Centar Informacijske Sigurnosti

Pregled EU propisa na području informacijske sigurnosti

travanj 2012.

CIS-DOC-2012-04-047

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Politiku informacijske sigurnosti primarno određuje okruženje u kojem se ona koristi. Zbog brzog razvoja informacijske i komunikacijske tehnologije, kao i sveprisutnosti Interneta i složenog sigurnosnog okruženja sigurnosni rizici su iznimno porasli tijekom posljednjih dvadesetak godina. Uslijed globalizacije i raspada hladnoratovske podjele svijeta, došlo je i do promjene koncepta prijetnji, gdje su hladnoratovske blokovske prijetnje ustupile mjesto globaliziranim prijetnjama terorizma, u svim mogućim oblicima i na svim mogućim područjima. Kako bi se moglo odgovoriti na ovakve prijetnje dolazi do promjene u pristupu kod tri ključna elementa politike informacijske sigurnosti (osoba, procesa i tehnologija). Novi pristup mora biti upravljan prije svega novim okruženjem sveopće globalizacije, sve većom ovisnosti poslovnih procesa o tehnologiji, ali i transformacijom tržišnog društva temeljenog na privatnom vlasništvu u informacijsko društvu temeljenom na znanju – informacijama.

Zbog toga je osnovna namjena sigurnosne politike Europske unije (eng. *European Union, EU*)[1] zaštita integriteta, dostupnosti i tajnosti informacija te informacijskih sustava. Vijeće EU (engl. *Council of the European Union*) glavna je zakonodavna institucija Europske unije te je usvojilo konvencije, europske sporazume, pripadajuće protokole i preporuke kojima se nastoji regulirati pitanje mrežne i informacijske sigurnosti.

U drugom poglavlju govorit će se o važnosti uspostavljanja zakonodavnog okvira o informacijskoj sigurnosti te će se objasniti važniji pojmovi povezani s informacijskom sigurnošću. Sljedeće poglavlje opisuje ciljeve i zahtjeve koje europsko zakonodavstvo mora ispuniti na tom području. U četvrtom poglavlju navest će se najvažniji propisi s područja informacijske sigurnosti, kao i oni koji su važni za omogućavanje kvalitetne sigurnosne politike.

[1] **Europska unija** jedinstvena je međuvladina i nadnacionalna zajednica europskih država, nastala kao rezultat procesa suradnje i integracije koji je započeo 1951. godine između šest država (Belgije, Francuske, Njemačke, Italije, Luksemburga i Nizozemske). Europska unija formalno je uspostavljena 1. studenoga 1993. godine, stupanjem na snagu Ugovora o Europskoj uniji (poznatiji kao Ugovor iz Maastrichta). Europska unija danas broji 27 država članica. Prostire se na 4.325.675 km², a broji oko 502 milijuna stanovnika.

2. Zakonodavstvo Europske Unije na području informacijske sigurnosti

Uspostavljanjem sustava informacijske sigurnosti i upravljanjem ovim sustavom u svim segmentima potrebnim za jednu suvremenu zemlju, javna uprava obavlja svoju ulogu u okviru izgradnje informacijskog društva. Takvu ulogu javna uprava ima i u okviru tradicionalnog društva. Organizacija tradicionalnog društva počiva na sprečavanju potencijalnih prijetnji društvu te na brizi o razvoju zaštitnih i represivnih mjera. Na sličan način informacijska sigurnost predstavlja temelje za stvaranje i organizaciju informacijskog društva. Razvojem informacijske sigurnosti uspostavljaju se preventivne mjere te se stvaraju organizacijsko-tehničke pretpostavke za sustavni razvoj zaštitnih i represivnih postupaka u okviru informacijskog društva. Sustavom informacijske sigurnosti državna uprava stvara i temelje za formalni razvoj metoda i postupaka temeljenih na metodama računalne forenzike, ali i za prijelaz zakonodavstva iz tradicionalnih okvira u informacijsko društvo. Sve ove procese nije moguće uspješno provesti bez dobro razvijene informacijske sigurnosti na nacionalnoj razini. U tom procesu nužna je uloga državne vlasti, ali i propisa Europske unije kao čvrste pokretačke snage ovakvog procesa, koji treba doprijeti u sve pore jednog suvremenog društva. Slika 1. pokazuje zastavu Europske unije i najvišu domenu na području Europske unije.

Slika 1. Zastava i domena EU
Izvor: ukrfid.com

Aktualne promjene u zakonodavstvu EU u posljednjih nekoliko godina usmjerene su uvelike na razvoj sigurnosne politike EU i slijede iskustvo sigurnosnog modela Organizacije Sjevernoatlantskog ugovora (eng. *North Atlantic Treaty Organization, NATO*), stečenog u dugogodišnjem multinacionalnom okruženju. Stoga će i za sve buduće članice EU prepoznavanje važnosti ovog područja te sustavan pristup sigurnosti na nacionalnoj razini biti jedan od kriterija zrelosti zemlje kandidata.

