METODE ZAŠTITE OD GUBITKA I KRAĐE PODATAKA

Ljevaković, Kristian

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Kristian Ljevaković

METODE ZAŠTITE OD GUBITKA I KRAĐE PODATAKA

ZAVRŠNI RAD

Karlovac, 2021.

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate study of Safety and Protection

Kristian Ljevaković

METHODS OF PROTECTION AGAINST DATA LOSS AND THEFT

Final paper

Karlovac, 2021.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Kristian Ljevaković

METODE ZAŠTITE OD GUBITKA I KRAĐE PODATAKA

ZAVRŠNI RAD

Mentor: dr.sc. Damir Kralj, prof. v. š.

Karlovac, 2021.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Specijalistički diplomski stručni studij sigurnosti i zaštite

Usmjerenje: Zaštita na radu Karlovac, 24.02.2021.

ZADATAK ZAVRŠNOG RADA

Student: Kristian Ljevaković Matični broj: 0422418016

Naslov: Metode zaštite od gubitka i krađe podataka

Opis zadatka:

- na osnovi dostupnih izvora te vlastitih iskustava i saznanja stečenih kroz školovanje i praksu, ukratko analizirati važnost zaštite podataka u domeni evidencija po ZNR u svakodnevnoj upotrebi, a pogotovo u delikatnim djelatnostima od posebnog značaja (oružane snage, procesna postrojenja, energane, proizvodnja eksploziva i streljiva, banke i druge financijske ustanove i sl.);
- okvirno analizirati regulatorni dio tj. istražiti zakone koji obrađuju područje zaštite podataka i obaveze pravnih osoba u poduzimanju potrebnih mjera i radnji, kako kod nas tako i u EU regulativi (direktivama) uz isticanje razlika što znači gubitak, a što krađa podataka;
- u eksperimentalnom dijelu rada, na osnovi prethodnih teorijskih analiza i iskustava stečenih kroz praktičnu produkcijsku evaluaciju, dati tehnološki opis i procjenu mjera prevencije i sanacije stanja za pojedini ovakav scenarij, a sukladno mogućnostima dati i neke konkretne dostupne slučajeve i primjere iz prakse.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
24.02.2021.	15.04.2021.	23.04.2021.

Mentor: Predsjednik Ispitnog povjerenstva:

dr.sc. Damir Kralj, prof. v. š. dr.sc. Vladimir Tudić, prof.v.š.

PREDGOVOR

Izjavljujem da sam rad napisao samostalno koristeći se znanjem stečenim kroz studiranje te navedenom literaturom.

Zahvaljujem se mentoru dr.sc. Damiru Kralju, prof. v. š. na svim savjetima i pomoći tijekom izrade ovog Završnog rada.

Također se želim zahvaliti svojim roditeljima koji su mi pružili mogućnost studiranja na Veleučilištu u Karlovcu.

SAŽETAK

Zaštita podataka bitna je u domeni evidencija zaštite na radu, a posebice u djelatnostima od posebnog značaja kao što su: oružane snage, procesna postrojenja, energane, proizvodnja eksploziva i streljiva, banke i druge financijske ustanove i drugo. Zaštita podataka od gubitka i krađe posebno je bitno tamo gdje osim problema u konzistenciji i poslovnoj povjerljivosti podataka, postoj posebne opasnosti po zdravlje i život radnika, moguće velike materijalne štete uključujući i teroristička djelovanja.

Zaštita podataka je proces kojim se osigurava podatke od oštećenja pri prijenosu i kontrolira pristup podacima u računalu. Kako bi podatci na svoje odredište stigli netaknuti i u istom obliku u kojem su poslani, podatke zaštićujemo od oštećenja u prijenosu i neovlaštenih upada ili preusmjeravanja tijekom prijenosa.

Ključne riječi: zaštita podataka, oporavak podataka, enkripcija, antivirus, vatrozid, protokoli za zaštitu, kibernetički napadi, hakeri, energetski sektor

SUMMARY

Data protection is important in the field of occupational safety records, and especially in activities of special importance such as: the armed forces, process plants, power plants, production of explosives and ammunition, banks and other financial institutions and others. Protection of data against loss and theft is especially important where, in addition to problems in the consistency and business confidentiality of data, there is a special danger to the health and life of workers, possible major material damage, including terrorist acts.

Data protection is a process of securing data in transmission and controlling access to data in the computer. In order for your destination data to arrive intact and in the same form in which it was sent, the data is protected from damage in transmission and unauthorized intrusions or diversions during transmission.

Keywords: data protection, data recovery, encryption, antivirus, firewall, security protocols, cyber-attacks, hackers, energy sector

Sadržaj

1. UVOD

Zaštita podataka je proces kojim se osigurava digitalne podataka od neovlaštenog pristupa, gubitka ili krađe tijekom cijelog njihovog životnog ciklusa. To je koncept koji obuhvaća svaki aspekt informacijske sigurnosti, od fizičke sigurnosti hardvera i uređaja za pohranu do administrativnih i kontrolnih pristupa, kao i logičku sigurnost softverskih aplikacija. Također uključuje organizacijske politike i postupke.

Kada se pravilno primijene, strategije zaštite podataka zaštititi će informacijsku imovinu organizacije od kibernetičkih kriminalnih aktivnosti, ali također štite i od prijetnji iznutra i ljudskih pogrešaka, što i danas ostaje među vodećim uzrocima proboja podataka. Sigurnost podataka uključuje upotrebu alata i tehnologija koji poboljšavaju sposobnost organizacije da prepozna gdje se nalaze njezini kritični podaci i kako se koriste. U idealnom slučaju ti bi alati trebali biti u mogućnosti primijeniti zaštitu poput enkripcije, maskiranja podataka i obrade osjetljivih datoteka te bi trebali automatizirati izvještavanje radi pojednostavljenja revizija i pridržavanja regulatornih zahtjeva. [1]

Nepravilno rukovanje podacima, što uključuje brisanje i prepisivanje datoteka, također donosi veliki dio rizika gubitaka informacija. Zbog važnosti izgubljenih podataka razvijene su razne tehnike obnove podataka za svaki od navedenih tipova oštećenja. [2]

Zaštita podataka bitan je čimbenik zaštite na radu, osobito u energetskom sektoru, jer gubitkom podataka može doći do gašenja cijelog sustava i neočekivanih posljedica u postrojenjima za proizvodnju energije, posebice nuklearnim postrojenjima. Svi sustavi moraju imati dodatne izvore napajanja u slučaju nestanka struje, a sustave je potrebno zaštiti i od neovlaštenog pristupa. Neovlašteni pristup može rezultirati krađom i/ili brisanjem podataka. Kibernetički napadi na energetski sektor nisu rijetkost, ali uspješni kibernetički napadi sa velikim posljedicama jesu. Europska unija ima za cilj osigurati energetske sustave koji pružaju osnovne usluge europskom društvu, zaštitu podatke u energetskim sustavima i privatnost europskog građanina.

Podaci iz zapisa s područja zaštite na radu često sadržavaju i osobne podatke radnika. Državne institucije i javne ustanove moraju na zahtjev tijela državne uprave osigurati dostupnost podataka s područja zaštite na radu, a pri tome moraju voditi brigu o zakonu i propisima o zaštiti osobnih podataka.

Cilj ovog rada je na osnovu analiziranih dostupnih podataka i stečenog znanja ukazati na važnost zaštite podataka od gubitka i krađe, osobito u djelatnostima od posebnog značaja kao što su energetska postrojenja, te upoznati se s metodama obnavljanja izgubljenih podataka i zaštitom sustava od proboja podataka. Također, važno je i upoznati se sa zakonskom regulativom u Republici Hrvatskoj i Europskoj uniji te primjerima slučajeva krađe podataka.

Glavna metoda za pisanje ovog rada bila je istraživanje i analiza dostupnih pisanih i mrežnih izvora koji sadrže i obrađuju metode zaštite podataka i zakonsku regulativu, ali i moje vlastito iskustvo u zaštiti, čuvanju te obnavljanju izgubljenih podataka.

2. PODACI

Podatak (eng. *data*) je skup entiteta koji sadrži opis nekog događaja, zapažanja ili činjenice. Element podatka može biti broj, riječ, slika ili neki drugi proizvoljan zapis. Ukoliko podatak predstavlja činjenicu za koju je utvrđeno da neosporno vrijedi, tada podatak predstavlja informaciju. Razlika između pojmova podatak i informacija prilično je jasna nakon formalne definicije. Ipak, distinkcija na prvi pogled nije tako očita i nerijetko je kod ljudi prisutna konfuzija u razumijevanju tih pojmova.

Odnos između podatka i informacije može se opisati na sljedeći način: svaka informacija je podatak, ali svaki podatak nije informacija. Sirovim podacima nazivaju se brojevi, znakovi, slike ili ostali izlazi iz uređaja koji pretvaraju fizičke veličine u simbole, u širem smislu riječi. Izraz „sirovi podaci“ je termin relativnog značenja jer se obrada podataka najčešće događa u nekoliko faza gdje se obrađeni podaci iz jedne faze mogu smatrati sirovim podacima za sljedeću. Mehanički uređaji za računanje klasificirani su prema načinu na koji zapisuju podatak. Analogna računala predstavljaju podatke kao što su: napon, udaljenost, položaj ili neku drugu fizikalnu veličinu.

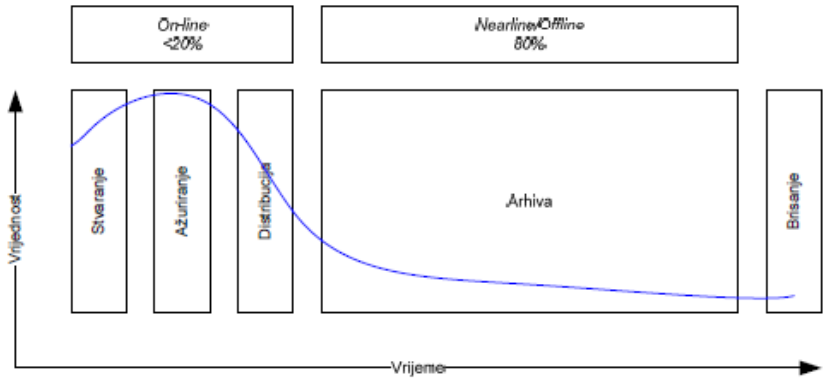
Digitalna računala predstavljaju podatke kao nizove simbola uzete iz brojevnog sustava. Najčešće se u digitalnim računalima koristi binarni sustav. Binarni sustav se sastoji od dva znaka, '0' i '1'. Binarnim se sustavom mogu konstruirati simboli više razine poput slova ili brojeva. Postoje različiti oblici podataka, a većina ih se da sustavno podijeliti na logičke i suvislo odvojene cjeline. [3]

2.1. Upravljanje životnim ciklusom podataka i informacija

Među podacima razlučuju se aktivni i neaktivni podaci, odnosno informacije. Životni ciklus podataka počinje njihovim prikupljanjem. Aktivni podaci označavaju podatke koji se upotrebljavaju svakodnevno u uobičajenim poslovnim procesima korisnika. S vremenom ti podaci gube svoju važnost. Učestalost pristupa opada uz postupno gubljenje poslovne vrijednosti pa informacije svoj životni vijek konačno završavaju arhiviranjem ili njihovim odlaganjem.

2.1.1. Aktivni podaci

Aktivni podaci nose poslovnu korist organizaciji, poduzeću, odnosno korisniku. Svaki uspješan i efikasan poslovni proces zahtjeva jednostavan i neometan pristup aktivnim podacima. Upravljanje podacima temelji se na vrlo jednostavnom načelu: prijenosu podatka iz sloja u sloj kroz vrijeme (Slika 1.). Razumijevanjem načina na koji se podaci prenose, odnosno zadržavaju u pojedinom sloju korisnici razvijaju strategije i obrasce korištenja kako bi optimirali upotrebu medija za pohranu. Na taj se način optimira ukupna cijena spremanja podataka tijekom njihova životnog ciklusa. Sličan, ali složeniji, pristup primjenjuje se kod pohrane podataka u relacijsku bazu podataka. Kompleksnost u ovom slučaju povećava inherentna međuzavisnost podataka. Relacijske baze podataka jedni su od čestih i velikih korisnika prostora za pohranu podataka, a ujedno su, zbog prirode korištenja, jedan od najsloženijih mehanizama pristupa podacima. Složenost upravljanja relacijskim bazama podataka čini upravo ta međuzavisnost podataka. Zbog toga je vrlo važno razviti efikasne mehanizme upravljanja kako baza ne bi izašla van granica nadzora. U protivnom bi svaki dohvat podataka iz baze postajao sve skuplji što bi u konačnici rezultiralo lošim performansama čitavog sustava. [3]



Slika 1. Vremenski tok podataka [3]

2.1.2. Neaktivni podaci

Nakon što podaci više nisu potrebni za poslovni proces korisnika, oni postaju neaktivni. Ipak, to ne znači da su i nepotrebni te da ih se može izbrisati s medija na kojemu su pohranjeni. U devedesetim godinama i prije, za pohranu neaktivnih podataka koristili su se mikrofilmovi i trake.

Pojam upravljanje životnim ciklusom odnosi se na koordiniranje prolaskom informacija kroz informacijski sustav; od njihova nastanka i inicijalne pohrane sve do trenutka kada isti podaci postaju nepotrebni i slijedi im brisanje. Ovakvi sustavi automatiziraju procese uključene u upravljanje podacima, a radi se o organizaciji podataka u međusobno odvojene slojeve temeljenoj na unaprijed određenim pravilima te automatizaciji prijenosa podataka iz jednog sloja u drugi, temeljenoj također na uspostavljenim pravilima. Primjer pravila može se ilustrirati situacijom kada se podaci kojima se češće pristupa spremaju na skuplje, ali i brže medije, dok se podaci s manjim značajem spremaju na jeftinije i sporije medije.

