Newsletter Nacionalnog CERT-a – CERT info

Sadržaj

Tema mjeseca: Sigurnosne kopije

Svake godine 31. ožujka ističemo važnost stvaranja sigurnosnih kopija svojih podataka i prisjećamo se osjećaja, gubitaka i stresa koje su nam uzrokovale situacije u kojima smo izgubili najdraže obiteljske fotografije, diplomske radove, kontakte ili važne dokumente u digitalnom obliku.

31. ožujka – Svjetski dan sigurnosnih kopija

Što je sigurnosna kopija?

Sigurnosna kopija (*engl. backup*) je pričuvna kopija podataka pohranjena na nekom drugom mjestu (drugom disku, u oblaku i sl.) koja se koristi za oporavak ako dođe do gubitka ili kompromitacije originalnog seta podataka.

O podacima može ovisiti cijelo poslovanje i vrijedi pravilo da je **„Vrijednost podataka veća je od vrijednosti uređaja!"** jer se posljedice gubitka, nedostupnosti ili oštećivanja podataka mjere u milijunima eura uz reputacijsku štetu.

Zašto je važno imati sigurnosne kopije?

Prekid poslovanja uslijed kvarova računala ili diskovnih medija, prekida opskrbe električnom energijom može dovesti do gubitka informacija. Istu posljedicu može imati i ljudska pogreška ili zlonamjerno djelovanje unutar radnog okruženja. Je li zaposlenik iz znatiželje kliknuo na poveznicu ili otvorio privitak u e-poruci kojim je preuzet zlonamjerni kôd ili je nezadovoljni zaposlenik neovlašteno pristupao podacima i dokumentima tvrtke s ciljem nanošenja štete također može značajno utjecati na daljnje poslovanje, a može se spriječiti ili umanjiti šteta postojanjem sigurnosne kopije.

Procedura izrade i brige o sigurnosnim kopijama dio je **osnova kibernetičke higijene** čijom se primjenom i pridržavanjem značajno povećava otpornost na kibernetičke napade.

Sigurnosna kopija **umanjuje štetu i učinak incidenta** u kojem je došlo do utjecaja na autentičnost, cjelovitost, dostupnost i povjerljivost informacija u sustavu što može biti posljedica prekida u radu, gubitka uređaja, kompromitacije korisničkih računa, virusa, prirodne katastrofe i drugo.

Za poslovanje i poslovne podatke je važno osigurati izradu sigurnosnih kopija kako bi se osigurao kontinuitet poslovanja, umanjile štete radi prekida u poslovanju i osigurao nastavak ključnih poslovnih aktivnosti tvrtke, institucije ili organizacije u slučajevima kibernetičkog incidenta.

Za osobne i privatne podatke važno je osigurati izradu sigurnosnih kopija jer nam naši podaci imaju određenu financijsku i emocionalnu vrijednost. U slučaju da sve pohranjujemo na jedan uređaj koji nam bude ukraden, uništen, neispravan ili nedostupan dovodimo se u situaciju da nam ti podaci više nisu dostupni ili dohvatljivi.

Što sve obuhvaća dobra praksa izrade sigurnosnih kopija?

Izrada sigurnosnih kopija uz **postupak povrata podataka** treba biti jedna od osnovnih procedura kojom se neki sustav štiti od gubitka podataka i omogućava mu brz i ispravan povrat podataka.

Uz izradu potrebno je **redovito testirati i provjeravati sigurnosne kopije**. Provjerava se ispravnost sigurnosnih kopija i pouzdanost medija na kojima se one nalaze. U slučaju da sigurnosna kopija pokazuje određene greške koje utječu na autentičnost, cjelovitost, dostupnost ili povjerljivost informacija gubi svoju namjenu.

U kojim situacijama će nam dobro doći sigurnosna kopija?