Istraživanja provedena u razvijenim zemljama Europske unije i svijeta pokazuju da financijske investicije i tehnološka dostignuća nisu dovoljni za stvaranje informacijskog društva. Sve razvijene zemlje posljednjih godina se ubrzano i intenzivno okreću programima informacijske sigurnosti u svim segmentima državnog i gospodarskog sektora, ali i programima razvoja sigurnosne kulture u najširim slojevima društva. Ako se uspoređuje iskustvo tradicionalnog društva sa suvremenim informacijskim društvom kojem težimo, lako je uočiti kako je razvoj tradicionalnog društva prošao sve faze razvoja opće sigurnosne politike te ih se ne može izbjeći ni u razvoju informacijskog društva. Za usporedbu možemo uzeti tradicionalno područje prometa, u kojemu razvoj i primjenu prometnih tehnologija i resursa nije moguće odvojiti od područja sigurnosti u prometu, a preventivne i represivne mjere međusobno se prožimaju i ravnopravno razvijaju te su prisutne u životu svakog građanina počevši od njegove najranije dobi i predškolskih programa.

2.1. Opći pojmovi

Prije opisa i objašnjenja sigurnosnih mjera potrebno je definirati osnovne pojmove koji se koriste u informacijskoj sigurnosti, tj. definirati što je to podatak, informacija, informacijski sustav, itd.

Najvažniji pojmovi na području informacijske sigurnosti su:

- **podatak**: skup prepoznatljivih znakova zapisanih na određenom mediju,
- **informacija**: podatak s određenim značenjem, odnosno saznanje koje se može prenijeti u bilo kojem obliku (pisanom, audio, vizualnom, elektroničkom ili nekom drugom),
- **informacijski sustav**: svaki sustav kojim se prikupljaju, pohranjuju, čuvaju, obrađuju, prikazuju, dohvaćaju i isporučuju informacije tako da budu dostupne i upotrebljive za svakoga tko ima pravo njima se koristiti,
- **informatička oprema**: fizički uređaji i/ili sredstva koja čine informacijski sustav,
- **informacijska sigurnost**: definira se kao očuvanje:
  - **povjerljivosti** – osiguranje da je informacija dostupna samo onima koji imaju ovlašteni pristup istoj,
  - **integriteta** – zaštita postojanja, točnosti i cjelokupnosti informacije kao i procesnih metoda,
  - **raspoloživosti** – osiguranje da autorizirani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva,
- **zaštita**: skup mjera za očuvanje sigurnosti,
- **nadzor:** provjera učinkovitosti sustava zaštite,
- **odgovornost**: ponašanje po zadanom skupu pravila,
- **ovlaštenje**: pravo postupanja u zadanim okvirima,
- **vlasnici podataka**: odgovorni za sve radnje s podacima koji su u njihovoj nadležnosti, tijekom životnog ciklusa podataka. Pri tome, radnje s podacima podrazumijevaju nastajanje, obrađivanje, pohranjivanje i arhiviranje podataka,
- **informacijska infrastruktura**: obuhvaća svu infrastrukturu u određenom državnom tijelu ili pravnoj osobi koja na bilo koji način utječe na temeljna svojstva povjerljivosti, dostupnosti ili cjelovitosti podataka i u okviru koje podaci nastaju, obrađuju se ili pohranjuju,
- **vlasnici informacijske infrastrukture**: odgovorni za planiranje i provođenje organizacijskih i tehničkih mjera u skladu s važećim propisima informacijske sigurnosti,
- **pravo pristupa i korištenja informacijskih resursa:** određuje se isključivo po načelu poslovne potrebe (eng. *need to know*), a ne po hijerarhijskom konceptu ranga radnog mjesta,
- **sigurnosna akreditacija**: postupak u kojem mjerodavno neovisno akreditacijsko tijelo službeno potvrđuje pravnoj ili fizičkoj osobi sposobnost provođenja određenih poslova. Odnosi se na provjeru sposobnosti pravnih osoba za provođenje procesa informacijske sigurnosti, sukladno mjerodavnim propisima informacijske sigurnosti. Proces informacijske sigurnosti sastoji se od niza propisanih mjera i metoda uvedenih u obliku organizacijskih i tehničkih provjera u poslovne procese određene pravne osobe ili državnog tijela,
- **sigurnosno akreditacijsko tijelo**: neovisna pravna osoba ovlaštena zakonom ili ona koju akreditira određeno središnje akreditacijsko tijelo, koja obavlja provjeru sposobnosti pravnih osoba za provođenje procesa informacijske sigurnosti u okviru vlastitog poslovnog procesa,
- **potvrda o sigurnosnoj akreditaciji**: akreditacijsko tijelo općenito izdaje potvrdu o akreditaciji pravnoj ili fizičkoj osobi za koju se utvrdi da ispunjava zahtjeve akreditacijskog procesa. Potvrda o sigurnosnoj akreditaciji označava zadovoljavanje propisanih zahtjeva procesa informacijske sigurnosti koju izdaje određena pravna osoba ili državno tijelo. Potvrda o akreditaciji izdaje se uvijek na ograničeni vremenski rok. Uobičajeni rokovi za sigurnosne akreditacije su dvije, četiri i pet godina. Istekom akreditacijskog roka provodi se ponovna provjera, koja osim propisanih zahtjeva procesa informacijske sigurnosti ima za cilj utvrditi i kvalitetu upravljanja životnim ciklusom podataka, informacijske infrastrukture, fizičke sigurnosti i osoblja. Potvrdom o sigurnosnoj akreditaciji daje se ovlast za obavljanje određenih poslova,