Izraz upravljanje životnim ciklusom informacija nije identičan upravljanju ciklusom podataka, iako se nerijetko ta dva pojma koriste ravnopravno. Sustavi orijentirani na podatke koriste atribute datoteka (vrstu, veličinu, datum nastanka, uređivanja i sl.) za dohvat podataka na zahtjev korisnika. Sustavi temeljeni na upravljanju informacijama uvelike su složeniji i omogućavaju pretragu, odnosno dohvat podataka korištenjem složenih upita poput konkretnih vrijednosti pojedinih parametara spremljenih u datotekama. Hijerarhijsko upravljanje pohranom jedan je od mogućih načina upravljanja podacima. Radi se o tehnici koja omogućuje automatski prijenos podataka između medija različitog cjenovnog ranga. Razlog potrebi za takvim upravljanjem je prvenstveno u cijeni uređaja za pohranu. Očito je kako bi najjednostavnije i najefikasnije rješenje bilo korištenje uređaja visokih performansi. Ipak, cijena je ta koja uvjetuje korištenje uređaja lošijih karakteristika. [3]

3. VRSTE GUBITAKA PODATAKA

3.1. Fizička oštećenja

Širok raspon pogrešaka može izazvati fizičko oštećenje medija za pohranu. CD/DVD mediji mogu imati izgrebenu podlogu, tvrdi disk može biti oštećen prilikom pada, a trake za pohranu mogu jednostavno puknuti. Ipak, kao jedan od najčešćih problema u računalima javlja se oštećenje tvrdog diska glavom za čitanje/pisanje.

Fizičko oštećenje (Slika 1.) uvijek uzrokuje neki gubitak podataka, a u većini slučajeva ima za posljedicu i oštećenje datotečnog sustava. [2]

Slika 2. Uništeni tvrdi disk [2]

3.2. Logičke greške

Osnovni uzroci logičkih pogrešaka su:

- gubitak napajanja koji sprječava zapis struktura datotečnog sustava na medij,
- problemi sa sklopovljem i upravljačkim programima i
- rušenje sustava.

Rezultat bilo koje logičke pogreške je dovođenje sustava u nekonzistentno stanje što može uzrokovati razne probleme, poput:

- neočekivanog ponašanja (npr. upravljački programi prijavljuju negativnu vrijednost slobodnog
- prostora),
- rušenja sustava i
- gubitak podataka.

Postoje razni programi za ispravak spomenutih stanja, a svi operacijski sustavi sadrže barem osnovni alat za popravak datotečnog sustava. Primjeri uključeni u poznatije operacijske sustave su:

- „fsck“ korisnički program za „Linux“ platforme,
- „Disk Utility“ program namijenjen „Mac OS X“ okruženju i
- „chkdsk“ program za „Microsoft Windows“ platforme. [2]

3.3. Obrisani podaci

Brisanje podataka je metoda prepisivanja podataka kojom se u potpunosti uklanjanju svi elektronički zapisi podataka na tvrdom disku ili drugom digitalnom mediju. Trajno brisanje podataka nije isto što i osnovno brisanje datoteka. Postoje metode koje omogućuju potpuno uklanjanje podataka poput demagnetiziranja i fizičkog uništavanja diska.

Postoje tri razine uklanjanja podataka:

1. Čišćenje osjetljivih informacija – uklanjanje osjetljivih podataka s uređaja za pohranu na takav način da je korisnik siguran kako izbrisane podatke nije moguće rekonstruirati uporabom raznih funkcija sustava ili programa za obnovu podataka. Ipak, podatke je još uvijek moguće obnoviti uporabom nekih specijaliziranih laboratorijskih tehnologija. Obično se koristi kao administrativna zaštita protiv slučajnog otkrivanja podataka u organizacijama.

2. Potpuno čišćenje – uklanjanje osjetljivih podataka sa sustava ili uređaja za pohranu s namjerom da se ne mogu rekonstruirati nikakvim poznatim tehnikama. Obično se obavlja prije otpuštanja medija izvan kontrole firme, kao što je odbacivanje medija ili premještaj u drugo sigurnosno okruženje.
3. Uništavanje – fizičko uništavanje medija spaljivanjem, taljenjem, mljevenjem, bušenjem ili na neki drugi način kako bi se spriječila obnova podataka.

Jedna od metoda brisanja podataka je njihovo prepisivanje novim podacima. Kod najjednostavnijeg oblika prepisivanja pohranjenih podataka zapisuju se neki podaci (obično uzorci nula) po svim sektorima diska, što pruža zaštitu od čitanja podataka s medija uporabom osnovnih funkcija sustava. Kako bi se izbrisali svi tragovi podataka te onemogućila uporaba tehnika obnove podataka, treba se koristiti neki složeniji uzorak (npr. uzorak nula i jedinica). [2]

4. METODE OPORAVKA PODATAKA

4.1. Oporavak od fizičkog oštećenja

Obnova podataka nakon fizičkog oštećenja može uključivati raznovrsne tehnike. Neka oštećenja mogu biti ispravljena zamjenom dijelova tvrdog diska. Iako ovaj postupak može omogućiti rad diska, ne isključuje postojanje logičkih pogrešaka. Posebna procedura izrade slike diska koristi se za obnovu svakog bita koji je moguće pročitati s površine diska. Jednom kada je slika dobivena i spremljena na medij, može biti detaljno analizirana kako bi se rekonstruirali izvorni podaci. [2]

Primjeri procedura za oporavak od fizičkog oštećenja su:

- Otklanjanje ugroženih tiskanih pločica (eng. *printed circuit board*, PCB) komponenti (Slika 2.) te njihova zamjena s ispravnim dijelovima,
- Montiranje glave za pisanje/čitanje s obzirom na neoštećeni disk,
- Uklanjanje oštećenih dijelova diska i njihova zamjena novim.

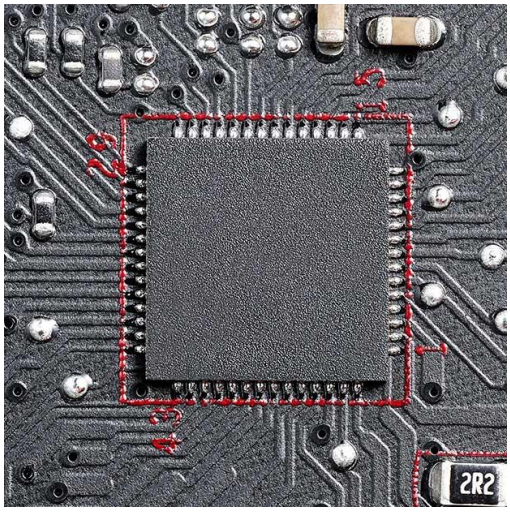
Najčešće se koristi kombinacija svih navedenih procesa. [2]

Hakiranje tiskanih pločica (Slika 3.) znači tajno dodavanje mnogo malih komponenata na tiskanoj pločici i preuzimanje kontrole nad određenim sabirnicama podataka. Dizajneri tiskanih pločica započinju stvaranjem dva elektronička dokumenta, sheme i rasporeda (eng. *layout*). Shema opisuje sve komponente i kako su međusobno povezane. Raspored prikazuje gotovu ploču i predmete na ploči, uključujući i komponente i njihove oznake. [4]

U prvoj vrsti napada shemi se dodaju dodatne komponente. Ovaj je napad vjerojatno najteže otkriti jer se shema obično smatra najtočnijim odrazom namjere dizajnera i stoga ima težinu autoriteta. U drugoj vrsti napada u raspored se mogu dodati dodatne komponente. To je jednostavan postupak, ali budući da postoje posebne provjere procesa za usporedbu rasporeda sa shemom, teže je proći neopažen: u najmanju ruku tehničar bi morao krivotvoriti rezultate usporedbe. A borba protiv ovog oblika napada je jednostavna: neka inženjer ili bolje grupa inženjera promatra usporedbu raspored-shema od početka dok kraja. [4]

Slika 3. Tiskana pločica [4]

Hakiranje kontrolera napajanja: Ovaj čip (Slika 4.) je posebno plodna meta jer djeluje kao kontroler za sve istosmjerne napone koji napajaju procesor, grafičku karticu i još mnogo toga. Pod nadzorom je sabirnice za upravljanje sustavom. Dakle, ako hakirani dio omogućava ljudima da preuzmu kontrolu nad sabirnicom za upravljanje sustavom, mogli bi resetirati napone kako bi oštetili računalo ili ograničili njegov rad. Kontrola sabirnice za upravljanje sustavom također bi mogla dopustiti hakeru da ometa komunikaciju između procesora i ugrađenih senzora, a to bi također moglo dovesti do oštećenja. [4]



Slika 4. Kontroler napajanja [4]

4.2. Oporavak od logičke pogreške

Dvije osnovne tehnike obnove podataka nakon logičkih pogrešaka su:

1. provjera konzistentnosti
2. metoda „rezbarenja podataka“

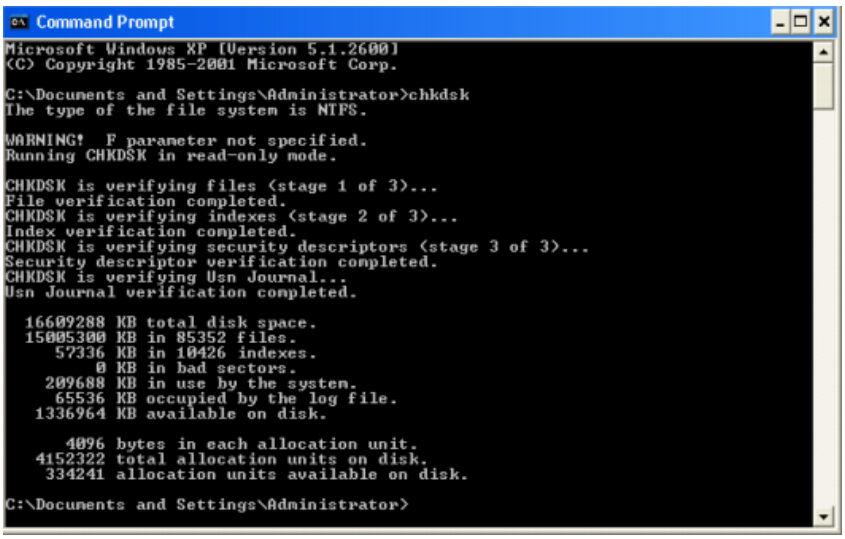
Dok većina logičkih oštećenja može biti popravljena uporabom ovih tehnika, programi za obnovu podataka ne mogu garantirati da neće doći do gubitka podataka. Na primjer, u datotečnom sustavu „FAT“, kada dvije datoteke dijele istu jedinicu za dodjelu memorije, gubitak podataka jedne od datoteka je garantiran. [2]

4.2.1. Provjera konzistentnosti

Provjera konzistentnosti uključuje skeniranje i provjeru logičke strukture diska kako bi se provjerila konzistentnost u skladu sa specifikacijom. Na primjer, u većini datotečnih sustava direktoriji moraju imati barem zapise:

- točka (.) – pokazuje na njih same,
- točka-točka (..) – pokazuje na roditeljski direktorij.

Program za ispravljanje pogreške datotečnog sustava može čitati svaki direktorij i osigurati da ovi zapisi postoje i pokazuju na ispravne direktorije. Ako otkrije nepravilnosti, takav program pruža ispis poruke o pogreški kako bi se problem mogao ispraviti. Na opisani način funkcioniraju i programi „chkdsk“ (Slika 3.) i „fsck“ [2]



Slika 4. Naredba „chkdsk“ [2]

4.2.2. Metoda „Rezbarenja podataka“

Metoda „rezbarenja podataka“ (eng. *Data carving*) nazvana tako jer služi za traženje zaglavlja datoteka te kopiranje i rekonstrukciju izbrisanih datoteka je tehnika obnavljanja podataka koja omogućuje identificiranje i izdvajanje dijelova koji pripadaju podacima bez informacija o dodijeljenom memorijskom prostoru. Tehnika obično pretražuje područja diska tražeći željene potpise datoteka. Činjenica da ne postoje informacije o dodjeli memorije znači da je potrebno specificirati veličinu podataka prilikom traženja podudarajućeg potpisa datoteke. Ovo donosi mogućnost pogrešne detekcije ovisno o složenosti potpisa datoteke. Također, postoje zahtjevi za pohranom obnovljenih podataka u slijedna područja (a ne fragmentirano). Metoda „rezbarenja podataka“ donosi uštedu na vremenu i resursima. [2]

4.3. Oporavak obrisanih podataka

Svaki operacijski sustav sadrži neki oblik zaštite od slučajnog brisanja datoteka. Obrisane datoteke je tako moguće lako povratiti ako je to potrebno. Jedan od primjera je komponenta „Koš za smeće“ kod operacijskog sustava „Microsoft Windows“. Također, postoje razni specijalizirani programi koji omogućuju obnavljanje određenog oblika datoteka (slikovnih datoteka, dokumenata, glazbenih datoteka, poruka elektroničke pošte i dr.). [2]

5. TEHNOLOGIJE ZA ZAŠTITU PODATAKA

5.1. Enkripcija podatka

Enkripcija podataka je tehnologija za zaštitu podataka koja šifrira podatke na tvrdom disku. Enkripcija diska se može vršiti u obliku softvera ili hardvera. Enkripcija se obično primjenjuje na dva načina:

Enkripcija spremišta – često nazivanog "podaci u mirovanju" – predstavlja najčešći način enkripcije čitavog diska, pogona ili uređaja. Ova vrsta enkripcije stupa u funkciju tek nakon prestanka rada sustava, isključivanja pogona ili blokiranja ključa za enkripciju.

Enkripcija sadržaja – poznata kao "granularna enkripcija" – tipično označava enkripciju datoteka ili teksta na razini aplikacije. Najbliži primjer je enkripcija e-mail poruka, gdje format poruke mora ostati netaknut kako bi ga klijent mogao obraditi, ali se tijelo e-mail poruke zajedno sa svim prilozima šifrira. [5]

5.2. Maskiranje podataka

Maskiranje strukturiranih podataka je proces prikrivanja (maskiranja) određenih podataka u tablici baze podataka kako bi podatci bili osigurani i korisnikove informacije osjetljivog sadržaja ne bi mogle «procuriti» iz autorizirane okoline. [6]

5.3. Brisanje podataka

Brisanje podataka je metoda kojom se u potpunosti uništavaju svi elektronski podatci na tvrdom disku ili nekom drugom digitalnom mediju kako bi se osigurali da podatci ili informacije ne procure nakon što se uređaj prestane koristiti. [6]

6. PROGRAMSKA PODRŠKA

6.1. Antivirus

Antivirusni programi ili antivirus je računalna programska podrška koja se koristi za zaštitu, identifikaciju i uklanjanje računalnih virusa, kao i drugih programa koji mogu oštetiti programsku podršku, a jednim imenom se naziva malware. Antivirusni program je najbolja zaštita od virusa i crva. On može spriječiti instaliranje virusa, a može i otkriti, izolirati i ukloniti viruse i crve s korisnikovog računala.

