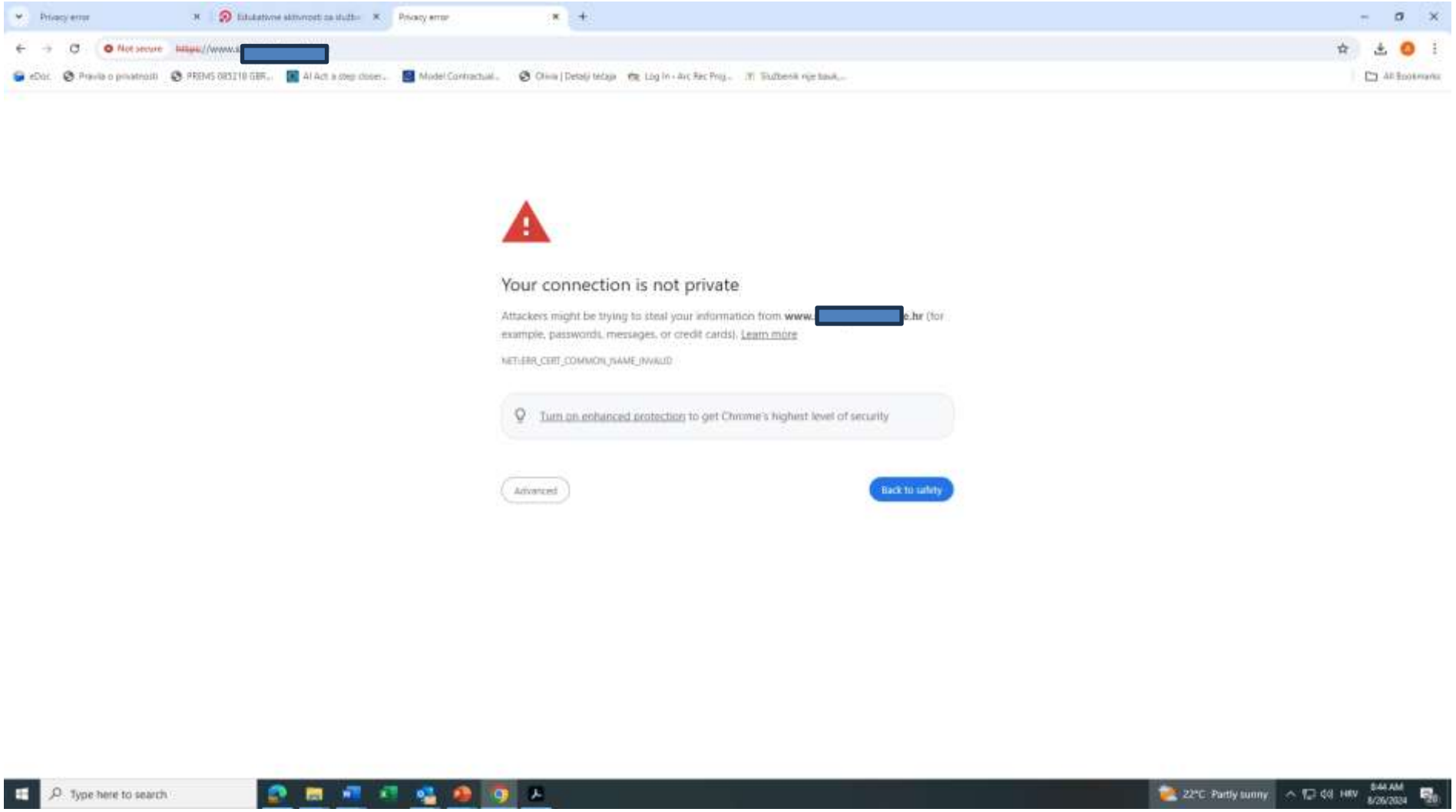
• Implementirati opcije “HttpOnly” i “secure” za sve korištene kolačiće

• Ograničiti informacije koje se vraćaju prilikom kreiranja korisničkog računa ili prilikom resetiranja lozinke, kako ne bi informirali napadača o postojanju – ili ne – računa povezanog s identifikatorom (npr. e-mail adresa).

•čuvati se najčešćih napada na web stranice navedenih u OWASP Top 10 (npr.: SQL injekcije, XSS injekcije, manipulacije URL-om).

ŠTO NE RADITI?