- Sigurnosna kopija omogućava povrat podataka u situacijama kada je uređaj na kojem se podaci nalaze izgubljen, oštećen ili ukraden;
- Sigurnosna kopija omogućava povrat podataka u situacijama kada su podaci postali nedostupni, oštećeni ili izmijenjeni od strane neovlaštene osobe;
- Sigurnosna kopija je najbolje rješenje kod ransomware napada kada su podaci od strane napadača šifrirani i time nedostupni, a za njihovo se „otključavanje" i dostavu dekripcijskog ključa ucjenjuje žrtvu uz traženje velikih novčanih iznosa i prijetnjama za nanošenje reputacijske štete.

Koje su najbolje prakse za izradu sigurnosnih kopija?

Strategija 3-2-1 za izradu sigurnosnih kopija

„Izradite najmanje tri kopije podataka, od čega su dvije pohranjene na istoj lokaciji, ali na različitim uređajima, a jedna na skroz drugoj lokaciji."

Preuzmi infografiku: Sigurnosne kopije – 3-2-1 - kopiraj

https://www.cert.hr/wp-content/uploads/2023/07/Sigurnosne-kopije-3-2-1-kopiraj.png

Sigurnosna kopija osigurava provedbu zakonskih obveza čuvanja financijskih i drugih sličnih podataka i izvještaja. Ovisno o propisanim rokovima za čuvanje određenih podataka definira se i **politika izrade sigurnosnih kopija**.

Danas postoje brojne mogućnosti **čuvanja sigurnosnih kopija u oblaku** i niste ograničeni samo na kopije koje se nalaze na vašem poslužitelju ili nekom drugom uređaju već su vam podaci dostupni i u vašem rezerviranom i zaštićenom oblaku.

Prilikom procesa izrade sigurnosnih kopija pažnju je potrebno posvetiti i **smještaju podataka**. Naime, podaci se mogu spremati na lokalnom računalu i na udaljenom računalu koji služi kao datotečni poslužitelj ili na nekim prenosivim medijima.

Koji je proces izrade sigurnosnih kopija?

Sam proces izrade sigurnosnih kopija odvija se u nekoliko faza:

1) identifikacija podataka,
2) određivanje prikladnog medija,
3) označavanje sigurnosnih kopija,
4) čuvanje sigurnosnih kopija,
5) smještaj sigurnosnih kopija,
6) testiranje sigurnosnih kopija.

Lista za provjeru:

- jesu li adekvatno i sustavno izrađene sigurnosne kopije svih podataka, operativnog sustava i pomoćnih programa?
- postoje li zapisi o sadržaju sigurnosnih kopija i njihovom smještaju?
- postoje li zapisi o licenciranim aplikacijama?
- postoje li kopije medija ili zapisa spremljene na udaljenoj lokaciji?
- provodi li se povremeno postupak vraćanja podataka s medija?
- može li novi hardver čitati podatke s postojećih medija?
- hoće li se zbog postojećih licenci aplikacija pokretati na novom hardveru?
- je li proveden postupak potpunog vraćanja podataka u određenom vremenskom periodu?

Vrste medija za pohranu sigurnosnih kopija

Svaka vrsta medija ima svoje prednosti, ovisno o čimbenicima poput cijene, kapaciteta, sigurnosti, brzine i trajnosti.

Vanjski diskovi (HDD i SSD) – veliki kapacitet pohrane, pristupačne cijene i jednostavnost korištenja.

USB stickovi – prijenosni i praktični za manje sigurnosne kopije zbog manjeg kapaciteta.

Mrežna pohrana (NAS - Network Attached Storage) – centralizirano rješenje za sigurnosne kopije više uređaja, često korišteno u tvrtkama i kućnim mrežama.

Pohrana u oblaku – usluge poput Google Drive-a, Dropbox-a, OneDrive-a i AWS-a omogućuju udaljenu pohranu s visokom razinom sigurnosti i dostupnosti.

Optički diskovi (CD, DVD, Blu-ray) – Rjeđe korišteni, ali i dalje pogodni za dugotrajnu arhivu podataka.

Magnetna traka (LTO traka) – česta u poslovnim okruženjima zbog pouzdanosti i isplativosti za velike količine podataka.