Antivirusni program radi stvaranjem potpisa svakog virusa ili komada malwarea. Potpis identificira sekciju koda koje se pojavljuje samo u malwareu. Svaki put kada antivirusni program skenira neki prilog u elektroničkoj pošti ili ispituje datoteke na tvrdom disku, on traži potpise poznatih virusa i crva. Antivirusni program vas može zaštiti od poznatih virusa koji se pojavljuju na nekoliko mjesta: u dolaznim i odlaznim porukama elektroničke pošte, porukama u sustavu za dopisivanje u realnom vremenu (chat, MSN, Skype…) i na tvrdom disku vašeg računala. Većina antivirusnih proizvoda isporučuje se sa skenerom u realnom vremenu koji provjerava vaše datoteke svaki put kada im pristupate.

Lažni antivirusni programi (neki od engleskih naziva su rogue security software i fake antiviruses) se korisniku lažno predstavljaju kao oni pravi. Ova vrsta zlonamjerne programske podrške pokušava navesti korisnika na kupnju tako što će simulirati pregledavanje njegovog računala i pokušati ga zastrašiti porukom da je pronađen ogroman broj nepostojeće zlonamjerne programske podrške te da će ih biti moguće ukloniti tek ako korisnik kupi program. Lažni antivirusni programi najčešće instaliraju zlonamjerne internetske stranice. [7]

6.2. Anti-spyware programi

Specijalizirani programi za uklanjanje špijunske programske podrške se zovu antišpijunski (eng. *antispyware*) programi. Oni često bolje prepoznaju većinu špijunskih programa, dobro prepoznaju i adware, a neki od poznatijih su Spybot Search & Destroy, Lavasoftov Ad-Aware, SUPERantispyware, CA Antispyware, Windows Defender i Sunbelt CounterSpy. Anti-spyware programi mogu skenirati tvrdi disk i pronaći nepoželjnu programsku podršku. Kada otkriju nepoželjni program pitaju da li ga korisnik želi izbrisati, izolirati ili ga ostaviti gdje je. Izoliranjem ga ostavljate na svom računalu ali spriječavate njegovo funkcioniranje.

Anti-spyware software ne nudi potpunu zaštitu od svih malwarea. Anti-spyware i antivirusni proizvodi počeli su se poklapati, a samo anti-spyware program nije dovoljan za zaštitu od virusa, crva i trojanskih konja. Anti-spyware proizvodi ne mogu skenirati elektroničku poštu koja postaje popularan put širenja zaraze za spyware. Postoje i programi koji mogu vršiti i imunizaciju internetskih preglednika. Imunizacija internetskih preglednika sprječava instalaciju određenih špijunskih programa na računalo te blokiraju opasne ActiveX skripte. Za potpunu zaštitu potrebno je koristiti antivirusni i anti-spyware program.[7]

6.3. Sigurnosni tokeni

Sigurnosni tokeni su usko povezani sa problemima e-trgovine te provjere autentičnosti. Autentikacija s dva faktora je autentikacija kod koje nešto imamo (pametna kartica ili token) i znamo nešto čime dokazujemo da je to što imamo uistinu naše (PIN ili upravo generirani broj na tokenu). Drugim riječima, kod autentikatora „nešto što imaš“ korisnik mora dokazati da je autentikator njegov. To će dokazati dodatnim upisivanjem PIN-a (eng. *Personal identification number*) kod pametnih kartica ili broja koji je u tom trenutku generirao token, ako je kao autentikator korišten token.

Sigurnosi token je poseban uređaj koji generira jednokratne zaporke, no kad je u pitanju autentikacija, token može biti bilo što. Tako se npr. pametna kartica često naziva token. [7]

Postoje različiti tipovi tokena. Osnovna podjela je na:

1) tokene koji generiraju statičke zaporke
2) tokene koji generiraju sinkrone dinamičke zaporke
3) tokene koji generiraju asinkrone zaporke
4) tokene koji rade na načelu izazova/odgovora.[7]

6.4. Vatrozid

Vatrozid (eng. *firewall*) je sigurnosni element (mrežni uređaj ili program) smješten između neke lokalne mreže i javne mreže (Interneta), a koji je dizajniran kako bi zaštitio povjerljive, korporativne i korisničke podatke od neautoriziranih korisnika (blokiranjem i zabranom prometa po pravilima koje definira usvojena sigurnosna politika). Služi sprječavanju neželjenog upada uljeza u lokalnu mrežu. Osnova rada vatrozida zasniva se u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i priključku u oba smjera. Vatrozid postavlja ograničenja na dolazni, ali i odlazni promet te prikriva identitet korisničkog računala što onemogućava, odnosno otežava, dobivanje informacija o računalu koje bi olakšale upad.

Vatrozid možemo shvatiti kao vrstu polupropusne barijere koja zaustavlja promet informacija prema vašem računalu te prema definiranim parametrima određuje što će propustiti, a što blokirati. Budući da aplikacije koriste priključke za pristup računalima, jedan od poslova vatrozida je da nadzire koji portovi smiju komunicirati s računalom.

Vatrozid može biti programski ili sklopovski:

1. Programski vatrozid omogućava zaštitu jednog računala, osim u slučaju kada je isto računalo postavljeno na zaštitu čitave mreže
2. Sklopovski vatrozid omogućuje zaštitu čitave mreže ili određenog broja računala. Za ispravan rad vatrozida potrebno je precizno odrediti niz pravila koje definiraju kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom sigurnosnom politikom se određuje nivo zaštite koji se želi postići primjenom vatrozida. [7]

7. PROTOKOLI ZA ZAŠTITU

Nekoliko je načina zaštite podataka i provjere njihove autentičnosti. Uz do sada spomenute koristimo i protokole za sigurno trgovanje preglednicima koristimo Secure Sockets Layer (SSL), korporacije u svijetu već odavno koriste Electronic Data Interchange (EDI), najpoznatiji od novih rješenja je Secure Electronic Transactions protokol (SET), a ima i drugih. [7]

7.1. Security Socket Layer – SSL

Security Socket Layer je protokol koji omogućuje šifrirani prijenos informacija putem HTTP, SSL omogućuje korištenje digitalnih certifikata tako da Web pretraživač može provjeriti autentičnost neke Web lokacije. Digitalni certifikat vjerodostojnosti koji potvrđuje da je treća strana povjerila vjerodostojnost nositelja certifikata. Svi se Web pretraživači isporučuju s već učitanim sposobnostima za korištenje SSL-a i nije potrebno dodatno koristi li se SSL adresa na traci za http://. (HTTPS je zaštićena verzija Hypertext Transfer Protocola.) vidjet ćete i ikonu lokota u donjem desnom kutu pretraživača. [7]

7.2. Electronic data interchange - EDI

EDI je protokol koji se koristi za razmjenu informacija, dokumenata, te raznih drugih poslovnih transakcija poput narudžbi, plaćanja i sličnog. poslovanje i prije svega je sigurno i pouzdano rješenje. [7]

EDI je razmjena strogo oblikovanih poruka s računala na računalo koje predstavljaju dokumente koji nisu novčani instrumenti. EDI podrazumijeva slijed poruka između dviju strana, od kojih svaka može služiti kao pokretač ili primatelj. Formatirani podaci koji predstavljaju dokumente mogu se prenositi od izvornika do primatelja putem telekomunikacija ili fizički na elektroničkom mediju za pohranu.[8]

EDI pruža tehničku osnovu za automatizirane komercijalne "razgovore" između dvaju entiteta, bilo internih bilo eksternih. Pojam EDI obuhvaća cjelokupni postupak elektroničke razmjene podataka, uključujući prijenos, tijek poruka, format dokumenta i softver koji se koristi za interpretaciju dokumenata. Međutim, EDI standardi opisuje strogi format elektroničkih dokumenata, a EDI standardi dizajnirani su u početku u automobilskoj industriji, neovisno o komunikacijskim i softverskim tehnologijama. [9]

EDI dokumenti obično sadrže iste podatke koji se obično mogu naći u papirnatom dokumentu koji se koristi za istu organizacijsku funkciju. Na primjer, proizvođač koristi narudžbu EDI 940 za otpremu iz skladišta kako bi skladištu rekao da isporuči proizvod maloprodaji. Obično ima adresu za isporuku, adresu za naplatu i popis brojeva proizvoda i količina.

Drugi je primjer skup poruka između prodavača i kupaca, poput zahtjeva za ponudu, ponude kao odgovor na zahtjev, narudžbenice, potvrde narudžbenice, obavijesti o otpremi, primanja savjeta, računa i savjeta o plaćanju. Međutim, EDI nije ograničen samo na poslovne podatke koji se odnose na trgovinu, već obuhvaća sva područja kao što su medicina (npr. Evidencija pacijenata i laboratorijski rezultati), prijevoz (npr. Informacije o spremnicima i modalima), inženjerstvo i građevinarstvo itd. U nekim slučajevima, EDI će se koristiti za stvaranje novog protoka poslovnih informacija. To je slučaj u Naprednoj obavijesti o pošiljci koja je dizajnirana da obavijesti primatelja o pošiljci, robi koja se prima i kako se pakira. [9]

7.3. Secure Electronic Transactions – SET

SET ili Protokol za sigurne elektroničke transakcije. SET treba sačuvati privatnost i integritet online plaćanja kreditnim karticama u realnom vremenu. Temelji se na stvaranju digitalnih „certifikata“ ili potvrda koje provjeravaju identitet kupca i prodavača prije ego što se pokrene mrežna transakcija plaćanja. Sadržaj transakcije zatim se zaštićuje zaporkom, zbog daljnjeg poboljšanja sigurnosti. [7]

8. PROBOJ PODATAKA

Proboj podataka je namjerno ili nenamjerno puštanje sigurnih ili privatnih / povjerljivih podataka u nepouzdano okruženje. Ostali pojmovi za ovaj fenomen uključuju nenamjerno otkrivanje podataka, curenje podataka, kao i izlijevanje podataka. Incidenti se kreću od usklađenih napada „crnih šešira“ ili pojedinaca koji hakiraju radi neke osobne koristi, povezane s organiziranim kriminalom, političkim aktivistima ili nacionalnim vladama, do neopreznog odlaganja rabljene računalne opreme ili medija za pohranu podataka i nehakiranog izvora.

Definicija: "Kršenje podataka je sigurnosno kršenje pri kojem se osjetljivi, zaštićeni ili povjerljivi podaci kopiraju, prenose, pregledavaju, kradu ili koriste od strane neovlaštenih osoba." Proboj podataka može uključivati financijske podatke poput kreditne kartice ili bankovni podaci, osobni zdravstveni podaci, osobni podaci, poslovne tajne korporacija ili intelektualno vlasništvo. Većina proboja podataka uključuje prekomjerno izložene i ranjive nestrukturirane podatke - datoteke, dokumente i osjetljive informacije.

Kršenje podataka može biti prilično skupo za organizacije s izravnim troškovima (sanacija, istraga, itd.) I neizravnim troškovima (reputacijska šteta, pružanje kibernetičke sigurnosti žrtvama ugroženih podataka, itd.)

Proboj podataka može obuhvaćati incidente poput krađe ili gubitka digitalnih medija kao što su tvrdi diskovi ili prijenosna računala koja sadrže takve medije na kojima se takvi podaci čuvaju nešifrirano, objavljivanje takvih podataka na svjetskoj mreži ili na računalu dostupnom na drugi način. s Interneta bez odgovarajućih mjera zaštite informacija, prijenos takvih podataka u sustav koji nije potpuno otvoren, ali nije odgovarajuće ili formalno akreditiran za sigurnost na odobrenoj razini, kao što je nešifrirana e-pošta, ili prijenos takvih podataka u informacije sustavi potencijalno neprijateljske agencije, poput konkurentske korporacije ili strane države, gdje bi ona mogla biti izložena intenzivnijim tehnikama dešifriranja. [10]

ISO / IEC 27040 kršenje podataka definira kao: ugrožavanje sigurnosti koje dovodi do slučajnog ili nezakonitog uništavanja, gubitka, promjene, neovlaštenog otkrivanja ili pristupa zaštićenim podacima koji se prenose, pohranjuju ili obrađuju na drugi način. [10]

8.1. Povjerenje i privatnost

Pojam pouzdanog okruženja pomalo je fluidan. Odlazak pouzdanog člana osoblja s pristupom osjetljivim informacijama može postati povreda podataka ako član osoblja zadrži pristup podacima nakon prestanka odnosa povjerenja. U distribuiranim sustavima to se može dogoditi i s raspadom mreže povjerenja. Kvaliteta podataka jedan je od načina za smanjenje rizika od povrede podataka, dijelom i zato što vlasniku podataka omogućuje da podatke ocjenjuje prema važnosti i daje bolju zaštitu važnijim podacima.

Većina takvih incidenata koji se objavljuju u medijima uključuju privatne podatke o pojedincima, na pr. brojevi socijalnog osiguranja. Gubitak korporativnih podataka kao što su poslovne tajne, osjetljivi korporativni podaci i detalji ugovora ili državnih podataka često se ne prijavljuje, jer za to nema uvjerljivog razloga u odsustvu potencijalne štete za privatne građane i javnosti oko takvih događaj može biti štetniji od gubitka samih podataka. [10]

9. ZAŠTITA PODATAKA U HRVATSKOJ I EUROPSKOJ UNIJI

9.1. Zakon o zaštiti osobnih podataka u RH

Zakon o zaštiti osobnih podataka[11] uređuje zaštitu osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradbom i korištenjem osobnih podataka u RH uključujući njihovo iznošenje iz RH. Svrha zaštite osobnih podataka je zaštita privatnog života i ljudskih prava, ali i temeljnih sloboda u koje ulazi i prikupljanje, obradba i korištenje osobnih podataka. Zaštita osobnih podataka zajamčena je Ustavom RH i to svakoj fizičkoj osobi bez obzira na rasu, boju kože, spol, jezik, vjeru, političko ili drugo uvjerenje, nacionalno ili socijalno podrijetlo, imovinu, rođenje, naobrazbu, društveni položaj ili neko drugo svojstvo ili obilježje. [12]

9.1.1. Definicije

Osobnim podatkom Zakon smatra svaki podatak ili informaciju koja se odnosi na fizičku osobu (ne na organizaciju, poduzeće, tijelo uprave i sl.) koju se može identificirati. Nije bitno je li osoba već identificirana, ili se može identificirati nekim postupkom, je li to izravno ili neizravno, dolazi li se do identiteta preko jednog ili skupine podataka. [12]

Pojam obrade osobnih podataka u Zakonu obuhvaća baš sve aktivnosti nad podacima od prikupljanja i pohrane, preko obradbe u tehničkom smislu i provođenja matematičkih operacija na podacima do prenošenja i objave podataka. Zakon se odnosi na sve obradbe bez obzira izvodi li ih tijelo države ili lokalne uprave, pravna osoba bilo kojeg oblika ili fizička osoba. Zakon se ne odnosi na obradbu koju (isključivo) za svoje osobne ili obiteljske potrebe (potrebe kućanstva) provode fizičke osobe. [12]

Zbirka osobnih podataka je skup podataka, organiziran i dostupan prema nekom (skupu) kriteriju. Pojam osobnog podatka i zbirke se odnosi na podatke bez obzira na formu i medij u kojem se nalaze: tiskani, elektronički ili dr. te bez obzira obrađuju li se ručno ili automatski. [12]

Iznimke

Podaci koji se prikupljaju u svrhu državne sigurnosti, obrane te suzbijanja korupcije, organiziranog kriminala i terorizma ne podliježu pod Zakon o zaštiti osobnih podataka. Svi ostali slučajevi moraju biti u skladu s ovim Zakonom.