- Prenositi osobne podatke u URL-u (npr.: vjerodajnice, lozinke)
- Koristiti nesigurne usluge (npr.: nekriptirana autentifikacija, nekriptirani protok)
- Koristiti poslužitelje koji hostaju web stranice kao radne stanice (npr.: pregledavanje web stranica, pristup e-pošti)
- **Postavljati baze podataka na poslužitelj koji je izravno dostupan s Interneta**
- Koristiti generičke korisničke račune (tj. dijeljene između nekoliko korisnika)


Privacy error
Not secure
Your connection is not private
Attackers might be trying to steal your information from www.[redacted].hr (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_COMMON_NAME_INVALID
Turn on enhanced protection to get Chrome's highest level of security
Advanced
Back to safety
Type here to search
22°C Partly sunny
8:44 AM
8/26/2024

ZAŠTO VAM TREBA HTTPS/SSL CERTIFIKAT?

Možda mislite da niste dovoljno zanimljivi da bi bili žrtva hakerskog napada, ali ističemo da se napadi provode putem raznih zlonamjernih softvera (botova) koji automatski prolaze kroz razne web adrese i napadaju nasumično sve. Uz nedostatak SSL protokola, vaši i podaci vaših korisnika mogu vrlo lako biti kompromitirani jer takvi zlonamjerni softveri prvenstveno vrebaju slabo zaštićene stranice.

Organizacijske mjere

- ✓ Organizacijske mjere zaštite odnose se na dokumentirano uređenje unutar organizacije/društva na način da se internim aktima uredi područje zaštite osobnih podataka koje obrađujete, odnosno da se, primjerice, vodi evidencija pristupa osobnim podacima (tzv. logovi) i odredi kojim osobnim podacima zaposlenici imaju pristup prilikom obavljanja svojih poslova

- ✓ ovi interni akti ukoliko sadržavaju odgovarajuće tehničke i organizacijske mjere koje se u poduzeću doista i provode, a nisu "samo mrtvo slovo na papiru", služe kao dokaz usklađenosti s Općom uredbom o zaštiti podataka

Neki od takvih internih akata su:

• **Pravilnik o informacijskoj sigurnosti** kojim se, između ostalog, propisuju tehničke mjere zaštite koje se primjenjuju za zaštitu podataka od neovlaštenog pristupa u poslovnom subjektu.

• **Pravilnik kojim se uređuje obrada osobnih podataka (Pravilnik o obradi osobnih podataka):** propisuje tko obrađuje osobne podatke, u koju svrhu, koji je pravni temelj obrade, koji je opseg osobnih podataka u obradi, tko ima pravo pristupa i obrade osobnih podataka, koliko dugo se podaci čuvaju, koje su tehničke mjere zaštite provedene za taj sustav pohrane (bazu podataka), kako ispitanici mogu ostvariti svoja prava itd.

• **Politika pohrane podataka (može biti dio pravilnika o obradi osobnih podataka ili zasebni dokument)** osigurava provedbu više načela koja se odnose na obradu osobnih podataka uključujući ograničenje svrhe, smanjenje količine podataka i ograničenje pohrane. **Politikom pohrane podataka potrebno je odrediti koliko dugo će se osobni podaci čuvati ili, ako to nije moguće, kriterije koji se koriste za određivanje tog razdoblja**

• **Politika odgovora na incidente i plan kontinuiteta poslovanja (može biti dio Pravilnika o obradi osobnih podataka/Politike informacijske sigurnosti ili zasebni dokument)** bi trebala sadržavati upute za zaposlenike o tome koga obavijestiti o potencijalnom sigurnosnom incidentu i koje radnje mogu odmah poduzeti kako bi se spriječila daljnja šteta

• **U ugovornim klauzulama unutar ugovora o radu** može biti definirano koje sustave pohrane (baze podataka) će zaposlenik obrađivati i koja ovlaštenja će imati za obradu tih sustava pohrane (baza podataka), odnosno kojim osobnim podacima će imati pristup i kako će rukovati s tim osobnim podacima.