- **sigurnosni certifikat**: potvrda o sukladnosti određenog proizvoda, procesa ili usluge s nacionalnom normom ili formalnim tehničkim zahtjevima za proizvode, procese ili usluge. Sigurnosni certifikat odnosi se na osobe, proizvode ili sustave informacijske sigurnosti. Sigurnosnim certificiranjem se omogućuje korištenje pojedinih tržišnih proizvoda u propisanim uvjetima s ciljem sustavnog ostvarivanja projekata informacijske infrastrukture. Primjerice proizvod tvrtke X, model Y, tip Z u inačici W, može se koristiti za razmjenu podataka u državnoj upravi do stupnja tajnosti „službena tajna – tajno“,
- **sigurnosno certifikacijsko tijelo**: laboratorij neovisan o dobavljaču, potvrdbeno tijelo, nadzorno ili drugo tijelo koje sudjeluje u postupku ocjenjivanja sukladnosti. Sigurnosno certificiranje za potrebe tijela državne vlasti uobičajeno se organizira u središnjim državnim tijelima za sigurnost komunikacija (eng. *National Communications Security Authority, NCSA*). Temeljni posao sigurnosnog certifikacijskog tijela je formiranje i redovito ažuriranje liste certificiranih proizvoda za upotrebu u nacionalnom sustavu informacijske sigurnosti. Postupci provođenja certificiranja sastoje se od laboratorijskih provjera i/ili preuzimanja određenih međunarodnih lista certifikata po utvrđenoj metodologiji. Liste certificiranih proizvoda koriste se u procesu sigurnosnog akreditiranja,
- **tijela javne vlasti:** državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i druge osobe na koje su prenesene javne ovlasti.

3. Ciljevi i zahtjevi Europske politike informacijske sigurnosti

Cilj europske politike mrežne i informacijske sigurnosti je poboljšati postojeće nedovoljne propise i podignuti razinu svijesti o računalnom kriminalu na području cijele Europe. Također, namjera joj je okupiti države članice u informacijsku zajednicu kako bi se mogle zajedničkim snagama uspješnije boriti protiv računalnog kriminala i zlonamjernih napadača.

Vijeće EU donijelo je propise i zakone o sigurnosnoj politici u kojima se opisuju aktivnosti u području mrežne i informacijske sigurnosti za zemlje članice kojima je cilj:

- podizanje svijesti putem javnog informiranja te edukacijom,
- osnivanje zajedničkog CERT-a (engl. *Computer Emergency Response Team*), ali i nacionalnih CERT-ova, organizacija s ciljem učinkovitog odgovora na sigurnosne incidente,
- tehnološka podrška za istraživanja i razvoj sigurnosti te stvaranje strategije unapređenja mrežne i informacijske sigurnosti,
- promocija standardizacije i certifikacije u informacijskoj sigurnosti putem postojećih sigurnosnih standarda,
- usklađivanje propisa na državnoj razini,
- međunarodna suradnja na području mrežne i informacijske sigurnosti.

Sigurnosna politika namijenjena trima glavnim skupinama:

- građani: mora im se osigurati zaštita osobnih podataka koja predstavlja osnovni uvjet individualne slobode u demokratskoj državi,
- tvrtke: potrebno je štititi intelektualno vlasništvo, ali i osobne podatke građana, poticati konkurentnost i produktivnost. Ovi zahtjevi se moraju osigurati primjenjivanjem sigurnosne politike na složenim računalnim sustavima,
- državni aparati: odgovorni su za zaštitu osjetljivih i povjerljivih podataka te za osiguranje dugoročnog pozitivnog poslovanja državnih institucija i infrastrukture.

Sigurnost informacija se omogućuje donošenjem i ispunjavanjem tehničkih, operacijskih i zakonskih uvjeta. Sigurnosna politika mora osigurati zaštitu osobnih sloboda, primjenu strogih sigurnosnih provjera te osiguravanje računalnih i ljudskih resursa.

Sigurnosni zahtjevi mrežne i informacijske sigurnosti koji se moraju osigurati sastoje se od slijedećih važnih i povezanih značajki:

- dostupnosti podataka,
- integriteta podataka i
- tajnosti podataka.

Mrežnu i informacijsku sigurnost se može definirati kao sposobnost obrane informacijskog sustava i mreže od gubitka dostupnosti, narušavanja integriteta i kompromitiranja tajnosti informacija. Ovo se odnosi na informacije koje su spremljene ili se prenose uporabom određenih usluga, a mogu biti ugrožene nenamjernim događajima ili zlonamjernim djelovanjem.