Zakon definira da se bez privole ispitanika podaci prikupljaju i obrađuju i:

- u svrhu zakonskih obveza voditelja zbirke osobnih podataka,
- u svrhu zaštite života i tjelesnog integriteta ispitanika ili drugih osoba
- za zadatke koji su u interesu ili izvršavanju javnih ovlasti
- kad ispitanik sam objavi svoje osobne podatke. [12]

9.1.2. Prikupljanje

Zakon predviđa da se već i prije faze prikupljanja podataka od ispitanika i u samom prikupljanju moraju obaviti postupci i aktivnosti koji su se tradicionalno rijetko sretali u praksi. U stvari, u odnosu na uobičajenu praksu, Zakon uvodi prilično ograničenja. [12]

Opseg

Podaci koji se traže od ispitanika moraju biti bitni za svrhu zbog koje se prikupljaju. To izravno definira opseg podataka koji će se prikupljati. U praksi se mogu uočiti navike prikupljanja podataka "po inerciji" iako zapravo nisu potrebni. Najčešći takvi podaci su spol, datum rođenja i telefonski broj ispitanika. Važno je da zakon omogućava ispitaniku da odbije dati bilo koji podatak za koji smatra da nije potreban za svrhu u koju se podaci prikupljaju. Ako onaj tko prikuplja podatke odbije takav stav ispitanika, ispitanik ima pravo podnijeti prijavu Agenciji (Agenciji za zaštitu osobnih podataka). [12]

9.1.3. Svrha i informiranje ispitanika

Jedno od najvažnijih ograničenja koje Zakon postavlja, a svrha mu je spriječiti neprimjereno i prekomjerno korištenje osobnih podataka, je definirano na slijedeći način. Ispitanik mora biti upoznat sa svrhom prikupljanja njegovih osobnih podataka. Ta svrha mora biti izričito navedena, i temom i opsegom, i mora biti ispitaniku jasna te mora biti u skladu sa zakonom.

Voditelj zbirke osobnih podataka ili izvršitelj obrade dužan je informirati ispitanika o :

- identitetu voditelja zbirke osobnih podataka,
- svrsi obrade u koju su podaci namijenjeni,
- korisnicima ili kategorijama korisnika osobnih podataka,
- vrsti davanja podataka: je li ona dobrovoljna ili obvezna (zakonska osnova),
- mogućim posljedicama uskrate davanja podataka.

Tako prikupljani podaci smiju se obrađivati isključivo u navedenu svrhu te se ne mogu davati na korištenje trećim osobama. Zakon dozvoljava daljnju obradbu prikupljenih osobnih podataka u povijesne, statističke ili znanstvene svrhe, ali "uz odgovarajuće zaštitne mjere". To konkretno znači da ili treba uklonit podatke koji osobne podatke mogu povezati s identitetom ispitanika, ili treba uvesti tehničke mjere i postupke koji će onemogućiti daljnje širenje informacija i korištenje neovlaštenim korisnicima ili bez evidencije korištenja. [12]

9.1.4. Podaci i rok njihova čuvanja

Zakon insistira na tome da osobni podaci koji se prikupljaju (čuvaju, obrađuju, objavljuju…) moraju biti točni, potpuni i ažurni. To implicira da voditelj zbirke podataka mora provoditi procedure koje će podatke učiniti takvima, ali i omogućiti ispitaniku uvid u podatke te način njihova ispravljanja, dopunjavanja i osvježavanja. Pod pojmom životnog vijeka podataka, najčešće se razmatraju problemi preuranjenog nestajanja dijela ili cjelokupnih zbirki podataka. Međutim, jednako je važno onemogućiti i njihov nepotrebno dugi život. [12]

Zakon konkretno propisuje da se podaci smiju čuvati u obliku koji dopušta identifikaciju ispitanika samo onoliko vremena koliko je potrebno za njihovu odobrenu obradbu, a nakon toga samo u obliku koji ne omogućava identifikaciju ispitanika i to samo za povijesnu, statističku i znanstvenu svrhu. [12]

Posebne kategorije podataka

Zakon prepoznaje posebne kategorije osobnih podataka koje smatra posebno osjetljivima. To su: porijeklo, politička stajališta, vjerska i druga uvjerenja, sindikalno članstvo, zdravlje i spolni život, osobni podaci o kaznenom i prekršajnom postupku.

Zakon izričito zabranjuje njihovo prikupljanje i daljnju obradbu, osim u okviru djelatnosti ustanove, udruženja ili bilo kojeg drugog neprofitnog tijela koje je neposredno vezano uz takve podatke koji se odnose isključivo na njihove članove. Na primjer, logično je da politička stranka ima podatke o svojim članovima, kao i vjerska organizacija, udruga bolesnika s nekom specifičnom bolesti i slično. Međutim, oni te podatke ne smiju na bilo koji način učiniti dostupnima trećoj strani. Ostale zbirke podataka ne smiju sadržavati takve podatke. Iznimka su slučajevi kad je takve podatke potrebno prikupiti u svrhu izvršavanja zakonskih obveza voditelja zbirke osobnih podataka, ili u svrhu zaštite života ili tjelesnog integriteta ispitanika ili druge osobe u slučaju kada ispitanik fizički ili pravno nije u mogućnosti dati svoj pristanak. Također je to moguće kad je ispitanik dao privolu za prikupljanje takvih njegovih osobnih podataka ili kad ih je sam već negdje objavio. U takvom slučaju, obradba podataka mora biti posebno označena i zaštićena, a uredbom Vlade propisuje će se način pohranjivanja i posebne mjere tehničke zaštite tih podataka [NN 139/04]. [12]

9.1.5. Obradba osobnih podataka

Osoba (pravna ili fizička) koja u skladu sa Zakonom vodi zbirku podataka ne mora isključivo sama obavljati obradbu podataka već taj posao može ugovorom povjeriti fizičkoj ili pravnoj osobi koja:

- je registrirana za tu djelatnost,
- jamči zaštitu podataka od trećih osoba ili korisnika,
- provodi tehničke – organizacijske i kadrovske mjere zaštite podataka

Ta osoba može provoditi obradbu isključivo na osnovi naloga kojeg izdaje isključivo voditelj zbirke osobnih podataka. [12]

Korištenje osobnih podataka

Treće osobe koje žele koristiti osobne podatke mogu to pravo dobiti isključivo temeljem pisanog zahtjeva voditelju zbirke. U zahtjevu moraju navesti svrhu i pravni temelj korištenja podataka. Korištenje osobnih podataka će se odobriti samo za obavljanje poslova utvrđenih zakonom. Voditelj zbirke mora voditi evidenciju o tome koji su osobni podaci dani kojem korisniku i u koju svrhu. Ispitanik ima pravo uvida u evidenciju o korištenju njegovih osobnih podataka. Podaci se mogu dati na korištenje i u znanstveno-istraživačke i statističke svrhe, ali ti podaci ne smiju omogućiti identifikaciju osoba kojima pripadaju. [12]

9.1.6. Prava ispitanika

Važno je da Zakon jasno i izričito definira prava ispitanika u vezi njihovih osobnih podataka. Na zahtjev ispitanika, voditelj zbirke dužan je u roku 30 dana:

- dostaviti potvrdu o tome obrađuju li se osobni podaci koji se odnose na njega ili ne,
- dati obavijest u razumljivom obliku o podacima koji se odnose na ispitanika čija je obrada u tijeku te o izvoru tih podataka,
- omogućiti uvid u evidenciju zbirke osobnih podataka te uvid u osobne podatke sadržane u zbirci osobnih podataka koji se odnose na njega te njihovo prepisivanje,
- dostaviti izvatke, potvrde ili ispise osobnih podataka sadržanih u zbirci osobnih podataka koji se na njega odnose, a koji moraju sadržavati i naznaku svrhe i pravnog temelja prikupljanja, obrade i korištenja tih podataka,
- dostaviti ispis podataka o tome tko je i za koje svrhe i po kojem pravnom temelju dobio na korištenje osobne podatke koji se odnose na njega,

- dati obavijest o logici bilo koje automatske obrade podataka koja se na njega odnosi,
- dopuniti, izmijeniti ili obrisati osobne podatke koji su netočni, nepotpuni ili neažurni.

Ažuriranje podataka obavlja voditelj zbirke i sam (bez da ga to ispitanik zatraži) i o tome obavještava ispitanika u roku 30 dana. Sve ove ispravke su o trošku imatelja zbirke podataka. Svatko tko smatra da su mu povrijeđena prava može podnijeti zahtjev Agenciji, koja će, nakon analize, donijeti rješenje. Protiv rješenja može se podnijeti upravni spor. Agencija može privremeno zabraniti obradbu podataka do pravomoćnog okončanja postupka. Ispitanik ima pravo na naknadu štete temeljem rješenja suda za opće nadležnosti. [12]

9.1.7. Nadzor nad obradbom osobnih podataka

Nadzor obavlja Agencija za zaštitu podataka. Agencija je samostalna i odgovorna Saboru koji na prijedlog Vlade imenuje ravnatelja Agencije. Agencija prikuplja evidencije o zbirkama te analizira obavijesti o namjeravanoj uspostavi zbirke. Tako prikupljene podatke objedinjuje u Središnjem registru kojeg objavljuje u "Narodnim novinama" i na webu Agencije [registar.azop.hr]. U registru se vode sve zbirke u RH osim zbirki koje vode nadležna državna tijela za područje državne sigurnosti, obrane te suzbijanja pojava: korupcija, organiziranog kriminala i terorizma. Evidencije iz Središnjeg registra dostupne su javnosti. Agencija ih objavljuje u „Narodnim novinama“ ili na drugi način Agencija provodi nadzor nad obradbom osobnih podataka time što:

- nadzire provođenje zaštite osobnih podataka,
- ukazuje na uočene zloupotrebe prikupljanja osobnih podataka,
- sastavlja listu država i međunarodnih organizacija koje imaju odgovarajuće uređen zaštitu osobnih podataka,
- rješava povodom zahtjeva za utvrđivanje povrede prava zajamčenih ovim Zakonom,
- vodi središnji registar,
- objavljuje rješenja u Narodnim novinama.

- nadzire provođenje zaštite osobnih podataka na zahtjev ispitanika, na prijedlog treće strane ili po službenoj dužnosti.
- razmatra sve zahtjeve koji se odnose na utvrđivanje povrede prava u obradi osobnih podataka i izvijestiti podnosioca zahtjeva o poduzetim mjerama.
- ima pravo pristupa osobnim podacima sadržanim u zbirkama osobnih podataka .
- prati uređenje zaštite osobnih podataka u drugim zemljama i surađuje s tijelima nadležnim za nadzor nad zaštitom osobnih podataka u drugim zemljama,
- nadzire iznošenje osobnih podataka iz Republike Hrvatske,
- izrađuje metodološke preporuke za unapređenje zaštite osobnih podataka i dostavlja ih voditeljima zbirki osobnih podataka,
- daje savjete u svezi s uspostavom novih zbirki osobnih podataka, osobito u slučaju uvođenja nove informacijske tehnologije,
- daje mišljenja, u slučaju sumnje, smatra li se pojedini skup osobnih podataka zbirkom osobnih podataka u smislu ovoga Zakona. [12]

9.2. Zakona o provedbi Opće uredbe o zaštiti podataka

9.2.1. Opće odredbe

Predmet Zakona

(1) Ovim Zakonom osigurava se provedba Uredbe (EU) 2016/679 [13] 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)

(2) Ovaj se Zakon ne odnosi na obradu osobnih podataka koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja, kao ni na područje nacionalne sigurnosti i obrane. [14]

9.2.2. Nadležna tijela

Nadzorno tijelo

Članak 4.

(1) Nadzorno tijelo u smislu odredbe članka 51. Opće uredbe o zaštiti podataka je Agencija za zaštitu osobnih podataka (u daljnjem tekstu: Agencija).

(2) Agencija je neovisno državno tijelo. Agencija je u svom radu samostalna i neovisna i za svoj rad odgovara Hrvatskome saboru.

(3) Sjedište Agencije je u Zagrebu. [14]

9.2.3. Obrada osobnih podataka u posebnim slučajevima

Privola djeteta u odnosu na usluge informacijskog društva

Članak 19.

(1) Kod primjene članka 6. stavka 1. točke (a) Opće uredbe o zaštiti podataka, u vezi s nuđenjem usluga informacijskog društva izravno djetetu, obrada osobnih podataka djeteta zakonita je ako dijete ima najmanje 16 godina.

(2) Odredba stavka 1. ovoga članka primjenjuje se na dijete čije je prebivalište u Republici Hrvatskoj.

(3) Postupanje suprotno odredbama ovoga članka smatra se kršenjem članka 8. Opće uredbe o zaštiti podataka i podliježe sankcioniranju sukladno članku 83. Opće Uredbe o zaštiti podataka. [14]

Obrada genetskih podataka

Članak 20.

(1) Zabranjena je obrada genetskih podataka radi izračuna izgleda bolesti i drugih zdravstvenih aspekata ispitanika u okviru radnji za sklapanje ili izvršavanje ugovora o životnom osiguranju i ugovora s klauzulama o doživljenju.

(2) Privolom ispitanika ne može se ukinuti zabrana iz stavka 1. ovoga članka.

(3) Odredba stavka 1. ovoga članka primjenjuje se na ispitanike koji u Republici Hrvatskoj sklapaju ugovore o životnom osiguranju i ugovore s klauzulama o doživljenju ako obradu provodi voditelj obrade s poslovnim nastanom u Republici Hrvatskoj ili koji pruža usluge u Republici Hrvatskoj.