• **Izjavom o povjerljivosti** zaposlenik organizacije/društva ili vanjski suradnik daje pisanu izjavu da će osobne podatke obrađivati u skladu sa zakonskim odredbama o zaštiti osobnih podataka kao i da će nad istima provoditi odgovarajuće mjere zaštite te da ih neće zloupotrijebiti i davati neovlaštenim trećim stranama

• **Ugovor o obradi osobnih podataka između voditelja i izvršitelja obrade:** voditelj obrade dužan je koristiti usluge samo onih izvršitelja obrade koji daju dostatna jamstva za provedbu odgovarajućih tehničkih i organizacijskih mjera. **Kako bi to osigurali, voditelji obrade trebali bi s izvršiteljima obrade sklopiti ugovore koji sadržavaju sve elemente iz članka 28. Opće uredbe o zaštiti podataka. – modul u Oliviji I template ugovora**

Podizanje svijesti o važnosti zaštite podataka kod zaposlenika i primjena internih pravilnika u svakodnevnom poslovanju

- ✓ **Ljudski faktor je najbitniji u postupku provođenja informacijske sigurnosti i zaštite podataka i ako kod svih zaposlenika (od direktora do pomoćnog osoblja) ne postoji odgovarajuća razina svijesti o važnosti informacijske sigurnosti i odgovornosti svakog pojedinca o zaštiti podataka, sve ostale preporuke i propisane mjere zaštite neće imati puno značaja**

Od iznimne važnosti je da svi zaposlenici, bez obzira na kojoj se poslovnoj razini nalaze ("od direktora do pomoćnog osoblja"), budu svjesni:

- **koje sve osobne podatke koriste i obrađuju u svom svakodnevnom radu**
- **kojim kategorijama osobnih podataka ti podaci pripadaju,**
- **gdje se ti podaci nalaze,**
- **koji su potencijalni rizici od krađe, zlouporabe i gubitka tih podataka,**
- **na koji način te podatke mogu zaštititi,**
- **kako se to negativno može reflektirati na poslovni subjekt u kojem rade, a u krajnjoj mjeri i na njih same,**
- **da je potrebno svakodnevno se pridržavati preporučenih i propisanih mjera zaštite radi smanjenja potencijalnih rizika od neovlaštenog pristupa i zlouporabe na najmanju moguću mjeru + phishing, ransomware**

ZAGLAVLJE TVRTKE, MEMORANDUM

IZJAVA O POVJERLJIVOSTI

Ovom izjavom obvezujem se da ću sukladno propisima koji uređuju područje zaštite osobnih podataka, Uredbom (EU) 2016/679 europskog parlamenta i vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakonom o provedbi Opće uredbe o zaštiti podataka, čuvati povjerljivost svih osobnih podataka kojima imam pravo i ovlast pristupa a koji se nalaze u sustavima pohrane koje vodi tijelo/društvo u kojem sam zaposlen/a te da ću iste osobne podatke koristiti isključivo u točno određenu (propisanu) svrhu.

Također se obvezujem da osobne podatke kojima imam pravo i ovlast pristupa neću dostavljati/davati na korištenje niti na bilo koji drugi način učiniti dostupnima trećim (neovlaštenim) osobama, te se obvezujem da ću povjerljivost istih osobnih podataka čuvati i nakon prestanka ovlasti pristupa osobnim podacima.

Upoznat/a sam da bilo kakvo neovlašteno raspolaganje osobnim podacima kojima imam pravo pristupa u svojem radu predstavlja povredu radne obveze.

Datum: _____

Ime i prezime: _____

Potpis: _____

https://azop.hr/wp-content/uploads/2020/12/6-izjava_o_povjerljivosti_obrazac-1.docx

DNEVNIK.hr

STANJE NA CESTAMA

HAK još uvijek hakiran, ali postoji alternativa pomoću koje se možete informirati

Stranice Hrvatskog autokluba www.hak.hr i dalje su hakirane, sve relevantne informacije o stanju u prometu građani mogu dobiti na stranicama www.revijahak.hr, a kako se u četvrtak navodi na toj stranici promet prema moru, zbog blagdanskog produženog vikenda, je pojačan.

Piše **Hina**, 08. lipnja, 2023. @ 12:14

premium Vijesti sport 12 kultura video novac scena

ISTRAGA U EOS-U

Stručnjak otkriva kako je došlo do curenja 180.000 osobnih podataka građana, a evo i kako do naknade štete!

Stručnjak blizak istrazi otkriva da se najvjerojatnijim čini teza kako nije riječ o hakerskom upadu već trgovanju podacima

Piše: Tomislav Rukavina

DANAS.hr HRVATSKA SVIJET CRNA KRONIKA SPORT VRIJEME TV RASPORED VIDE

RADI SE NA OTKLANJANJU...