RAID sustavi – redundantni nizovi neovisnih diskova pružaju zaštitu od kvarova diskova i osiguravaju sigurnost podataka.

Memorijske kartice (SD kartice, MicroSD) – koriste se za manje sigurnosne kopije, posebno u mobilnim uređajima i kamerama.

Hibridna rješenja za pohranu – kombinacija lokalne i cloud pohrane za ravnotežu između sigurnosti i dostupnosti.

Svaki korisnik sam za sebe treba donijeti odluku o tome koji su mu podaci važni i za koje podatke je potrebno izrađivati sigurnosne kopije. Organizacije koje se odluče na izradu sigurnosnih kopija mogu se susresti s nekoliko poteškoća u samom procesu kao što su visoka cijena izrade i čuvanja sigurnosnih kopija, nedostatak znanja za izradu sigurnosnih kopija ili otpor samih zaposlenika. Ipak, ovi čimbenici su zanemarivi u odnosu na mogućnost prekida poslovanja i propadanja organizacije u slučaju gubitka podataka.

Više informacija o sigurnosnim kopijama možete pronaći na:

https://www.cert.hr/svjetski-dan-sigurnosnih-kopija-ili-world-back-up-day/ - Svjetski dan sigurnosnih kopija ili World Back-up Day

https://www.cert.hr/NCosSigCop - Osnove sigurnosnih kopija

https://www.cert.hr/kibhig - Kibernetička higijena - osnovna sigurnosna zaštita

https://www.cert.hr/savjeti-za-povecanje-otpornosti-na-kiberneticke-napade/ - Savjeti za povećanje otpornosti na kibernetičke napade

Digitalni sadržaji o temi mjeseca

Osnove sigurnosnih kopija - dokument

3-2-1 kopiraj - poster

Data Backup Options – US CERT document

Konferencija „ConCERT“

U Zagrebu, 20. veljače 2025., održana je druga ConCERT konferencija u organizaciji CARNET-ovog Nacionalnog CERT-a. Na konferenciji se okupilo više od 200 stručnjaka iz Hrvatske i Slovenije, koji su razmijenili iskustva i znanja u borbi s kibernetičkim prijetnjama i najboljih odgovora i postupanja uslijed pojave kibernetičkih incidenata.

Odaziv je pokazatelj povećane svijesti o važnosti zaštite kibernetičkog prostora, otpornosti poslovanja na prijetnje i bržeg odgovora na kibernetičke incidente. Povećana svijest o sigurnosti mrežnih i informacijskih struktura, potaknuta novim zakonodavstvom i sofisticiranim prijetnjama, ojačava suradnju stručnjaka i njihovu međusobnu razmjenu znanja. ConCERT je postao ključni događaj za stvaranje zajednice povjerenja u kojoj stručnjaci dijele iskustva i rješenja za izazove u svojoj praksi, s ciljem prevencije napada koji ugrožavaju kritičnu infrastrukturu i gospodarstvo.

Konferenciju je otvorila **Nataša Glavor**, pomoćnica ravnatelja CARNET-a za Nacionalni CERT, koja je istaknula ključnu ulogu suradnje svih sektora u stvaranju sigurnog i otpornog digitalnog prostora.

> *“Kibernetički prostor mijenja se brže nego ikada, a izazovi zahtijevaju suradnju svih nas. Upravo zato je ova konferencija izuzetno važna – pruža prostor za otvorenu diskusiju, povezivanje i dijeljenje iskustava u povjerljivom okruženju.”*
>
> *Nataša Glavor*

U sklopu događanja, sudionici su imali priliku čuti predavanja predstavnika iz javnog i privatnog sektora, koji su analizirali sve od ransomware napada do izazova s kojim se suočavaju u otkrivanju počinitelja kibernetičkih kaznenih djela.