(4) Postupanje suprotno odredbama ovoga članka smatra se kršenjem članka 9. Opće uredbe o zaštiti podataka i podliježe sankcioniranju sukladno članku 83. stavku 5. Opće uredbe o zaštiti podataka. [14]

Obrada biometrijskih podataka

Članak 21.

(1) U tijelima javne vlasti obrada biometrijskih podataka može se provoditi samo ako je određena zakonom i ako je nužna za zaštitu osoba, imovine, klasificiranih podataka ili poslovnih tajni, uzimajući u obzir da ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom biometrijskih podataka iz ovoga članka.

(2) Smatrat će se da je obrada biometrijskih podataka u skladu sa zakonom ako je ona potrebna za ispunjenje obveza iz međunarodnih ugovora u vezi s identificiranjem pojedinca u prelasku državne granice. [14]

Članak 22.

(1) Obrada biometrijskih podataka u privatnom sektoru može se provoditi samo ako je propisana zakonom ili ako je nužna za zaštitu osoba, imovine, klasificiranih podataka, poslovnih tajni ili za pojedinačno i sigurno identificiranje korisnika usluga, uzimajući u obzir da ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom biometrijskih podataka iz ovoga članka.

(2) Pravni temelj za obradu biometrijskih podataka ispitanika radi sigurnog identificiranja korisnika usluga izričita je privola takvog ispitanika dana u skladu s odredbama Opće uredbe o zaštiti podataka. [14]

Članak 23.

Dopuštena je obrada biometrijskih podataka zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija, ako je propisano zakonom ili ako se takva obrada provodi kao alternativa drugom rješenju za evidentiranje radnog vremena ili ulaska i izlaska iz službenih prostorija, uz uvjet da je zaposlenik dao izričitu privolu za takvu obradu biometrijskih podataka u skladu s odredbama Opće uredbe o zaštiti podataka.

Članak 24.

(1) Odredbe ovoga Zakona o obradi biometrijskih podataka primjenjuju se na ispitanike u Republici Hrvatskoj ako obradu provodi:

– voditelj obrade s poslovnim nastanom u Republici Hrvatskoj ili koji pruža usluge u Republici Hrvatskoj

– tijelo javne vlasti.

(2) Odredbe ovoga Zakona o obradi biometrijskih podataka ne utječu na obvezu provođenja procjene učinka sukladno članku 35. Opće uredbe o zaštiti podataka.

(3) Odredbe ovoga Zakona o obradi biometrijskih podataka ne primjenjuju se na područje obrane, nacionalne sigurnosti i sigurnosno-obavještajnog sustava. [14]

Obrada osobnih podataka putem videonadzora

Članak 25.

(1) Videonadzor u smislu odredbi ovoga Zakona odnosi se na prikupljanje i daljnju obradu osobnih podataka koja obuhvaća stvaranje snimke koja čini ili je namijenjena da čini dio sustava pohrane.

(2) Ako drugim zakonom nije drugačije određeno, na obradu osobnih podataka putem sustava videonadzora primjenjuju se odredbe ovoga Zakona.

Članak 26.

(1) Obrada osobnih podataka putem videonadzora može se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine, ako ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem videonadzora.

(2) Videonadzorom mogu biti obuhvaćene prostorije, dijelovi prostorija, vanjska površina objekta, kao i unutarnji prostor u sredstvima javnog prometa, a čiji je nadzor nužan radi postizanja svrhe iz stavka 1. ovoga članka.

Članak 27.

(1) Voditelj obrade ili izvršitelj obrade dužan je označiti da je objekt odnosno pojedina prostorija u njemu te vanjska površina objekta pod videonadzorom, a oznaka treba biti vidljiva najkasnije prilikom ulaska u perimetar snimanja.

(2) Obavijest iz stavka 1. ovoga članka treba sadržavati sve relevantne informacije sukladno odredbi članka 13. Opće uredbe o zaštiti podataka, a posebno jednostavnu i lako razumljivu sliku uz tekst kojim se ispitanicima pružaju sljedeće informacije:

– da je prostor pod videonadzorom

– podatke o voditelju obrade

– podatke za kontakt putem kojih ispitanik može ostvariti svoja prava.

Članak 28.

(1) Pravo pristupa osobnim podacima prikupljenim putem videonadzora ima odgovorna osoba voditelja obrade odnosno izvršitelja obrade i/ili osoba koju on ovlasti.

(2) Osobe iz stavka 1. ovoga članka ne smiju koristiti snimke iz sustava videonadzora suprotno svrsi utvrđenoj u članku 26. stavku 1. ovoga Zakona.

(3) Sustav videonadzora mora biti zaštićen od pristupa neovlaštenih osoba.

(4) Voditelj obrade i izvršitelj obrade dužni su uspostaviti automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora koji će sadržavati vrijeme i mjesto pristupa, kao i oznaku osoba koje su izvršile pristup podacima prikupljenim putem videonadzora.

(5) Pristup podacima iz stavka 1. ovoga članka imaju nadležna državna tijela u okviru obavljanja poslova iz svojeg zakonom utvrđenog djelokruga.

Članak 29.

Snimke dobivene putem videonadzora mogu se čuvati najviše šest mjeseci, osim ako je drugim zakonom propisan duži rok čuvanja ili ako su dokaz u sudskom, upravnom, arbitražnom ili drugom istovrijednom postupku. [14]

Videonadzor radnih prostorija

Članak 30.

(1) Obrada osobnih podataka zaposlenika putem sustava videonadzora može se provoditi samo ako su uz uvjete utvrđene ovim Zakonom ispunjeni i uvjeti utvrđeni propisima kojima se regulira zaštita na radu i ako su zaposlenici bili na primjeren način unaprijed obaviješteni o takvoj mjeri te ako je poslodavac informirao zaposlenike prije donošenja odluke o postavljanju sustava videonadzora.

(2) Videonadzor radnih prostorija ne smije obuhvaćati prostorije za odmor, osobnu higijenu i presvlačenje. [14]

Videonadzor stambenih zgrada

Članak 31.

(1) Za uspostavu videonadzora u stambenim odnosno poslovno-stambenim zgradama potrebna je suglasnost suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova.

(2) Videonadzorom može se obuhvatiti samo pristup ulascima i izlascima iz stambenih zgrada te zajedničke prostorije u stambenim zgradama.

(3) Zabranjeno je korištenje videonadzora za praćenje radne učinkovitosti domara, spremačica i drugih osoba koje rade u stambenoj zgradi. [14]

Videonadzor javnih površina

Članak 32.

(1) Praćenje javnih površina putem videonadzora dozvoljeno je samo tijelima javne vlasti, pravnim osobama s javnim ovlastima i pravnim osobama koje obavljaju javnu službu, samo ako je propisano zakonom, ako je nužno za izvršenje poslova i zadaća tijela javne vlasti ili radi zaštite života i zdravlja ljudi te imovine.

(2) Odredbe ovoga članka ne isključuju primjenu članka 35. Opće uredbe o zaštiti podataka na sustavno praćenje javno dostupnog područja u velikoj mjeri. [14]

Obrada osobnih podataka u statističke svrhe

Članak 33.

(1) U okviru obrade osobnih podataka u svrhu proizvodnje službene statistike u skladu s posebnim propisima iz područja službene statistike, tijela koja proizvode službenu statistiku nisu dužna osigurati ispitanicima pravo pristupa osobnim podacima, pravo na ispravak osobnih podataka, pravo na ograničenje obrade osobnih podataka niti pravo na prigovor na obradu osobnih podataka, i to radi osiguravanja uvjeta nužnih za ostvarivanje svrhe službene statistike u mjeri u kojoj je vjerojatno da bi se takvim pravima moglo onemogućiti ili ozbiljno ugroziti postizanje tih svrha te kada su takva odstupanja od prava prijeko potrebna za postizanje tih svrha.

(2) Tijela nadležna za proizvodnju službene statistike dužna su primjenjivati tehničke i organizacijske mjere zaštite podataka prikupljenih za potrebe službene statistike.

(3) Voditelji obrade osobnih podataka prilikom prijenosa osobnih podataka tijelima nadležnima za službenu statistiku nisu dužni obavještavati ispitanike o prijenosu osobnih podataka u statističke svrhe.

(4) Obrada osobnih podataka u statističke svrhe smatra se podudarnom svrsi za koju su podaci prikupljeni, pod uvjetom da se poduzmu odgovarajuće zaštitne mjere.

(5) Osobni podaci obrađeni u statističke svrhe ne smiju omogućiti identifikaciju osobe na koju se podaci odnose. [14]

9.2.4. Postupak u nadležnosti agencije i pravni lijekovi

Članak 34.

(1) Svatko tko smatra da mu je povrijeđeno neko pravo zajamčeno ovim Zakonom i Općom uredbom o zaštiti podataka, može Agenciji podnijeti zahtjev za utvrđivanje povrede prava.

(2) O povredi prava Agencija odlučuje rješenjem.

(3) Rješenje Agencije je upravni akt.

(4) Protiv rješenja Agencije žalba nije dopuštena, ali se tužbom može pokrenuti upravni spor pred nadležnim upravnim sudom.

Članak 35.

(1) Ako je rješenjem naloženo brisanje ili drugo nepovratno uklanjanje osobnih podataka, nezadovoljna stranka može zatražiti od nadležnog upravnog suda odgodu izvršenja brisanja ili drugog nepovratnog uklanjanja osobnih podataka ako dokaže da bi nerazmjernim naporima ponovno prikupila osobne podatke čije se brisanje odnosno nepovratno uklanjanje traži.

(2) Ako nadležni upravni sud prihvati zahtjev iz stavka 1. ovoga članka, stranka kojoj je naloženo brisanje ili drugo nepovratno uklanjanje osobnih podataka dužna je blokirati svaku obradu spornih osobnih podataka, osim njihova čuvanja, do donošenja pravomoćne sudske odluke. [14]

Preslike, pečaćenje i privremeno uzimanje sustava pohrane i opreme

Članak 37.

(1) Ovlaštene osobe, prema potrebi, mogu napraviti preslike dostupnih dokumenata, presnimiti sve sadržaje sustava pohrane i prikupiti druge relevantne informacije.

(2) Ako iz tehničkih razloga nije moguće tijekom nadzora napraviti preslike potrebne dokumentacije, ovlaštene osobe će, prema potrebi, oduzeti potrebne sustave pohrane i opremu koja sadržava druge relevantne informacije i zadržati je koliko je potrebno za izradu preslika te dokumentacije, a najduže do 15 dana od dana oduzimanja sustava pohrane i opreme.

(3) Ovlaštene osobe mogu zapečatiti sustave pohrane ili opremu za vrijeme nadzora i u opsegu prijeko potrebnom za provedbu nadzornih aktivnosti ako postoji opasnost od uništenja ili izmjena dokaza, a najduže 15 dana od dana pečaćenja sustava pohrane ili opreme.

(4) O kopiranju, pečaćenju i privremenom uzimanju sustava pohrane i opreme ovlaštena osoba dužna je sastaviti službenu zabilješku sa svim relevantnim informacijama o podacima ili opremi obuhvaćenoj radnjom i njezin primjerak predati nadziranom subjektu. [14]

Klasificirani podaci

Članak 39.

(1) Svaki pristup, kopiranje i bilo kakva druga obrada podataka koji su klasificirani s utvrđenim stupnjem tajnosti na temelju posebnog propisa provest će se sukladno propisima kojima se uređuje zaštita tajnosti podataka.

(2) Svaki pristup, kopiranje i bilo kakvu drugu obradu podataka koja je klasificirana s utvrđenim stupnjem tajnosti na temelju posebnog propisa provest će službenici koji imaju valjani certifikat za pristup klasificiranim podacima sukladno propisima kojima se uređuje zaštita tajnosti podataka. [14]

9.3. Pravo na zaštitu osobnih podataka kao temeljno pravo

Pravo na zaštitu osobnih podataka od samih je početaka njegova izučavanja izazivalo dvojbe u pogledu njegove pravne prirode. U pravnoj se znanosti sve do druge polovice dvadesetog stoljeća nije raspravljalo o pravu na zaštitu osobnih podataka bez spominjanja drugih prava s kojima se ono dovodi u vezu, a posebice prava na privatnost. Teškoće koje se javljaju pri pokušaju razdvajanja navedenih prava moguće je objasniti stavljanjem naglaska na teorijsku pozadinu prava na zaštitu osobnih podataka i njegovog odnosa s drugim bliskim pravima. [15]

Većina šire prihvaćenih definicija privatnosti je po prirodi negativna i uglavnom se svode na izbjegavanje neželjenog uznemiravanja određenog pojedinca, odnosno na problem neželjenog otkrivanja nekih podataka u vezi s privatnom sferom tog pojedinca u njegovu svakodnevnom životu. S druge strane, pravo zaštite osobnih podataka postoji upravo u svrhu olakšavanja protoka informacija, pritom štiteći osobne podatke pojedinaca. U tom kontekstu, cilj je privatnosti osigurati netransparentnost nečijega privatnog života, dok se zaštitom osobnih podataka nastoji postići upravo transparentnost svih drugih podataka koji nisu privatni. Navedena teza očitovala se i u činjenici što su prvi pravni propisi u okviru europskog prava koji su se doticali prava na zaštitu osobnih podataka, bili dovedeni u izravnu vezu s pravom na privatnost, na način da se pravo na zaštitu osobnih podataka smatralo ili podskupom interesa privatnosti ili pravom istovjetnim pravu na privatnost, njegovim pravom blizancem (eng. *twin-right*).

Spomenuto shvaćanje prema kojemu se pravo na zaštitu osobnih podataka ne može promatrati neovisno o pravu na privatnost, zadržalo se u prvom planu u pravnom poretku Europske unije i njenih država članica sve do dvadeset i prvog stoljeća. [15]

9.3.1. Protupravna obrada podataka

Temeljne promjene koje Uredba donosi u području zaštite osobnih podataka usmjerene su boljem položaju ispitanika i jačanju njegove kontrole nad vlastitim osobnim podatcima te višem stupnju sigurnosti njihove obrade. S gledišta odštetnog prava, Uredba je najviše promjena donijela u protupravnost kao pretpostavku odgovornosti za štetu. Detaljnim propisivanjem pravila obrade odredila je njene granice i to jednako za sve obrade podataka koji se odnose na osobe koje se nalaze na području Europske unije. Za utvrđenje protupravnosti ponašanja potencijalno odgovornih subjekata (voditelja i izvršitelja obrade podataka) ključno je da u Uredbi korišteni pojmovi budu jasno i precizno definirani. Jesu li nove definicije i izmjene dosadašnjih, zaista precizne i hoće li i u kom smislu biti nejasnoća, treba pričekati nešto duže razdoblje primjene Uredbe.