Potvrđeno za Danas.hr: Hakirana je stranica Hrvatskih voda. Sve prijavljeno policiji

— Foto: Davor Puklavec/PIXSELL/Shutterstock

Zbog hakerskog napada Hrvatske vode podnijele su kaznenu prijavu policiji

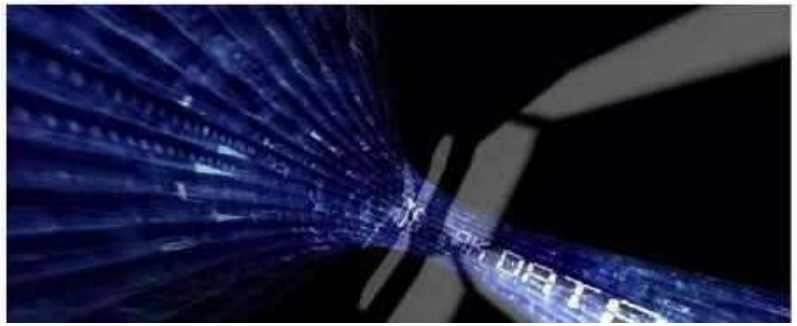
premium Vijesti sport 12 kultura video novac scena

IZ TVRTKE BZ KAPITAL

Procurili osobni podaci 77 tisuća hrvatskih građana, AZOP otvorio istragu

Došlo je do curenja baze podataka koja sadrži 77.317 redova zapisa o fizičkim osobama koje su dužnici tvrtke Bz Kapital d.o.o.

Piše: Vedran Vlarjanović



EDUCIRATI ZAPOSLENIKE O CYBER OPASNOSTIMA

1. Malware (zlonamjerni softver): programi dizajnirani da oštete ili neovlašteno pristupe računalnom sustavu ili podacima. Primjeri uključuju viruse, crve, trojance i spyware.

2. Phishing: oblik napada u kojem se korisnici lažno uvjeravaju da otkriju osobne podatke poput korisničkih imena, lozinki i kreditnih kartica.

3. Ransomware: vrsta zlonamjernog softvera koji kriptira podatke na računalu ili mreži i traži otkup za njihovo dekriptiranje.

4. Socijalni inženjering: Napadači mogu koristiti manipulaciju i obmane kako bi uvjerili ljude da otkriju osjetljive informacije ili izvrše radnje koje ugrožavaju sigurnost.

Poduzeće ima otvoren poslovni račun u jednoj banci. Na e-mail poduzeća pristigla je elektronička pošta s nazivom te banke, a u poruci je pisalo da banka moli ažuriranje nove verzije mobilnog bankarstva. Za to se trebalo prijaviti na link koji se nalazio u elektroničkoj pošti.

Ulaskom na link zatražen je korisnički broj za ulaz u mobilno bankarstvo, pin i jednokratna zaporka koja je pristigla SMS porukom s broja banke.

Zaposlenica poduzeća je otvorila zlonamjernu poruku, kliknula na poveznicu, unijela tražene podatke i s poslovnog računa poduzeća je nestalo nekoliko tisuća eura.

Posljedice needuciranosti?

Reputacijska, financijska šteta za organizaciju, moguće negativne posljedice za zaposlenike

Jučer je primljena kaznena prijava od ovlaštenog zastupnika trgovačkog društva iz Orehovice zbog počinjenoga kaznenog djela računalne prijevare. Iz prijave je vidljivo kako je s poslovnog računa spomenutoga trgovačkog društva, otvorenog u jednoj od banaka u Hrvatskoj, nepoznati počinitelj proveo nekoliko isplatnih transakcija prema inozemstvu u ukupnom iznosu od nekoliko stotina tisuća kuna, izvijestila je Policijska uprava.

Dosad provedenim kriminalističkim istraživanjem utvrđeno je kako je na službenu adresu elektroničke pošte oštećenoga trgovačkog društva primljena lažna elektronička poruka banke (tzv. phishing mail) u kojoj je otvoren poslovni račun te je zatraženo ažuriranje podataka preko dostavljene poveznice. Otvaranjem poveznice otvorena je lažna stranica banke za poslovne korisnike, a zatim su uneseni traženi podatci.