Vlatka Marčan iz **Nacionalnog koordinacijskog središta za industriju, tehnologiju i istraživanje u području kibernetičke sigurnosti (NKS)** detaljno je predstavila rad NKS-a, njegove korisnike i zadatke. NKS je, kako je istaknula, angažiran na četiri ključna područja uključujući uspostavu Zajednice stručnjaka i suradnju s drugim NKS-ovima putem Mreže, edukaciju te financijsku potporu u okviru EU natječaja. Naglasila je važnost suradnje u prekograničnim projektima i promociji rada Mreže i Zajednice, uključujući i Europski centar za kibernetičku sigurnost – ECCC.

Stručnjaci iz **Nacionalnog centra za kibernetičku sigurnost** podijelili su svoja iskustva i znanja o modernim ransomware napadima, objašnjavajući kako oni funkcioniraju na tehničkoj razini, koje korake napadači poduzimaju te kako se možemo zaštititi. Istaknuli su zabrinjavajuću činjenicu kako napadačima, od trenutka kada uđu u mrežu, do ostvarivanja potpunih administratorskih ovlasti, često ne treba više od 24 sata. Naglasili su kako je ključno uspostaviti adekvatne mjere zaštite i detekcije, no ulaganje u skupe alate samo po sebi nije dovoljno za osiguranje sustava.

Ivan Birtić, suradnik za računalnu sigurnost u **CARNET-ovom Sektoru za Nacionalni CERT**, prenio je svoje iskustvo s testiranjem sigurnosti web aplikacija te koje su njihove najčešće ranjivosti. Naglasio je kako se najčešće susreću s neažuriranim sustavima, ranjivostima autentifikacije, autorizacije te inercijom ranjivih strana za otklanjanje ranjivosti. Svima koji žele svoje aplikacije učiniti sigurnijima poručuje da je potrebno razmišljati kao napadač.

Renato Grgurić i **Dragan Marić** iz **Službe kibernetičke sigurnosti Ministarstva unutarnjih poslova** govorili su o tome tko su najčešći počinitelji kibernetičkih napada i koji su glavni izazovi u njihovom pronalaženju. Istaknuli su kako otkrivanje počinitelja može biti zahtjevan proces zbog različitih pravnih regulacija, nedostupnosti podataka, anonimiziranja identiteta počinitelja te stalnog razvoja novih metoda napada, ali i nespremnosti određenih država na suradnju. Prikazali su i primjer uspješne akcije u kojoj je sudjelovala Služba kibernetičke sigurnosti u suradnji s drugim europskim tijelima.

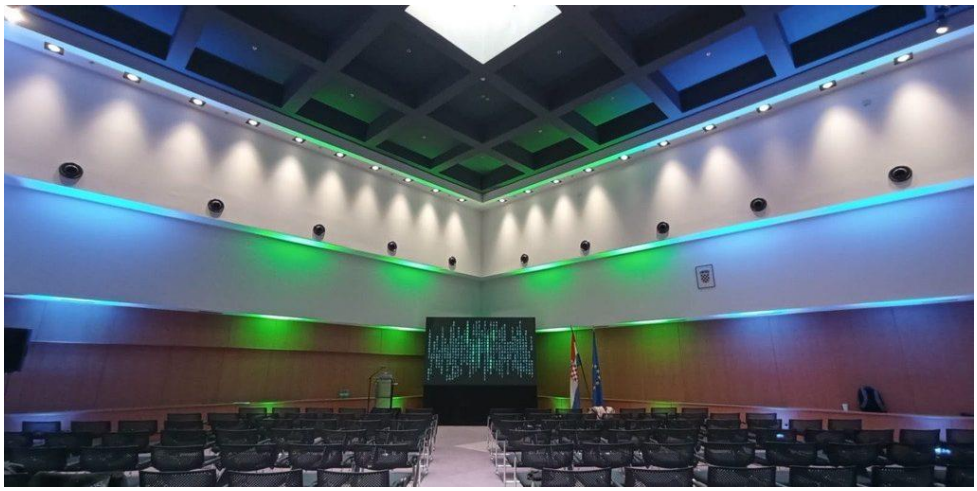
Neven Zitek iz **SPAN**-a je predstavio aktualnu sliku kibernetičkog okruženja i skrenuo pozornost na očekivane trendove i prijetnje u 2025. godini. Naveo je kako su ransomware napadi financijski motivirani, a da je za čak 68% kompromitacija i dalje kriv ljudski faktor i nenamjerno maliciozno ponašanje djelatnika. Za 2025. godinu predviđa porast postojećih prijetnji, uključujući ransomware napade, napade pod pokroviteljstvom država, kibernetičke napade vođene umjetnom inteligencijom, iskorištavanje IoT uređaja, a promjenu će donijeti i razvoj kvantnih računala.