Povrede prava na zaštitu osobnih podataka mogu proizlaziti iz povrede načela obrade podataka, povrede prava ispitanika i povreda pojedinih obveza voditelja i izvršitelja obrade. Svaka obrada osobnih podataka koja nije u skladu s odredbama Uredbe je protupravna, ali nije svaka takva obrada potencijalni uzrok štete za osobu čiji se podatci obrađuju, odnosno podobna da bude štetna radnja. To su samo obrade koje udovoljavaju definiciji povrede iz članka 4. točka 12. Uredbe: povreda osobnih podataka znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podatcima koji su preneseni, pohranjeni ili na drugi način obrađivani, kojima je oštećeniku prouzročena konkretna šteta. Dakle, potrebno je da zbog „slučajnog ili nezakonitog“ uništenja, gubitka i izmjene, odnosno neovlaštenog otkrivanja ili pristupa njegovim osobnim podatcima oštećenik pretrpi određeni imovinski ili neimovinski gubitak. U tom je smislu moguće razlikovati dvije temeljne vrste potencijalnih štetnih radnji, slučajna i nezakonita uništenja, gubitke, otkrivanja… (podataka). [15]

9.3.2. Subjekti odgovornosti za štetu

U odnosu na dosadašnje pravno uređenje, Uredba je proširila krug potencijalno odgovornih subjekata. Odgovornošću su izričito obuhvaćeni voditelji i izvršitelji obrade (čl. 82. st. 1. Uredbe), dok je Direktiva 95/46/EZ u svom članku 23. stavku 1. spominjala samo nadzornike obrade. Za nadzornika je hrvatski Zakon o zaštiti osobnih podataka koristio pojam voditelja zbirke osobnih podataka i navodio ga kao jedinu potencijalno odgovornu osobu. Budući da je Uredba u cijelosti obvezujuća i izravno se primjenjuje, nacionalni zakonodavci ne mogu mijenjati ili dopunjavati njene definicije. Voditelj obrade u Uredbi se definira kao fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka (čl. 4. t. 7. Uredbe). Izvršitelj obrade je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade (čl. 4. t. 8. Uredbe). Kada je kao voditelj ili izvršitelj obrade pri kojoj je došlo do kršenja Uredbe ili Zakona o njenoj primjeni sudjelovalo neko tijelo javne vlasti u Republici Hrvatskoj, iako mu ne može biti izrečena upravna novčana kazna, ono odgovara za štetu koja je pritom prouzročena. Kao subjekti potencijalno odgovorni za štetu zbog povrede prava na zaštitu osobnih podataka, javljaju se, dakle, sve fizičke i pravne osobe u ulozi voditelja ili izvršitelja obrade, države članice (koje odgovaraju za tijela javne vlasti koja se nađu u tim ulogama), te sama Unija (kada osobne podatke obrađuju njene institucije i tijela).

Potencijalni oštećenici su sve fizičke osobe, koje se nalaze na području Unije, bez obzira na njihovo državljanstvo i boravište, čiji su osobni podatci obrađivani. Međutim, budući da Uredba propisuje da pravo na naknadu štete ima svaka osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog njenog kršenja (čl. 82. st. 1. Uredbe), kao oštećenici se mogu javiti i osobe čiji podatci nisu bili predmetom obrade, već trpe štetu kao posljedicu kršenja Uredbe pri obradi podataka neke druge osobe (tzv. posredni oštećenici). [15]

Budući da nacionalna pravila o odgovornosti vrlo rijetko priznaju posrednim oštećenicima pravo na naknadu (u pravilu samo kada je ono izričito propisano), ne čudi da se oštećenicima smatralo samo subjekte čiji su podatci obrađivani. I hrvatski je zakonodavac pod „svaka osoba“ razumijevao samo ispitanika. Kako će, neposredno primjenjujući Uredbu, sudska praksa nacionalnih sudova država članica definirati opseg kruga potencijalnih oštećenika, tek predstoji vidjeti, ali treba polaziti od toga da je europski zakonodavac pod pojmom svaka osoba imao u vidu širi krug osoba od samih ispitanika. Neki autori upozoravaju da će se, budući da pravo na naknadu prema članku 82. stavku 1. Uredbe imaju i drugi pojedinci koji su pretrpjeli štetu, posebna pažnja morati posvetiti postojanju uzročne veze između štete te treće osobe i povrede prava na zaštitu podataka. Kao mogući primjer navodi se situacija u kojoj je oštećenik zbog povrede pravila Uredbe o obradi podataka ostao bez posla i zbog toga nije mogao izvršiti obvezu uzdržavanja te se uzdržavanu osobu navodi kao mogućeg oštećenika koji bi mogao postaviti zahtjev za naknadu štete. Kao posredni oštećenici, iako su predmet zaštite samo podatci fizičkih osoba, mogle bi se pojaviti i pravne osobe, npr. poslodavac koji pretrpi štetu zbog nezakonite obrade podataka svoga zaposlenika. [15]

10. KIBERNETIČKA SIGURNOST U ENERGETSKOM SEKTORU U EU

Kritične infrastrukture pružaju ključne usluge koje podupiru nesmetano funkcioniranje modernog društva i služe kao okosnica gospodarskih aktivnosti. Te kritične infrastrukture uključuju sektore energije, telekomunikacija, financija, zdravstva i prometa. Energetska infrastruktura je nesumnjivo među jednom od najsloženijih i kritičnih infrastruktura, jer ovi drugi sektori ovise na njemu pružiti njihove osnovne usluge. Stoga nedostupnost u opskrbi energijom ima veliki potencijalni utjecaj na gospodarstvo i pravilno funkcioniranje civilnog društva koji može trajati dulje od vremena samog incidenta.

Potencijalni poremećaj kroz dulje vremensko razdoblje mogao bi utjecati na društvo, industriju i trgovinu s visokim rizikom utjecaja na bruto domaći proizvod (BDP). Međutim, mora se primijetiti da takva razina prijetnje još nije ostvarena unutar Europske unije.

Ciljevi na visokoj razini:

- ✓ Osigurati energetske sustave koji pružaju osnovne usluge europskom društvu.
- ✓ Zaštitite podatke u energetskim sustavima i privatnost europskog građanina.

Ovi su ciljevi na visokoj razini zajednički među dionicima jer odražavaju potrebu za zaštitom energetskih sustava i podataka potrebnih za učinkovito upravljanje tim sustavima. [16]

10.1. Energetski sektor - promjene u infrastrukturi

Digitalne tehnologije igraju sve značajniju ulogu u energetskom sektoru. Pametniji sustav energija može obavljati proizvodnju, prijenos i upravljanje mrežom s boljom preciznošću i s bržim vremenom odgovora od sustava koji ovisi o čovjeku, stoga optimizira upravljanje energijom, daje prioriteta upotrebi i brzom odgovoru na prekide rada. [16]

Sustavi za kontrolu energije uključuju hijerarhiju međusobno povezanih fizičkih i elektroničkih sustava, uređaji za nadzor i upravljanje, koji uglavnom djeluju u stvarnom vremenu i tipično su povezani s centralnom nadzornom stanicom ili kontrolnim centrom. Kontrolni sustavi obuhvaćaju nadzornu kontrolu i sustave za akviziciju podataka (eng. *Supervisory Control And Data Acquisition,* SCADA) koji se koriste za praćenje i kontrolu operacija u slučaju transporta energije i u distribucijskoj mreži su široko raspršene. Distribuirani upravljački sustavi (eng. *Distributed Control System*, DCS) koriste se za pojedinačne objekte ili mala geografska područja.

Upravljački sustavi povezani su s udaljenim komponentama poput udaljenih terminalnih jedinica (eng. *Remote Terminal Unit,* RTU) i programibilnih logičkih kontrolera (eng. P*rogrammable Logic Controller*, PLC) koji nadgledaju sustave podataka i pokreću programirane kontrolne aktivnosti kao odgovor na ulazne podatke i upozorenja. SCADA sustavi prikupljaju, prikazuju i pohranjuju informacije prikupljene iz pretvarača, senzora, upravljačke oprema, uređaja i automatiziranih funkcija. Oni čine dio procesa upravljačkih sustava koji se koriste za upravljanje u stvarnom vremenu, na primjer prijenosom i distribucijom električne energije ili prijenos i distribucija po plinovodima.

U proizvodnim sustavima procesi proizvodnje energije moraju se kontrolirati. Izgaranje nafte, ugljena ili plina, a također i postupci nuklearne fisije generiraju toplinu koja se koristi za pogon turbina. Ove turbine proizvode energiju, a cjelokupni proizvodni proces kontroliraju analogni i / ili digitalni sustavi koji su povezani s glavnom kontrolnom sobom u kojoj ljudi nadgledaju procese. Obnovljivi izvori (vjetar, solarna energija, hidroelektrane) sustavi su koji su međusobno vrlo povezani i njihovu proizvodnju energije kontroliraju centralne stanice koje uzimaju u obzir prirodno nepredvidivo ponašanje obnovljivih izvora poput vjetra i sunca.

Trenutno se energetski sektor sastoji od naslijeđenih tehnologija i tehnologija sljedeće generacije. Nove tehnologije uvode nove inteligentne komponente (npr. brojila električne energije ili plina, digitalni ventili ili pumpe) do energetske infrastrukture koja komunicira na naprednije načine (dvosmjerna žičana i bežične komunikacije) nego u prošlosti. Te se nove komponente obično temelje na informacijskim i komunikacijskim tehnologijama koje se mogu međusobno povezati s lokalnim mrežama. [16]

Tipično se ‘analogne’ komponente zamjenjuju novim digitalnim sustavima jer rezervni dijelovi više nisu dostupni ili su zastarjeli.

Osiguravanje otpornosti sustava opskrbe energijom na kibernetičke rizike i prijetnje postaje sve važnije kako široko rasprostranjena uporaba informacijskih i komunikacijskih tehnologija postaje temelj za funkcioniranje infrastruktura u energetskim sustavima. Povećana učinkovitost u uslugama opskrbe dolazi s cijenom: povećana izloženost kibernetičkim incidentima i napadi. Na međusektorski način, ove prijetnje odnose se na sve - proizvodnju, prijenos, distribucijske i procesne tehnologije te na usluge na energetskom tržištu.

Digitalizacija energetskog sektora također postavlja pitanje kako se suočiti s rizicima i prijetnjama od kibernetičkih incidenata i napada koji utječu na osobne podatke i podatke o strateškoj energetskoj infrastrukturi, koji su ponekad presudni za sigurnost opskrbe energijom. [16]

10.2. Energetski sektor - promjene u kibernetičkoj sigurnosti

Fokus kibernetičke sigurnosti u energetskom sektoru je podrška pouzdanosti i otpornosti čak i u slučaju kibernetičkih napada. Za razliku od informacijskih sustava, kontrolni sustav u energetskom sektoru koji je napadnut ne može se lako odspojiti s mreže jer bi to moglo dovesti do sigurnosnih problema, izbacivanja ili čak zamračenja. U kibernetičkoj sigurnosti definirana su tri općeprihvaćena cilja zaštite: povjerljivost, cjelovitost i dostupnost. U energetskom sektoru najveći prioritetni cilj ovisi o industriji specifične primjene. Na primjer u proizvodnji i prijenosu, dostupnost i cjelovitost su najvažnije. Izmijenjeni ili odgođeni podaci mogu na kraju dovesti do pogrešne konfiguracije uređaje što na kraju može utjecati na pouzdanost sustava. Za naprednu mjernu infrastrukturu, povjerljivost osobnih podataka kupaca su najkritičniji. U nuklearnoj sigurnosti ciljevi su sprječavanje kibernetičkih djela koji bi mogli izravno ili neizravno dovesti do neovlaštenog uklanjanja nuklearnog ili drugog radioaktivnog materijala, sabotaže nuklearnog materijala ili nuklearnih postrojenja ili krađe nuklearno osjetljivih informacija. [16]

Uz sve veću upotrebu digitalnih uređaja i naprednijih komunikacija povećao se ukupni kibernetički rizik. Na primjer, kako se trafostanice moderniziraju, nove oprema je digitalna, a ne analogna. Ovi novi uređaji uključuju komercijalno dostupan operativni sustave, protokole i aplikacije koji pružaju veće područje napada. Ovo u kombinaciji s međusobnom povezanosti povećava složenost rješavanja odgovarajućih kibernetičkih rizika i daje mogućnosti potencijalnom napadaču.

Napadači mogu biti državnih akteri, nedržavni akteri, nezadovoljni zaposlenici, iskusni hakeri i hakerske skupine, organizirani kriminalci, haktivisti i teroristi. Postoje i nezlonamjerni događaji u kibernetičke sigurnosti, kao što su pogreške korisnika / administratora ili tehničke greške, što izgleda isto i može na kraju imati isti učinak kao koordinirani napad.

Bez obzira na izvor incidenta u kibernetskoj sigurnosti, potencijalni utjecaj na energetski sektor je isti: izbacivanje, zatamnjenje ili pogrešna konfiguracija upravljačkih sustava. Uz stalne promjene u energetskom sektoru kibernetička sigurnost mora ići u korak sa sve sofisticiranijim kibernetičkim prijetnjama.

Izazovi u kibernetičkoj sigurnosti specifični za energetski sektor koje su ustanovili stručnjaci platforme za kibernetičku sigurnost (eng. *Energy Expert Cyber Security Platform,* EECSP) su sljedeće:

- Stabilnost mreže u prekograničnoj međusobno povezanoj energetskoj mreži.
- Koncepti zaštite koji odražavaju trenutne prijetnje i rizike.
- Rukovanje kibernetičkim napadima unutar EU.
- Učinci kibernetičkih napada koji nisu u potpunosti uzeti u obzir u pravilima postojeće električne mreže ili nuklearnog postrojenja.
- Uvođenje novih visoko povezanih tehnologija i usluga.
- Outsourcing infrastrukture i usluga.
- Cjelovitost komponenata koje se koriste u energetskim sustavima.
- Povećana međuovisnost na tržištu.
- Dostupnost ljudskih resursa i njihovih kompetencija.
- Ograničenja nametnuta mjerama kibernetičke sigurnosti u odnosu na stvarno vrijeme / dostupnost zahtjeva. [16]

10.3. Rukovanje kibernetičkim napadima unutar EU

Ovaj je izazov relevantan za cijeli energetski sektor.