Glavni ciljevi informacijske sigurnosti su:

- zaštita povjerljivih informacija od kompromitiranja, špijunaže i neovlaštenog korištenja,
- zaštita informacija koje se razmjenjuju putem informacijskih sustava i mreža od narušavanja integriteta i dostupnosti,
- zaštita informacija od sabotaže i zlćudnih namjera,
- ograničavanje posljedica i usvajanje potrebnih dopunskih mjera u slučaju napada zlonamjernih osoba ili nekog drugog načina ugrožavanja informacija.

Sigurnosne mjere moraju biti osmišljene kako bi:

- osigurale dostupnost, integritet i tajnost podataka,
- osigurale pristupanje podacima na temelju prioriteta,
- onemogućile neovlašten pristup povjerljivim podacima,
- osigurale identifikaciju osoba čiji položaj može ugroziti sigurnost povjerljivih podataka.

Važan temelj za sigurnost je klasifikacija informacija. Zbog toga je potrebno posvetiti posebnu brigu pravilnoj klasifikaciji prema određenim razinama kako ne bi došlo do pretjerane ili nedostatne klasifikacije informacija. Sigurnosna politika EU primjenjuje se za klasificirane informacije na području EU. Pod pojmom EU klasificirane informacije podrazumijeva se bilo koja informacija ili materijal čije neovlašteno korištenje može uzrokovati potencijalnu štetu interesima Unije ili nekoj od zemalja članica.

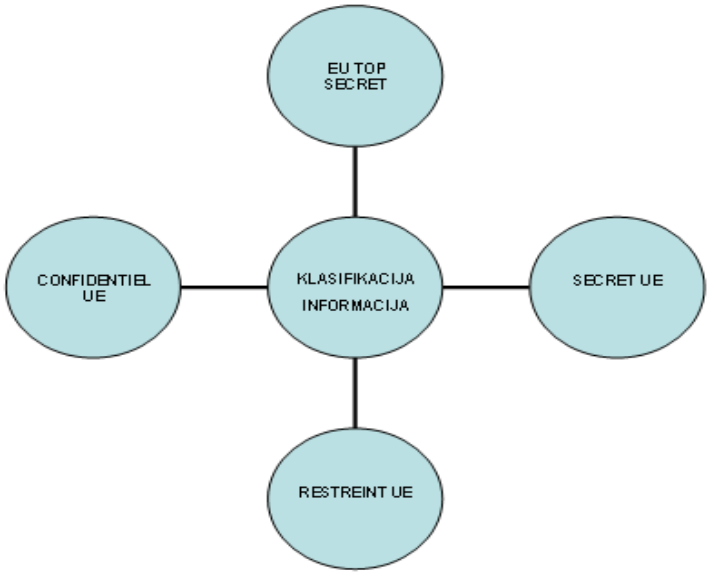
Prema sigurnosnoj politici EU pod dokumentima se podrazumijevaju pisma, bilješke, zapisnici, izvješća, memorandumi, poruke, skice, fotografije, dijapozitivi, filmovi, mape, grafikoni, matrice, trake pisaćih mašina ili pisača, trake, kazete, računalni diskovi, CD ROM uređaji, ili bilo koji drugi fizički medij na kojem se informacija može spremiti i prenositi.

U EU postoje 4 razine klasificiranja informacija:

- strogo povjerljivo (fra. très secret ue / eng. eu top secret): ova oznaka pridaje se informacijama i materijalima čije neovlašteno otkrivanje može izazvati izuzetno ozbiljnu štetu interesima Europske unije ili nekoj od zemalja članica,
- tajno (fra. secret ue): ova oznaka pridaje se informacijama i materijalima čije neovlašteno korištenje može izazvati ozbiljnu štetu interesima Europske unije ili nekoj od zemalja članica,
- povjerljivo (fra. confidentiel ue): ova oznaka pridaje se informacijama i materijalima čije neovlašteno korištenje može izazvati štetu interesima Europske unije ili nekoj od zemalja članica,
- ograničeno (fra. restreint ue): ova oznaka pridaje se informacijama i materijalima čije neovlašteno korištenje može biti nepogodno za interese Europske unije ili neke od zemalja članica.

Potrebno je provoditi ponovni pregled svake klasificirane informacije. Organizacije i institucije koje rade s povjerljivim informacijama trebaju slijediti standardiziran način klasifikacije i zaštite iste razine povjerljivih informacija.

Slika 2 prikazuje razine klasifikacije informacija u Europskoj uniji.



Slika 2. Klasificiranje informacija
Izvor: CIS

Pri upravljanju povjerljivim podacima važno je voditi računa o tome da:

- podaci trebaju biti povjerljivi samo kada je to nužno i opravdano te moraju biti jednoznačno označeni, a klasifikacijska oznaka treba važiti onoliko dugo koliko je to potrebno,
- je za klasifikaciju podataka odgovoran vlasnik podataka,
- je potrebno poštivati jasno određenu proceduru za klasifikaciju podataka,
- klasificiranim podacima klase „strogo povjerljivo“ treba imati pristup što manji broj osoba.