Agenciji za naplatu potraživanja EOS Matrix d.o.o. izrečena upravna novčana kazna u iznosu od 5,47 milijuna eura

lis 5, 2023

Izrečena upravna novčana kazna Zagrebačkom holdingu

RUJ 13, 2023

Upravna novčana kazna u iznosu od 15.000 eura izrečena hotelu

RUJ 26, 2023

Upravne novčane kazne zbog nezakonite obrade osobnih podataka putem kolačića

RUJ 14, 2023

Gradu Zagrebu naložene mjere vezane uz videonadzor javnih površina

SRP 5, 2023

Sportskoj kladionici izrečena upravna novčana kazna od 380.000 eura

SVI 18, 2023

Agenciji za naplatu potraživanja izrečena upravna novčana kazna u iznosu od 2,26 milijuna eura

SVI 4, 2023

Izrečena upravna novčana kazna zbog nezakonite obrade osobnih podataka

OŽU 2, 2023

Upravna novčana kazna u iznosu od 15.000 eura izrečena hotelu

Agencija za zaštitu osobnih podataka izrekla je **upravnu novčanu kaznu** u iznosu od **15.000,00 eura (113.017,50 kuna)** voditelju obrade hotelu (odnosno pravnoj osobi unutar koje posluje predmetni hotel), zbog sljedeće utvrđenih povreda Opće uredbe o zaštiti podataka**:**

- Voditelj obrade obrađivao je osobne podatke ispitanika (gostiju hotela) u **prekomjernom opsegu** i to podatke o **sigurnosnom broju bankovne kartice (CVC broj), kao i preslike osobnih dokumenata prilikom rezervacije smještaja** u hotelu putem online obrasca hotela i putem e-pošte. Za obradu CVC broja bankovne kartice i preslike osobnog dokumenta nije dokazano postojanje pravne osnove, čime je **povrijeđen članak 6. stavak 1. Opće uredbe o zaštiti podataka**. Hotel nije imao obvezu prikupljati CVC broj s bankovne kartice osoba koje su izvršile rezervaciju smještajne jedince, s obzirom na to da je rezervacija smještaja bila moguća i bez dostavljanja predmetnog podatka.
- Voditelj obrade **nije na jasan/transparentan način informirao ispitanike** o obradi njihovih osobnih

VIDEONADZOR

ZAHTJEV ZA UTVRĐIVANJE POVREDE PRAVA

IZVJEŠĆIVANJE O POVREDI OSOBNIH PODATAKA

IMENOVANJE SLUŽBENIKA ZA

1. Utvrđuje se da je nepoduzimanjem odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka od strane društva xy d.o.o. iz Zagreba, izvršitelja obrade, društva xx d.o.o., kao pravnog prednika društva__, kao voditelja obrade, protivno članku 32. stavku 1. točke b) i d) te stavku 2. Opće uredbe o zaštiti podataka, došlo do kršenja sigurnosti koje je dovelo do neovlaštene obrade osobnih podataka 28085 ispitanika.

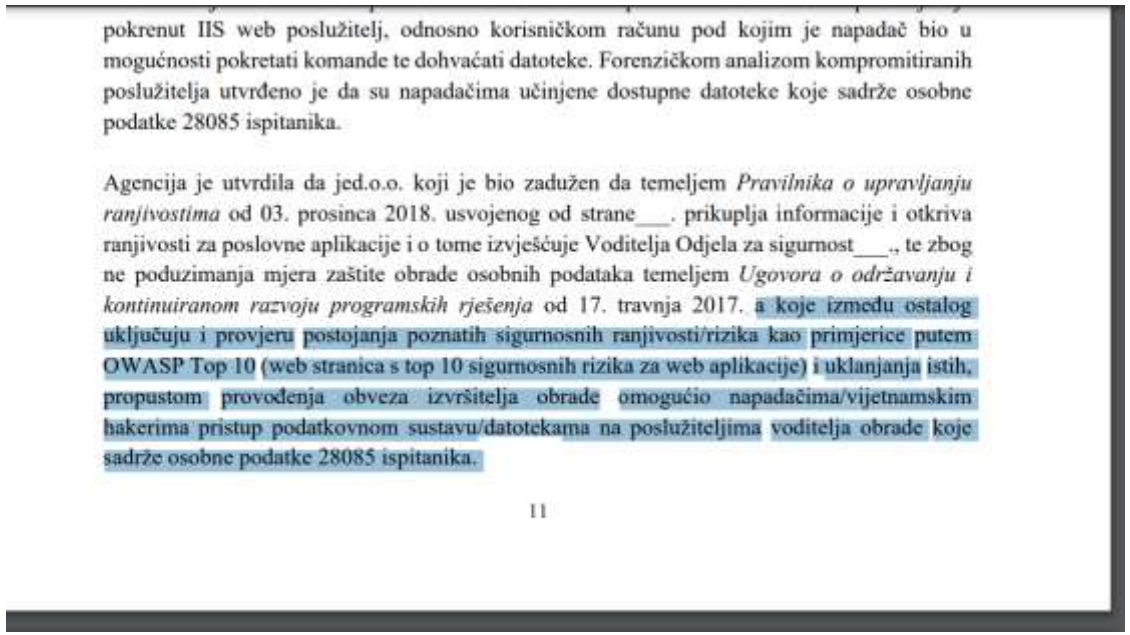
2. Za kršenje opisano u točki 1. izreke ovog rješenja, u skladu s odredbama članka 83. stavka 2. i stavka 4. točke a) Opće uredbe o zaštiti podataka, izriče se društvu xy, kao izvršitelju obrade, upravna novčana kazna u iznosu od:

230.000,00 kuna
(slovima: dvijestotinetridesettisućakuna)

Društvo xy dužno je platiti izrečenu upravnu novčanu kaznu u korist državnog proračuna u roku od 15 dana od dana pravomoćnosti ovog rješenja u korist računa broj:

HR1210010051863000160, model HR64 i poziv na broj odobrenja: 6092-25860-03401210102, s naznakom – "upravne novčane kazne koje izriče AZOP".

1



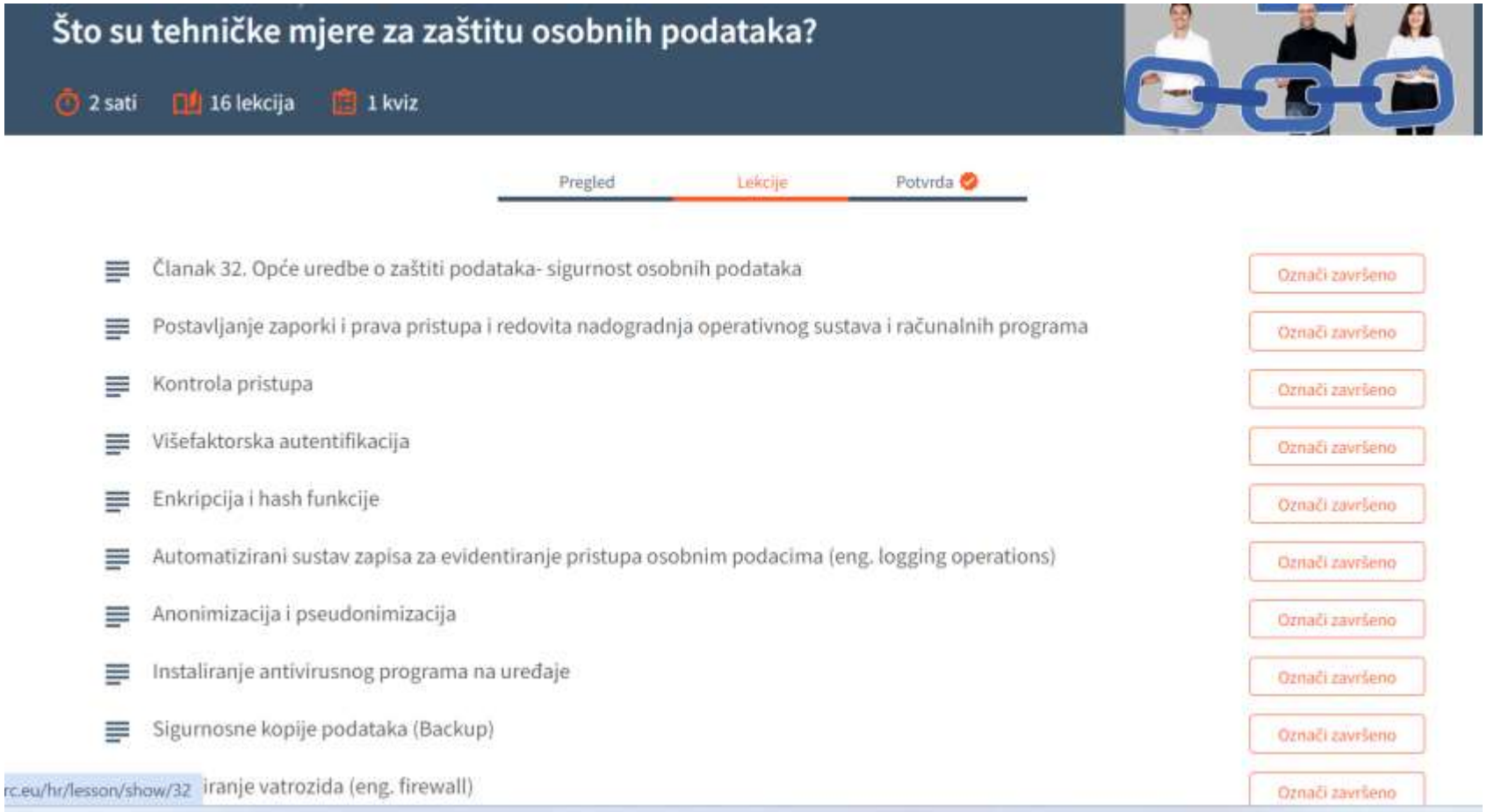
pokrenut IIS web poslužitelj, odnosno korisničkom računu pod kojim je napadač bio u mogućnosti pokretati komande te dohvaćati datoteke. Forenzičkom analizom kompromitiranih poslužitelja utvrđeno je da su napadačima učinjene dostupne datoteke koje sadrže osobne podatke 28085 ispitanika.