Gorazd Božić iz **slovenskog nacionalnog CERT-a** podijelio je podatke o prijetnjama s kojima se Slovenija suočava. Osvrnuo se na drastičan porast obrađenih kibernetičkih incidenata, koji je od 2008. godine porastao za više od 1300%, s 325 na 4668 prijavljenih incidenata do 2024. godine. Najveće financijske gubitke uzrokuju investicijske prijevare, dok se mobiteli sve više koriste kao vektori napada. Također, naglasio je rastuću sofisticiranost socijalnog inženjeringa, koji je potpomognut upotrebom alata baziranih na umjetnoj inteligenciji.

Vanja Švajcer, sigurnosni stručnjak s dugogodišnjim iskustvom, govorio je o zlonamjernim grupama čiji je cilj ostvarivanje financijske koristi. Jedna od taktika koju koriste ove grupe je stvaranje lažnih zaposlenika i agenata za zapošljavanje kako bi preuzeli identitete stvarnih softverskih inženjera i stekli pristup osjetljivim podacima putem kompromitiranih korisničkih računa. Švajcer je također upozorio na opasnosti koje nose video intervjui, gdje se često koriste lažni identiteti. Za kraj, dao je preporuke za zaštitu od takvih napada.

Mislav Major iz **INFIGO IS**-a pružio je uvid u rad Red Teama, specijalizirane skupine koja simulira napade na organizacije kako bi otkrila sigurnosne ranjivosti. Naglasio je važnost multidisciplinarnog pristupa, jer je za učinkovito testiranje sigurnosnih sustava potrebno imati stručnjake s različitim znanjima. Svako testiranje od strane Red Teama, kako je objasnio, osnažuje infrastrukturu organizacije, omogućava implementaciju novih zaštita, te ispravljanje ranjivosti i miskonfiguracija.

Vlatko Košturjak iz **Diverta, Marlink grupacije**, trenutačni CRO (*Chief Research Officer*) govorio je o korištenju umjetne inteligencije u pisanju kôda i izradi aplikacija. Takve metode mogu dovesti do ranjivosti u aplikacijama koje mogu iskoristiti napadači. Košturjak je upozorio da su zlonamjerne skupine već počele koristiti ovu tehnologiju, pa je važno da se ne odustane od tradicionalnih metoda testiranja aplikacija kako bi se spriječile sigurnosne prijetnje.



Statistika obrađenih incidenata – veljača 2025.

Prema dostupnim statistikama Nacionalnog CERT-a za veljaču 2025. godine vidljivo je kako je najveći broj prijavljenih i obrađenih incidenata u kategoriji *„phishing napad"*.

Phishing napad	28	24%
Neželjene poruke	21	18%
Ostale vrste financijski motiviranih prijevara	20	17%
Napadačka infrastruktura	12	10%
Neovlaštena izmjena sadržaja	8	7%
Pogađanje pristupnih podataka	8	7%
Ispad usluge	5	4%
Ostalo	4	3%
Kompromitirani uređaj	3	3%
Poslovne prijevare	3	3%
Krađa pristupnih podataka	2	2%
Pokušaj iskorištavanja ranjivosti	1	1
Uskraćivanje usluge	1	1%
Ukupno	**116**	

Najava događanja

31. 3. – Dan sigurnosnih kopija

9.4. – 11.4.2025. - CUC 2025. „Od inspiracije do akcije"

Prethodni brojevi

Newsletter Nacionalnog CERT-a – CERT info - siječanj 2025.

Newsletter Nacionalnog CERT-a – CERT info - veljača 2025.