Važno je voditi računa o dodijeljivanju klasifikacija informacija sukladno opisima određenih razina klasifikacija informacija prilikom postupka klasifikacije informacija. Moguće je da se unutar jednog dokumenta pojavi određeni dio koji ima drugačiju razinu klasifikacije te se tada taj dio mora tako i označiti, no cjelokupni dokument dobiva onu razinu klasifikacije koja je jednaka najvišoj razini barem jednog dijela dokumenta.

Jednom klasificirani dokumenti mogu se deklasificirati te im se može smanjiti razina klasifikacije, međutim taj postupak mora biti popraćen pisanim dokazom. Ukoliko postoji mogućnost naknadnog smanjivanja razine klasifikacije dokumenta ili njegove deklasifikacije, preporučljivo je prilikom prve klasifikacije dokumenta unijeti datum ili vremenski period u kojem će vrijediti trenutna razina klasifikacije.

Prilikom oblikovnja sigurnosne politike koja će se primjenjivati na području svih država članica Europske unije važno je ustanoviti minimalne sigurnosne standarde koji trebaju biti zadovoljeni. Oni obuhvaćaju:

- ljudske resurse,
- sigurnost informacija,
- sigurnost informacijskih i računalnih sustava,
- fizičku sigurnost,
- razmjenu i prijenos informacija trećim stranama.

Kako bi osigurali potpunu sigurnost informacijskog sustava važno je odrediti smjernice i standarde vezane uz ljudske resurse. Vrlo je bitno obavljati sigurnosnu provjeru zaposlenih prilikom dodjeljivanja ovlaštenja u obavljanju poslova. Ovlaštene osobe koje imaju pristup informacijama klasificirane kao „povjerljivo“ moraju biti provjerene na odgovarajući način prije nego li im se omogući pristup tim informacijama.

Potrebno je provoditi sigurnosne provjere osoblja i u slučaju kada imaju zaduženja koja uključuju tehničke operacije ili održavanje komunikacijskih i informacijskih sustava, a sadrže povjerljive podatke. Pri provođenju provjere važno je utvrditi zadovoljava li osoba slijedeće kriterije:

- neupitnu lojalnost,

- diskreciju i integritet pri rukovanju povjerljivim podacima.

Pojedinac kojem se može dati ovlaštenje za pristup povjerljivim informacijama mora posjedovati osobine poput lojalnosti, pouzdanosti, povjerljivosti te vjerodostojnosti i ne smije predstavljati neprihvatljiv rizik i opasnost za sigurnost povjerljivih informacija.

Važno je osigurati temeljitost postupaka koji propisuju temeljitu provjeru osoba koje:

- imaju pristup informacijama klase „strogo povjerljivo“,
- obavljaju dužnosti koje uključuju dugotrajan pristup većem broju informacija klase „povjerljivo“,
- obavljaju poslove koje zahtijevaju pristup kritičnim komunikacijskim ili informacijskim sustavima preko kojih bi mogli imati mogućnost neovlaštenog pristupa velikom broju povjerljivih podataka te mogu nanijeti veliku štetu svojim zlonamjernim postupcima ili tehničkom sabotažom.

Organizacije, institucije i tijela koja rukuju povjerljivim informacijama ili održavaju važne informacijske i komunikacijske sustave moraju održavati sigurnosnu provjeru osoblja i revizije ovlaštenja koja su dodijeljena individualnom zaposleniku te voditi zapise o tome.

Osobe koje su na važnim položajima i kojima je omogućen pristup povjerljivim informacijama moraju biti dobro upućene u posao koji obavljaju. Upute moraju biti detaljne te se trebaju ponavljati u određenim vremenskim razmacima kako bi se osiguralo sigurno provođenje postupaka prilikom obavljanja posla. Također se preporuča provođenje postupka u kome je osoblje dužno vlastoručnim potpisom potvrditi potpuno razumijevanje sigurnosnih pravila koja se odnose na obavljanje poslova.

Uprava je dužna nadgledati zaposlenike koji imaju pristup povjerljivim podacima te kritičnim informacijskim ili komunikacijskim sustavima. Uz to mora nadgledati i podnositi izvješća o svakom incidentu, uočenim ranjivostima te ostalim sigurnosnim problemima.

Važno je provoditi mjere osiguravanja fizičke sigurnosti. One obuhvaćaju primjenu tehničkih i fizičkih procedura zaštite na mjestima gdje se spremaju povjerljive informacije. Pri tome moraju biti zadovoljeni uvjeti fizičke sigurnosti koji se odnose na široki spektar tehničkih i fizičkih mjera zaštite kojima se štite povjerljivi podaci u skladu sa stupnjem klasifikacije, mogućim ranjivostima te prijetnjama informacijama. Glavni cilj koji se mora postići primjenom fizičkih sigurnosnih mjera jest onemogućavanje neovlaštenog pristupa povjerljivim podacima.