Agencija je utvrdila da jed.o.o. koji je bio zadužen da temeljem *Pravilnika o upravljanju ranjivostima* od 03. prosinca 2018. usvojenog od strane___. prikuplja informacije i otkriva ranjivosti za poslovne aplikacije i o tome izvješćuje Voditelja Odjela za sigurnost___., te zbog ne poduzimanja mjera zaštite obrade osobnih podataka temeljem *Ugovora o održavanju i kontinuiranom razvoju programskih rješenja* od 17. travnja 2017. a koje između ostalog uključuju i provjeru postojanja poznatih sigurnosnih ranjivosti/rizika kao primjerice putem OWASP Top 10 (web stranica s top 10 sigurnosnih rizika za web aplikacije) i uklanjanja istih, propustom provođenja obveza izvršitelja obrade omogućio napadačima/vijetnamskim hakerima pristup podatkovnom sustavu/datotekama na poslužiteljima voditelja obrade koje sadrže osobne podatke 28085 ispitanika.

11

KAŽNJEN IZVRŠITELJ OBRADE KOJI NIJE POSTUPIO PO NALOGU VODITELJA OBRADE! VAŽNOST UGOVORA VODITELJ-IZVRŠITELJ OBRADE!

KAKO MOŽE POMOĆI OLIVIA?



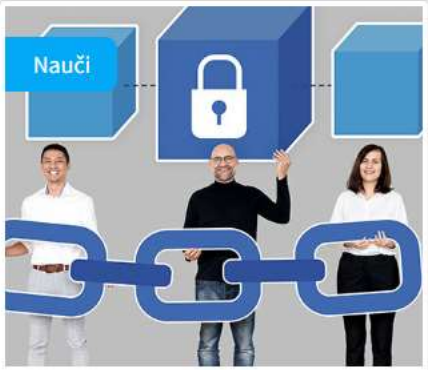
Pregled Lekcije Potvrda

Čestitke, Anamarija Bartolić!

Odradili ste sjajan posao i stoga ste nagrađeni dobro zasluženim certifikatom!

Preuzmite certifikat

Tehničke mjere



2 sati

Što su tehničke mjere za zaštitu osobnih podataka?

Detalji Lekcije

67 pitanja

Samoprocjena tehničkih mjera

Detalji Izvještaj

Popis lekcija

Tehničke mjere-video
Video

Članak 32. Opće uredbe o zaštiti podataka- sigurnost osobnih podataka
Čitanje

Postavljanje zaporki i prava pristupa i redovita nadogradnja operativnog sustava i računalnih programa
Čitanje

Kontrola pristupa
Čitanje

Višefaktorska autentifikacija
Čitanje

Enkripcija i hash funkcije
Čitanje

Automatizirani sustav zapisa za evidentiranje pristupa osobnim podacima (eng. logging operations)
Čitanje

37. Ugovorili smo usluge vanjske IT tvrtke koja brine o redovitoj nadogradnji naših IT sustava i operativnih sustava. S izvršiteljem obrade potrebno je sklopiti ugovor kojim će se izvršitelj obrade obvezati na radovito kvartalno nadograđivanje naših sustava i na redovito provjeravanje kritičnih i žurnih nadogradnji. Smatrate li ovu tvrdnju točnom?