Kibernetički napadi ne mare za zemljopisne granice, a napadi mogu imati utjecaj na cijelu EU. Kad se govori o rješavanju kibernetičkih napada u EU, mora se uzeti u obzir nekoliko aspekata:

- Mogućnosti prepoznavanja, otkrivanja, reagiranja i oporavka od kibernetičkih napada.
- Moguće prijetnje: iskusni državni i nedržavni akteri poput doušnika, hakerske skupine, organizirani kriminal, haktivisti i teroristi.
- Različita razina upravljanja: operater, države članice, EU, diplomacija ili vojska.
- Mogućnosti upravljanja krizama.
- Mogućnosti kibernetičkih odgovora.
- Istraživanje mogućnosti kibernetičkih napada i pripisivanje tih napada. [16]

10.3.1. Uvođenje novih visoko povezanih tehnologija i usluga

Energetska infrastruktura se modernizira kako bi se povećala energetska i operativna učinkovitost i pouzdanost. Digitalizacija u energiji pokrenuta je sve većom uporabom obnovljivih izvora, skladištenjem, e-mobilnosti, mikro mreže, distribuirane proizvodnje itd. Kao posljedica toga, nove mrežne tehnologije uvode milijune novih, inteligentnih komponenata u energetski sektor koje komuniciraju na mnogo napredniji način (dvosmjerna komunikacija žičanom i bežičnom komunikacijom) nego u prošlost. Uređaji koji se temelje na standardiziranim komponentama s uobičajenim ranjivostima i velikim brojem potencijalnih točaka napada neprestano se dodaju u energetske mreže.

Povećanom digitalizacijom energetskog sektora tehnološki napredak i trendovi imaju pojavili su se kao što su:

- Integracija Interneta stvari u uređaje. Ti uređaji, uključujući kućanske uređaje poput hladnjaka, perilica rublja itd., prije su bili samostalni i nije im se moglo pristupiti putem Interneta.

- Usluge u oblaku s 24/7 operacijama koje zahtijevaju automatsko izvještavanje o statusu i odgovor.
- Analitika za učinkovito upravljanje digitalnim uređajima pomoću tehnologija 'velikih podataka' za obradu podataka.
- Proširena telekomunikacijska infrastruktura i mreže s povećanom uporabom mobilnih uređaji i poticanje postavljanje novih aplikacija.
- Nove aplikacije s integracijom potražnje i odgovora, poput virtualnih postrojenja, mikro mreže ili usluga upravljanja oblakom za solarnu, građevinsku i kućnu automatizaciju. [16]

Povećana složenost energetskih mreža odražava se na način na koje se energija i s energijom povezane informacije i podaci koriste, dijele, obrađuju i kontroliraju. S jedne strane, u slučaju da upravljanje energetskom mrežom sve više ovisi o dostupnosti i cjelovitosti podatkovnih usluga, rizik od povrede podataka u kontekstu podataka relevantnih za mrežu mora biti dobro shvaćen. S druge strane, mora se uzeti u obzir i privatnost podataka. U ovom kontekstu, izazov je prijelaz prema digitalnim uslužnim programima koji postaju sve više podatkovno usmjereni i gdje će analitika 'velikih podataka' postati dio njihovih primarnih procesa. U tom kontekstu, dodavanje novih tehnologija i usluga u sustav mreža zahtijeva veliku pozornost na rizike kibernetičke sigurnosti i na kompetencije u njihovom rješavanju u okruženju koje se mijenja. [16]

11. SLUČAJEVI PROBOJA PODATAKA

11.1. Krađa podataka s mrežne pohrane Dropbox 2011. godine

Datoteke povjerene davatelju usluga pohrane u oblaku Dropbox bile su podložne neovlaštenom pristupu putem tri napada koje su osmislili istraživači sigurnosti i koji su svoje radove predstavili na USENIX Sigurnosnom simpoziju, ali davatelj usluga otada je uklonio propuste. Dropbox se također može koristiti kao mjesto za tajno pohranjivanje dokumenata i njihovo preuzimanje s bilo kojeg Dropbox računa koji kontrolira napadač.

Prvo su uspjeli lažirati hash vrijednosti koje bi trebale identificirati dijelove podataka pohranjenih u Dropboxovom oblaku. Dropbox provjerava ove vrijednosti da vidi jesu li dijelovi već pohranjeni u oblaku i ako jesu, samo ih povezuje s računom korisnika koji je poslao hash vrijednost. Lažiranjem hash vrijednosti uspjeli su omogućiti da im Dropbox odobri pristup proizvoljnim dijelovima podataka drugih korisnika. Budući da je neovlašteni pristup odobren iz oblaka, korisnik čije se datoteke distribuiraju nije znao da se to događa.

Drugi napad zahtijevao je krađu žrtvinog ID-a domaćina (eng. *host*) Dropbox-a, a to je 128-bitni ključ koji je Dropbox generirao koristeći specifične čimbenike kao što su korisničko ime, vrijeme i datum. Jednom kada napadač dobije žrtvin ID mogao bi ju zamijeniti za svoju. Kad je ponovo sinkronizirao svoj račun, sve žrtvine datoteke mogle su mu se preuzeti. Kod nas se za riječ „domaćin“ uvriježila engleska riječ „host“.

Treći napad iskorištava značajku koja korisnicima Dropboxa omogućuje da zahtijevaju dijelove datoteka putem SSL-a na određenom URL-u. Sve što je potrebno su dio hash vrijednosti i bilo koji valjani ID hosta - ne nužno ID hosta s kojim je traženi dio povezan. [17]

Ovaj posljednji napad Dropbox je otkrio zbog neusklađenosti između traženih dijelova i računa koji ih zahtijevaju. Ova su tri napada mogla biti korisni alati za krađu podataka iz organizacija koje su koristile Dropbox. Umjesto da su morali ukrasti cijele datoteke iz korporativnih mreža, bila je dovoljna hash vrijednost podataka koji su željeli. Tada se hash može poslati Dropboxu s bilo kojeg mjesta za preuzimanje stvarnih podataka. Napadi su se mogli koristiti za sakrivanje podataka u Dropboxovom oblaku. Neograničeni dijelovi podataka mogu se prenijeti u oblak bez povezivanja s računom napadača korištenjem modificiranog Dropbox klijenta. Da bi preuzeli podatke, napadači su mogli poslati hash vrijednosti tih podataka u Dropbox kao da ga namjeravaju prenijeti. Budući da je dio podataka s odgovarajućim hashom već u oblaku, Dropbox bi taj komad samo povezao s računom koji šalje hash. Bilo koji račun koji kontrolira napadač mogao je pristupiti podacima. [17]

11.2. Hakiranje SolarWinds softwera

Microsoft i sigurnosna kompanija FireEye otkrili su detalje o sofisticiranom hakerskom napadu koji iskorištava propust u poslovnom softveru, čije žrtve su kompanije i vladine agencije diljem svijeta

Zabilježen je novi organizirani hakerski napad na američke vladine agencije, kompanije koje se bave kibernetičkom sigurnošću, te druge kompanije iz javnog i privatnog sektora. Napad je, prema objavama Microsofta i sigurnosne kompanije FireEye, (koja je i sama bila žrtvom napada), državno orkestriran i vjeruje se da mu je izvorište u Rusiji. [18]

Napadači iskorištavaju propust u poslovnom softveru SolarWinds Orion kako bi kroz njega na računala svojih meta distribuirali trojanca pod nazivom Sunburst. Hakeri koriste više sofisticiranih metoda kojima otežavaju ili onemogućavaju otkrivanje napada te skrivaju svoje aktivnosti na napadnutim računalima, a smatra se da su već uspjeli pristupiti računalnim sustavima većeg broja organizacija diljem svijeta.

Nakon uspješnog napada hakeri uspijevaju ukrasti sigurnosne certifikate zaraženih računala pa svoje aktivnosti potom "potpisuju" takvim certifikatima i prikazuju ih kao sasvim legitimne, kao da dolaze od autoriziranih lokalnih korisničkih računa.

Žrtve napada su do sada, među ostalima, bile Državna riznica SAD-a i tamošnje Ministarstvo trgovine, kao i vladine, konzultantske, tehnološke, telekomunikacijske i energetske kompanije iz Sjeverne Amerike, Europe, Azije i Bliskog istoka. Sigurnosni stručnjaci očekuju daljnje napade iste vrste i u drugim državama i granama industrije. Napadi nisu automatizirani niti je malware načinjen tako da se širi samostalno. Naprotiv, svaki od napada na određenu žrtvu pomno je planiran i izveden "ručno" i strogo ciljano. [18]

U SAD-u će se u istragu ovog slučaja uključiti Agencija za kibernetičku sigurnost i infrastrukturu (eng, *Cybersecurity and Infrastructure Security Agency*, CISA) i FBI, a u Bijeloj kući već je održan sastanak vijeća za nacionalnu sigurnost. Strahuje se, naime, da su do sada otkriveni neovlašteni upadi u sustave federalnih tijela i agencija samo vrh ledene sante, odnosno da ih je vrlo vjerojatno neotkriveno značajno više.

S obzirom na to da SolarWindov ranjivi softver koristi velik dio od Fortuneovih top 500 kompanija u SAD-u, isto kao i 10 najvećih telekoma, sve grane Oružanih snaga, pa čak i NSA i ured predsjednika SAD-a, razmjeri napada mogli bi zaista biti neviđeni. Rusija, očekivano, negira umiješanost u ovaj slučaj. [18]

12. SUSTAVI ZA OTKRIVANJE NEOVLAŠTENIH UPADA

Sustav za otkrivanje upada kod nas uvriježenog naziva IDS (eng. *Intrusion detection system*), nadzire mrežni i sistemski promet zbog sumnjivih aktivnosti. Jednom kada se identificiraju potencijalne prijetnje, softver za otkrivanje upada šalje obavijesti da bi na njih upozorio. Najnoviji IDS softver proaktivno će analizirati i identificirati obrasce koji ukazuju na niz tipova kibernetičkih napada. Učinkovito rješenje trebalo bi biti u stanju otkriti sve prijetnje prije nego što se potpuno infiltriraju u sustav.

Sustav za otkrivanje neovlaštenih upada označava dolazni i odlazni zlonamjerni promet, tako da možemo poduzeti proaktivne korake kako bi zaštitili svoju mrežu. Učinkovit IDS informira IT osoblje kako bi moglo brzo i precizno odgovoriti na potencijalnu prijetnju.

Vatrozidi i programi protiv zlonamjernog softvera samo su jedan mali dio cjelovitog pristupa sigurnosti. Kada mreža raste, a nepoznati ili novi uređaji redovito uskaču i izlaze, potreban vam je softver za otkrivanje upada. Ovaj softver trebao bi snimati snimke cijelog vašeg sustava, koristeći znanje o potencijalnim upadima kako bi ih proaktivno spriječio. Softver sustava za otkrivanje upada obično se kombinira s komponentama dizajniranim za zaštitu informacijskih sustava kao dio šireg sigurnosnog rješenja. Punopravno sigurnosno rješenje također će sadržavati mjere kontrole autorizacije i provjere autentičnosti kao dio svoje obrane od upada.

Iako je ovo osnovna funkcija i svrha softvera za otkrivanje upada, nisu svi programi jednaki. Neki omogućuju provođenje pravila koja program zatim koristi za informiranje i izvršavanje određenih radnji i zadataka, dok drugi ne. Dostupne su i opcije IDS-a otvorenog koda, koje se mogu značajno razlikovati od softvera zatvorenog koda, pa je važno razumjeti nijanse sustava za otkrivanje upada u mrežu otvorenog koda prije nego što ga odaberete.

Najnoviji IDS programi vjerojatno će sadržavati specijalne i napredne značajke, pa vrijedi razmisliti koliko bi ove sofisticiranije komponente bile korisne za vaše poslovanje. Uostalom, možda neće biti isplativo za organizaciju s minimalnim zahtjevima za otkrivanje upada u mrežu da odabere najnapredniji i najnoviji IDS softver. [19]

12.1. Vrste sustava za otkrivanje neovlaštenih upada

Sustav za otkrivanje upada dolazi u dvije vrste: sustav za otkrivanje upada zasnovan na domaćinu (eng. *host-based intrusion detection systems*, HIDS) ili mrežni sustav za otkrivanje prodora (eng. *network intrusion detection systems,* NIDS). Jednostavnije rečeno, HIDS sustav ispituje događaje na računalu povezanom na vašu mrežu, umjesto da istražuje promet koji prolazi kroz sustav. Kao što mu samo ime govori, temelji se na hostu. S druge strane, NIDS ispituje mrežni promet. [19]

12.1.1. Mrežni sustav za otkrivanje neovlaštenih upada

Kao sustav koji ispituje i analizira mrežni promet, mrežni sustav za otkrivanje upada mora standardno sadržavati njuškalicu paketa koja okuplja mrežni promet. Iako se NIDS-ovi mogu razlikovati, oni obično uključuju mehanizam za analizu zasnovan na pravilima, koji se može prilagoditi vlastitim pravilima. U nekim slučajevima NIDS-ovi imaju korisničku zajednicu koja donosi pravila koja možete izravno uvesti kako bi uštedjeli vrijeme.

NIDS pravila također olakšavaju selektivno prikupljanje podataka. To je neophodno jer ako sav promet pohranite u datoteke ili ga pokrećete kroz nadzornu ploču, analiza podataka bila bi gotovo nemoguća. Dakle, ako imate pravilo dizajnirano za označavanje sumnjivog HTTP prometa, vaši će NIDS filtrirati nebitne podatke i pohraniti samo HTTP pakete s određenim karakteristikama. To sprječava da sustav bude preopterećen.

NIDS program obično se instalira na određenu opremu. Vrhunska rješenja za poduzeća obično se isporučuju u obliku mrežnog kompleta s ugrađenim programom. NIDS zahtijeva senzorski modul za prikupljanje prometa, ali ne morate nužno platiti skupi hardver. Možete učitati senzorski modul na LAN analizator ili odrediti uređaj za pokretanje zadatka. Samo osigurajte da uređaj koji odaberete ima dovoljno takta; u protivnom će vaša mreža zaostati. [19]

12.1.2. Sustav za otkrivanje neovlaštenih upada temeljen na hostu

Umjesto da istražuju promet, sustavi za otkrivanje upada utemeljeni na hostu istražuju događaje na računalu povezanom na vašu mrežu, uvidom u administrativne podatke. To obično uključuje datoteke konfiguracije i dnevnika. HIDS će sigurnosno kopirati vaše konfiguracijske datoteke, tako da možete vratiti prethodne postavke ako virus utječe na sigurnost sustava mijenjajući postavke uređaja. Također ćete se htjeti obraniti od korijenskog (eng. *root*) pristupa na platformama sličnim Unixu ili promjenama registra sustava Windows. HIDS ne može blokirati ove promjene, ali trebao bi vas obavijestiti kako biste mogli djelovati kako biste ih ispravili ili spriječili.