Fizička sigurnost podrazumijeva zaštitu informacija osmišljavanjem i primjenu sustava za nadzor ulaza i izlaza iz prostora u kojem se nalaze povjerljive informacije, i to za, ali i nakon radnog vremena. Fizička sigurnost također obuhvaća i zaštitu zgrada u kojima su smješteni informacijski i komunikacijski sustavi te povjerljive informacije.

Navedene kriterije mora se uzeti u obzir prilikom odabira razine fizičke sigurnosti:

- klasifikacija informacija,
- količina i oblik informacija,
- fizička priroda i smještaj zgrade u kojoj se nalaze informacije.

Prilikom oblikovanja fizičke sigurnosti također je potrebno uzeti u obzir procjenu vrijednosti resursa kao i prijetnje i ranjivosti prema ugroženim resursima.

Prema europskim propisima mrežna i informacijska sigurnost i sigurnosne mjere iz područja fizičke sigurnosti obuhvaćaju:

- sigurne zone za sve razine klasificiranih informacija osim sigurnosne razine klase „ograničeno“,
- administrativne zone za razinu informacija klase „ograničeno“,
- provođenje nadzora ulaza i izlaza u sigurne zone,
- stražarske službe za sigurne zone van radnog vremena,
- sigurnosna spremišta i sefove za spremanje klasificiranih informacija,
- zaključavanje te nadzor i provjeru ključeva i kombinacija za zaključavanje,
- uređaje za nadzor i provjeru pristupa,
- provjerenu sigurnosnu opremu,
- fizičku zaštitu aparata za kopiranje i telefaks uređaja.

Kako bi se zaštitio pristup povjerljivim informacijama neovlaštenim korisnicima, osigurao pristup informacijama ovlaštenim korisnicima te spriječilo mijenjanje ili brisanje informacija koju bi mogle počniti neovlašte osobe trebaju se poduzeti odgovarajuće sigurnosne mjere.

Za pristup informacijama, prema europskoj politici mrežne i informacijske sigurnosti, koristi se načelo trebam-znati (eng. *need-to-know*). Ovim načelom se osigurava pristup informacijama prema potrebama posla koji se obavlja, a ne prema hijerarhijskoj razini zaposlenika.

Sigurnost informacijskih sustava unutar EU poznata je pod nazivom INFOSEC. Ona podrazumijeva nekoliko tipova sigurnosti:

- COMPUSEC - sigurnost podataka na elektroničkim medijima i računalima,
- COMSEC - sigurnost podataka u sustavima za prijenos podataka,
- TECSEC - sigurnost informacijske infrastrukture u određenim prostorijama od različitih vrsta prisluškivanja.

Sigurnost informacijskih sustava uključuje nadgledanje informacijskih sustava kako bi se onemogućile i spriječile sabotaža, špijunaža, terorizam i ostale zlonamjerne aktivnosti. Također podrazumijeva i uzajamno djelovanje i usklađivanje svih strana uključenih u rad informacijskih i komunikacijskih sustava:

- projektanata sustava,
- odgovornih za implementaciju sustava,
- operativnosti informacijskog sustava,
- korisnika informacijskog sustava.

Prilikom stvaranja sigurnosne politike važno je utvrditi procedure prilikom komunikacije s trećim stranama. Trećim stranama smatraju se zemlje članice Europske unije ili međunarodne organizacije. U postupku razmjene informacija između Vijeća EU[2] i trećih strana sigurnosna politika EU propisuje određena ograničenja. Ukoliko je vlasnik informacije čija se razmjena traži Vijeće EU, tada je Vijeće EU odgovorno za donošenje odluke o razmjeni informacija. Ukoliko je vlasnik informacija čija se razmjena traži treća strana, a Vijeće EU zahtjeva informaciju, u tom slučaju Vijeće EU mora tražiti odobrenje treće strane za razmjenu informacija. Ako je nemoguće ustanoviti vlasnika informacije, tada Vijeće EU donosi odluku o korištenju informacija.

Ukoliko Vijeće EU prima povjerljive podatke od treće strane, te informacije moraju biti tretirane sukladno razini klasifikacije koju je dodijelila treća strana. Ako postoji nesuglasnost oko klasifikacije informacija koje se razmjenjuju, Vijeće EU i treća strana mogu izvršavati ispravke klasifikacije informacija na temelju međusobnog dogovora.

Organi EU preuzimaju opću odgovornost za usklađivanje pravila i vođenje prilikom podizanja svijesti o sigurnosti kao i prilikom uspostavljanja koherentnog zakonskog okvira kroz postupak usvajanja direktiva i okvirnih odluka. Zemlje članice EU imaju obvezu prilagoditi svoje nacionalne propise direktivama EU. Njihova obveza je primjeniti operacijske i praktične okvire te osigurati njihovo provođenje i poštivanje.