Točan odgovor: Da

Redovita nadogradnja IT sustava i operativnih sustava od strane vanjske IT tvrtke može znatno smanjiti rizik od ranjivosti, a potrebno je razmotriti nekoliko dodatnih čimbenika kako biste osigurali sigurnost sustava, **posebno u kontekstu zero-day ranjivosti**:

Hitne nadogradnje:

- Provjerite ima li vaš ugovor s vanjskom IT tvrtkom odredbu o hitnim nadogradnjama, posebno u **slučaju otkrivanja zero-day ranjivosti. Brza reakcija na takve situacije može biti ključna za očuvanje sigurnosti.**

Pratite Informacije o ranjivostima:

- Imajte sustav praćenja informacija o najnovijim zero-day ranjivostima u IT sustavima i operativnim sustavima. To vam omogućuje brzu reakciju i dogovor s IT tvrtkom ako se pojavi relevantna ranjivost.

Upravljanje nadogradnjama treće strane:

- Ako koristite aplikacije ili softver trećih strana, provjerite ima li IT tvrtka odgovornost za njihove nadogradnje. Ranjivosti u dodatnim komponentama mogu predstavljati rizik.

Testiranje nadogradnji:

- Osigurajte da se nadogradnje prvo testiraju u kontroliranom okruženju prije nego što se primijene na produkcijske sustave kako bi se izbjegle moguće negativne posljedice.

KVIZ+ UPITNIK ZA SAMOPROCJENU

Pregled | Lekcije | Potvrda

Popis lekcija

- Tehničke mjere-video
  Video
- Članak 32. Opće uredbe o zaštiti podataka- sigurnost osobnih podataka
  Čitanje
- Postavljanje zaporki i prava pristupa i redovita nadogradnja operativnog sustava i računalnih programa
  Čitanje
- Kontrola pristupa
  Čitanje
- Višefaktorska autentifikacija
  Čitanje

4. S aspekta zaštite osobnih podataka, sasvim je u redu da se svi zaposlenici prijavljuju putem iste snažne zaporke u poslovni program s kojim rade.

Točno | Netočno

Pregled Lekcije Potvrda

5. U kontekstu zaštite osobnih podataka i sigurnosti, operativni sustav je potrebno nadograđivati iz razloga (odabrati točan odgovor):

a) Kako bi dobili najnovije pozadinske slike zaslona

b) Kako bi dobili najnovije ikone za računalne programe

c) Kako bi „zakrpali" (eng. Patch) sigurnosne propuste koje su proizvođači uočili na dosadašnjim verzijama

d) Kako bi dobili nove programe koji su sastavni dio operativnog sustava

e) Kako bi dobili najnovije opcije koje nudi operativni sustav

Organizacijske mjere za zaštitu osobnih podataka

2 sati

Organizacijske mjere za zaštitu osobnih podataka

Detalji | Potvrda

4 pitanja

Izradite Pravilnik o sustavu informacijske sigurnosti

Detalji | Izvještaj

30 pitanja

Izradite svoj Pravilnik o zaštiti osobnih podataka

Detalji | Izvještaj

Kako se uskladiti s GDPR-om i pripremiti za nadzor AZOP-a?

Primjena GDPR-a u računovodstvu

Organizacijske i tehničke mjere u GDPR-u – upravljanje pristupom i zaštita podataka

Privacy by design and by default
Kako primijeniti u praksi tehničku i integriranu zaštitu osobnih podataka?

Kako uskladiti web stranicu s GDPR-om?

Umjetna inteligencija i zaštita osobnih podataka

Sigurnost – ključ GDPR usklađenosti

GDPR – Obrada i zaštita osobnih podataka u radnim odnosima

Usklađivanje poslovnih procesa s GDPR-om: "U čemu poduzetnici najviše griješe i kako prestati griješiti?"

Zaštita osobnih podataka i usklađivanje s GDPR-om u turizmu

Kako uskladiti stranicu s GDPR-om

Kako i kada provesti procjenu učinka na zaštitu podataka?

Tehničke i organizacijske mjere za zaštitu osobnih podataka

5 godina primjene GDPR-a: problemi, rješenja, kazne i primjeri dobre prakse

OLIVIA- prezentacije

OLIVIA- webinari