Hostovi koje nadziru HIDS-ovi moraju imati instaliran softver. Vaš HIDS može nadzirati samo jedan uređaj ako želite, ali uobičajeno je instalirati HIDS na svaki dio opreme povezan na vašu mrežu. To sprječava zanemarivanje bilo kakvih promjena konfiguracije na uređajima. Međutim, ako imate HIDS na svakom uređaju, prijava na svaki pojedinačno za pristup podacima dugotrajna je i radno zahtjevna. Zbog toga će vam trebati distribuirani HIDS sustav s centraliziranom konzolom ili upravljačkim modulom, tako da povratne informacije za svaki host možete pregledavati s jednog mjesta. Za sustav koji odaberete važno je šifrirati podatke koji prolaze između hostova i centralizirane konzole. [19]

12.1.3. NIDS nasuprot HIDS-u

NIDS pruža daleko veći kapacitet praćenja nego što to može HIDS, omogućujući vam presretanje kibernetičkih napada u stvarnom vremenu. S druge strane, HIDS je u stanju identificirati ako nešto nije u redu samo kad je postavka ili datoteka već promijenjena. Kombinacijom ova dva sustava možete postići preventivno i odgovorno rješenje. Imati HIDS je važno jer je HIDS aktivnost manje agresivna od NIDS aktivnosti - za početak, HIDS ne bi trebao koristiti toliko središnje jedinica za obradbu (eng, *Central processing unit*, CPU). Nijedna vrsta sustava ne generira mrežni promet. [19]

12.2. Metodologija otkrivanja neovlaštenih upada

Sustav za otkrivanje upada zasnovan na hostu i mrežni sustav za otkrivanje proboja imat će dva načina rada: zasnovan na potpisu i anomaliji. Gotovo svi IDS-ovi koriste oba načina, iako neki mogu koristiti samo jedan ili drugi način. [19]

12.2.1. IDS na temelju potpisa

Pristup IDS-u zasnovan na potpisu usredotočen je na identificiranje "potpisa" neovlaštenih upada. To može biti u obliku poznatog identiteta ili možda uzorka. Većina IDS-a koristi pristup zasnovan na potpisu.

Da bi ovaj način bio uspješan, treba ga redovito ažurirati, tako da razumije koji su identiteti i potpisi zajednički. Ti se identiteti i potpisi mijenjaju i razvijaju. Drugim riječima, ako napadač dovoljno detaljno promijeni detalje o načinu izvršavanja napada, možda će moći izbjeći pozornost IDS-a temeljenog na potpisu, jer IDS ne može pratiti promjene. Potpuno nove vrste napada također se mogu provući jer još uvijek ne postoje u IDS bazi podataka. Kako baza podataka raste, opterećenje obrade postaje veće. [19]

12.2.2. IDS zasnovan na anomaliji

Otkrivanje temeljeno na anomaliji, kao što mu samo ime govori, usredotočeno je na prepoznavanje neočekivanih ili neobičnih obrazaca aktivnosti. Ova metoda kompenzira sve napade koji prođu pored pristupa identificiranja uzorka temeljenog na potpisu. Međutim, prethodno nepoznato, ali unatoč tome valjano ponašanje, ponekad se može slučajno označiti.

IDS zasnovan na anomaliji dobar je za prepoznavanje kada netko istražuje mrežu, što može pružiti snažnu naznaku skorog napada. Primjeri anomalije uključuju višestruke neuspjele pokušaje prijave i neobične aktivnosti na portovima.

S NIDS-om pristup zasnovan na anomaliji znači da ćete trebati uspostaviti osnovno ponašanje, tako da sustav zna što se smatra "standardnom" aktivnošću. To pomaže sustavu da označi sve što se ne uklapa ili što bi se smatralo nenormalnim. [19]

12.2.3. IDS na temelju potpisa nasuprot IDS-a na osnovi anomalije

Metodologija koja se temelji na potpisu obično je brža od otkrivanja na temelju anomalija, ali u konačnici sveobuhvatan softver za otkrivanje upada mora ponuditi postupke potpisivanja i anomalija. To je zato što postoje prednosti i nedostaci softvera za otkrivanje upada koji se temelji na potpisu i na anomalijama, a koji se velikim dijelom nadoknađuju kada se to dvoje kombinira. [19]

12.3. Sustavi za sprječavanje upada

Sustavi za sprječavanje upada kod nas uvriježenog naziva IPS (eng. *intrusion prevention system*) i IDS softver grane su istog stabla i koriste slične tehnologije. Otkrivanje olakšava prevenciju, tako da IPS i IDS moraju raditi u kombinaciji da bi bili uspješni.

Ključna razlika između ovih protuprovalnih sustava je što je jedan aktivan, a drugi pasivan. Tipični nadzornik upada koji vas upozorava kada je nešto neobično ili sumnjivo može se nazvati pasivnim IDS-om. Sustav koji detektira i djeluje kako bi spriječio štetu i daljnje napade nazvao bi se reaktivnim. To je zato što reagira na upad, a ne samo da ga identificira.

Reaktivni IPS ili IDS obično ne implementira rješenja sam, već komunicira s aplikacijama i vatrozidima podešavajući njihove postavke. Reaktivni HIDS može komunicirati s više mrežnih pomagala, s ciljem vraćanja postavki uređaja. To mogu biti postavke jednostavnih protokola za upravljanje mrežom ili postavke upravitelja konfiguracija instaliranog na uređaju. Ako se napad pokrene na administratora, na to se ne može odgovoriti automatskim blokiranjem administratorske upotrebe ili promjenom lozinke za sustav. To je zato što bi na taj način zaključalo korijenskog (eng. *root*) korisnika izvan poslužitelja i mreže. [19]

Korisnici IDS-a ponekad se žale da su dobili poplave lažno pozitivnih rezultata kad su prvi put postavili IDS. Vaš će IPS automatski primijeniti obrambenu strategiju, na temelju otkrivanja upozorenja. Ako IPS nije pravilno kalibriran, to može prouzročiti kaos i dovesti do potpunog zaustavljanja vaše autentične mrežne aktivnosti.

Možete smanjiti broj lažno pozitivnih rezultata i umanjiti ometanje mreže uvođenjem vaših IDS-a i IPS-a u fazama. Možete prilagoditi okidače, kombinirati uvjete upozorenja i stvoriti upozorenja po mjeri. Kombinacijom uvjeta postaju složeniji, što može smanjiti vjerojatnost pojave lažnih pozitivnih rezultata. Međutim, teško je u potpunosti iskorijeniti lažne pozitivne rezultate bez rizika da sumnjiva aktivnost prođe kroz vašu obranu. Trebali biste težiti postizanju poštene ravnoteže, bez ugrožavanja vaše sigurnosti. Procesi otkrivanja i sprječavanja upada trebali bi imati mogućnost precizno usklađene interakcije s vatrozidima kako bi se osiguralo da istinski korisnici nisu zaključani i da autentična mrežna aktivnost nije poremećena. [19]

12.3. Izazovi upravljanja IDS-om

Tri su glavna izazova povezana s upravljanjem IDS-om.

Prvi izazov odnosi se na identificiranje lažnih pozitivnih rezultata. Ako IDS nije ažuran i prikladno dotjeran, što samo po sebi oduzima puno vremena, gubi se više vremena za suočavanje s lažnim pozitivnim rezultatima. Mnoge se organizacije koriste sekundarnom platformom za analizu, poput sigurnosnog incidenta i upravitelja događaja, kako bi im pomogle da analiziraju i istražuju upozorenja na učinkovitiji način. U osnovi, kada IDS generira upozorenje, ono se šalje sekundarnom sustavu analize, koji pomaže u rješavanju problema s lažno pozitivnim rezultatima.

Drugi izazov je kadroviranje. Razumijevanje konteksta prijetnji i sumnjivih aktivnosti izuzetno je važan aspekt upravljanja IDS-om. Širi se kontekst mijenja svaki dan, jer kibernetički kriminalci pokušavaju ići u korak sa sigurnosnim softverom. Uz to, svaki IDS implementiran je u određeni kontekst dotične organizacije. Da biste upravljali složenošću poslovno specifičnog konteksta i šireg konteksta, morate imati pristup obrazovanom i obučenom analitičaru sustava. IDS-ov analitičar prilagodit će IDS kontekstu, ali pronalazak nekoga tko ima vjerodajnice i iskustvo da to učinkovito učini nije jednostavan zadatak.

Treći izazov je utvrđivanje stvarnih rizika. Lažni pozitivi mogu biti dugotrajni i glomazni, ali nedostatak legitimne prijetnje može biti još gori. S IDS-om potrebno je znati prirodu napada da bi ga se prepoznalo i spriječilo. Stručnjaci to nazivaju problemom "nulte nule": netko se mora razboljeti prije nego što u budućnosti budete mogli prepoznati bolest. [19]

13. ZAKLJUČAK

Glavni cilj zaštite podataka je osigurati podatke od oštećenja pri prijenosu i spriječiti neovlaštene upade ili preusmjeravanje podataka. Nepravilno rukovanje podacima što uključuje brisanje i prepisivanje datoteka donosi veliki dio gubitaka informacija. Zbog važnosti izgubljenih podataka razvijeni su različiti alati koji služe za obnovu podataka. Ti programi omogućuju obnovu izbrisanih podataka, izradu sigurnosnih kopija, provjeru konzistentnosti sustava i dr. Podatke je osim gubitka potrebno zaštiti i od krađe što možemo učiniti enkripcijom podataka, maskiranjem podataka ili ako je rizik od krađe podataka velik, čak i brisanjem samih podataka.

Problemi privatnosti i sigurnosti na internetu najveći su problemi pri upotrebi interneta. Povećanjem broja korisnika i primjene interneta povećava se i mogućnost zlouporabe na internetu. Opasnosti na internetu su raznolike od raznih oglasa i reklamnih poruka kao mogućih nositelja malicioznog koda, preko provale u računala i mobitele te krađe njihovih podataka, pa do slanja virusa koji korisniku i tvrtkama mogu nanijeti veliku štetu. Zbog novih načina prikupljanja i obrade podataka javila se potreba za novom regulativom koji bi korisnicima dala više nadzora i prava nad prikupljanjem i korištenjem njihovih podataka. Europska unija tim je povodom donijela uredbu (Opća uredba o zaštiti podataka) kojom se regulira zaštita podataka i privatnost osoba unutar Europske unije, a donosi i propise vezane za iznošenje podataka u treće zemlje.

Mrežna sigurnost ključni je element za sigurnost svake tvrtke, ali i pojedinca. Svako računalo povezano na mrežu potrebno je zaštiti od neovlaštenog pristupa. Sigurnost i zaštita podataka postižu se nadzorom mrežnog i sistemskog prometa, te uočavanjem sumnjivih aktivnosti. Sustav za otkrivanje neovlaštenih upada označava dolazni i odlazni zlonamjerni promet, tako da možemo poduzeti proaktivne korake kako bi zaštitili svoju mrežu. Smatram da kvalitetnu zaštitu mreže možemo postići kombiniranjem sustava za otkrivanje neovlaštenih upada zasnovanih na mreži i domaćinu, te implementacijom sustava za sprečavanja upada kao aktivnog elementa sigurnosnog sustava. Jedan od većih problema koje susrećemo u primjeni sustava za otkrivanje neovlaštenih upada je identificiranje lažno pozitivnih rezultata, stoga je potrebno sustav uvijek održavati ažuriranim.

14. LITERATURA

[1] IBM, „Why is data security important“, dostupno na: https://www.ibm.com/ (31. ožujka 2021.)

[2] CARNet CERT, „ Obnavljanje izgubljenih podataka“, dostupno na: https://www.cis.hr/ (18. prosinac 2019.)

[3] CARNet CERT, „ Životni ciklus podataka“, dostupno na: https://www.cis.hr/ (17. veljače 2021.)

[4] Samuel H. Russ, „Three Ways to Hack a Printed Circuit Board?“, dostupno na: https://spectrum.ieee.org/ (31. ožujka 2021.)

[5] ESET, „Što je enkripcija“, dostupno na: https://encryption.eset.com/hr/ (19. prosinac 2019.)

[6] Wikipedia, „Zaštita podataka“, dostupno na: https://hr.wikipedia.org/ (18. prosinac 2019.)

[7] Prolić M., „Sigurnost rada na računalu“ završni preddiplomski rad, Sveučilište u Splitu, Prirodoslovno - matematički fakultet, Hrvatska, 2012.

[8] Federal Information Processing Standards Publications, „Electronic Data Interchange“, dostupno na: https://web.archive.org/ (31. ožujka 2021.)

[9] Wikipedia „Electronic data interchage“ dostupno na https://en.wikipedia.org (10.veljače.2021.)

[10] Wikipedia „Data breach“ dostupno na https://en.wikipedia.org (19.veljače.2021.)

[11] Narodne novine, „Zakon o zaštiti osobnih podataka“ (NN 103/03, 118/06, 41/08, 130/11 i 106/12 - pročišćeni tekst), dostupno na: https://narodne-novine.nn.hr/ (17. veljače 2021.)

[12] CARNet CERT, „Zakon o zaštiti osobnih podataka“, dostupno na: https://www.cis.hr/ (17. veljače 2021.)

[13] EUR-Lex, „Opća uredba o zaštiti podataka“ (EU 2016/679), dostupno na: https://eur-lex.europa.eu/ (31. ožujka 2021.)

[14] Narodne novine, „Zakon o provedbi Opće uredbe o zaštiti podataka“ (NN 42/2018), dostupno na: https://narodne-novine.nn.hr/ (17. veljače 2021.)

[15] M. Bukovac Puvača, A. Demark „Pravo na zaštitu osobnih podataka“, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 40, br. 1, 287-315 (2019)

[16] European Commision „Cyber Security in the Energy Sector“, dostupno na: https://ec.europa.eu/ (5. veljače 2021.)

[17] Tim Greene „Dropbox cloud was a haven for data thieves, researchers say“, dostupno na: https://www.computerworld.com (23. veljače 2021.)

[18] Sandro Vrbanus „Nova hakerska akcija distribucije trojanca navodno stiže iz Rusije“, dostupno na: https://www.bug.hr (23. veljače 2021.)

[19] IDS Systems „7 Best Intrusion Detection Software and Latest IDS Systems“, dostupno na: https://www.dnsstuff.com (25. veljače 2021.)

15. PRILOZI

15.1. Popis slika