Svaka zemlja članica imenovala je nacionalno tijelo čija je odgovornost sigurnost klasificiranih informacija. Zadaće takvog tijela jesu:

- održavanje sigurnosti povjerljivih informacija koje su u posjedu nacionalnih tijela,
- autorizacija uspostavljanja registra klase „strogo povjerljivo“,
- periodična inspekcija svih sigurnosnih postavki koje imaju za cilj zaštitu povjerljivih informacija,
- uspostavljanje postupka sigurnosne provjere osoblja bez obzira na nacionalnost unutar nacionalnih tijela ukoliko imaju pristup informacijama klasificiranim kao „strogo povjerljivo“, „tajno“ i „strogo povjerljivo“,
- osmišljavanje i provođenje sigurnosnih planova koji će sprečavati neovlašteni pristup klasificiranim informacijama.

[2] **Vijeće Europske unije** je tijelo u kojem se neposredno izražavaju interesi država članica Europske unije. To je mjesto gdje se najučinkovitije uspostavlja međusobna suradnja i dogovori između vlada država članica. Ono donosi zakonodavne odluke u EU i zaključuje ugovore s trećim državama. Od 1993. naziva se i Vijećem ministara. Ministarski sastav mijenja se ovisno o temi o kojoj se raspravlja. U pravilu u radu Vijeća sudjeluju ministri vanjskih poslova, međutim kada se raspravlja o poljoprivredi, sudjeluju ministri poljoprivrede, kada se radi o prometu, sudjeluju ministri zaduženi za transport i sl. Dužnost predsjedavajućeg Vijeća naizmjenično obnašaju države članice u trajanju od po šest mjeseci.

Po pitanju podizanja svijesti o mrežnoj i informacijskoj sigurnosti, zemlje članice trebaju uspostaviti edukacijski program kao i javnu informaciju i edukacijsku promociju putem masovnih medija. Potrebno je promovirati najbolju praksu iz područja mrežne i informacijske sigurnost te naglasiti važnost obrazovanja iz područja sigurnosti. Ova, pa i ostale specifične aktivnosti, koje zemlje članice trebaju poduzimati temeljem Odluke Vijeća EU o prihvaćanju sigurnosne politike, su temelj organizacije mrežne i informacijske sigurnosti u zemljama članicama.

4. Pregled propisa s područja informacijske sigurnosti

Vijeće EU usvojilo je konvencije, europske sporazume i pripadajuće protokole te preporuke kojima se nastoji regulirati pitanje mrežne i informacijske sigurnosti, ali i ostala pitanja koja se tiču informacijskog društva. Strategija EU prema sigurnosnoj problematici određena je upravo Odlukom Vijeća EU o prihvaćanju sigurnosne politike koja je donesena 19. ožujka 2001. godine, a stupila na snagu 1. prosinca 2001. godine te Odlukom Europske komisije o provođenju sigurnosne politike koja je donesena 6. lipnja 2001. godine. Ova odluka poznata je pod brojem 2001/264/EC i najbitnija je sastavnica sigurnosne politike na području Europe. U njoj su sadržani svi zahtjevi za sigurnost informacijskih i mrežnih sustava. Može se naći na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:101:0001:0001:EN:PDF

Drugi navedeni propisi su doneseni i usklađeni s njom kako bi osigurali provođenje uspješne strategije razvoja i sigurnosne politike. Najbitniji od njih su navedeni u sljedećim poglavljima.

4.1. Opći propisi

4.1.1. Uredba 1211/2009

Uredba Europskog parlamenta[3] i Europskog vijeća broj 1211/2009 donesena je 25. studenog 2009. godine. Ovim propisom zasnovano je Europsko regulatorno tijelo za električne komunikacije (eng. *Body of European Regulators for Electronic Communications, BEREC*) i njegov ured. Na slici 3 prikazan je logo BEREC-a.

Slika 3. Logo BEREC-a
Izvor: laquadrature.net

Ova regulativa definira propise osnivanja i rada Europskog regulatornog tijela za električne komunikacije. Glavni cilj ovog tijela je savjetovanje i pomaganje Europskoj komisiji u razvoju unutarnjeg tržišta i veza između nacionalnih regulatornih tijela (eng. *National Regulatory Authorities, NRA*) država članica i Komisije. Služi kao tijelo za razmatranje, raspravljanje i savjetovanje Europskog parlamenta, Vijeća i Komisije o pitanjima na području elektroničkih komunikacija. BEREC je u službi Europskog parlameta, Komisije i Vijeća te djeluje na njihovu molbu ili na vlastitu inicijativu.

[3] **Europski parlament** je tijelo Europske unije, čije članove izabiru izravno građani EU svakih pet godina, koliko traje mandat zastupnicima. Zajedno s Vijećem ministara čini zakonodavnu vlast Europske unije. Od 1. siječnja 2005. godine ukupno je 785 članova Parlamenta (zastupnika). Izbori se provode svake pete godine, na temelju općeg prava glasa. Ne postoji jedinstveni izborni sustav za izbor članova Europskog parlamenta, već je svaka država članica slobodna izabrati vlastiti sustav.

BEREC doprinosi funkcioniranju unutrašnjeg tržišta elektroničke komunikacije i usluge. Glavni ciljevi BEREC-a su:

- razvoj i širenje najboljih praksi na području elektroničkih komunikacija između nacionalnih regulatornih tijela kao što su pristup, metodologije i smjernice implemetacije regulatornog okvira EU,
- savjetovanje i pomoć nacionalnim regulatornim tijelima pri donošenju regulativa,
- donošenje zaključaka o nacrtima propisa, prijedloga i smjernica,
- objava izvještaja i donošenje savjeta na području elektroničkih komunikacija,
- pomoć Europskom parlamentu, Komisiji i Vijeću te nacionalnim regulatornim tijelima prilikom promicanja sigurnosne politike na području elektroničih komunikacija.

Cijeli tekst ove regulative može se pročitati na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R1211:EN:NOT

4.1.2. Direktiva 2002/21/EC

Direktiva 2002/21/EC Europskog parlamenta i Vijeća izadana je 7. ožujka 2002. godine. Ovom direktivom donesen je regulatorni okvir na području elektroničkih komunikacija, mreža i usluga.

Ova direktiva pruža zakonodavni okvir (eng. *Framework Directive*) i dio je paketa telekomunikacijskih propisa (eng. *Telecommunications Package*) donesenih za promjenu postojećih zakonodavnih okvira na području telekomunikacija. Svrha ovih propisa je povećanje konkurentnosti na području telekomunikacija.

Glavni cilj ove direktive je uspostava usklađenog zakonodavnog okvira na području elektroničkih komunikacija, mreža i usluga. Uključuje i propise o korisničkoj opremi koja služi za omogućavanje mrežnog pristupa. Sadrži odredbe o sljedećim mjerama:

- doseg općih odredaba s područja elektroničkih komunikacija,
- osnovne definicije,
- osnovne odredbe nacionalnih regulatornih tijela,
- novi koncept tržišne moći na području elektroničkih komunikacija,
- pravila za omogućavanje osnovnih resursa kao što su radiofrekvencije.

O ovoj direktivi može se više saznati na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:EN:NOT

4.1.3. Direktiva 2002/20/EC

Direktivu 2002/20/EC je Europski parlament i Vijeće izdali su 7. ožujka 2002. godine. Ovom direktivom donesen je regulatorni okvir na području autorizacije u elektroničkim komunikacijama, mrežama i uslugama.

Navedena direktiva dio je paketa telekomunikacijskih propisa te je poznata kao autorizacijska direktiva (eng. *Authorisation Directive*). Pruža zakonodavni okvir koji je donesen za promjenu postojećih nedovoljnih regulatornih propisa na području telekomunikacija.

Odredbe ove direktive pokrivaju mogućnosti autorizacije na području elektroničkih komunikacija, mreža i usluga, bilo da je komunikacija javna ili privatna. Ove odredbe se primjenjuju prilikom dodjeljivanja radiofrekvencija koje će se koristiti za elektroničku komunikaciju te uspostavu mreža i usluga.

Cilj ove odredbe je usklađivanje tržišta elektroničkih komunikacijskih mreža i usluga pomoću ograničavanja regulacije na najmanju razinu.

Zemlje potpisnice ove direktive moraju omogućiti:

- izbjegavanje ili smanjivanje destruktivne interferencije u radiokomunikacijama,
- osiguravanje kvalitete usluge,
- očuvanje učinkovitog korištenja radiofrekvencijskog sprekta,
- osiguravanje ispunjavanja ostalih intresnih ciljeva zemalja članica.

O ovoj direktivi može se više doznati na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:EN:NOT

4.1.4. Direktiva 2002/22/EC

Europski parlament i Vijeće 7. ožujka 2002. godine izdali su direktivu 2002/22/EC. Direktiva se odnosi na područje usluga i korisničkih prava vezanih uz elektroničke komunikacijske mreže i usluge. Ova direktiva dio je paketa telekomunikacijskih propisa te je poznata kao direktiva o univerzalnim uslugama (eng. *Universal Service Directive*).

Direktiva definira univerzalnu uslugu kao minimalni skup usluga određene kvalitete kojem svi krajnji korisnici moraju imati pristup po povoljnoj cijeni prema određenim nacionalnim standardima bez onemogućavanja konkurencije.

Ova direktiva pokriva područja:

- dostupnost univerzalne usluge,
- odredbe o pristupu mrežnoj i telefonskoj infrastrukturi na određenom području,
- javne telefonske govornice i ostale javne pristupne točke,
- posebne mjere za invalide,
- pritupačnost tarifa,
- kvalitetu usluga.

Cijelokupan tekst ove direktive može se naći na:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0022:EN:NOT

4.1.5. Direktiva 2002/19/EC

Direktivu 2002/19/EC izdali su Europski palament i Vijeće 7. ožujka 2002. godine, a odnosi se na pristup i povezivanje elektroničkih komunikacijskih mreža i pripadajućih objekata. Dio je paketa telekomunikacijskih odredbi i poznata je kao Direktiva o pristupu (eng. *Access Directive*).

Ova direktiva utvrđuje prava i obveze za operatore i poduzeća koja nude povezivanje i/ili pristup svojim mrežama. Omogućuje pravilima tržišnog natjecanja da djeluju kao sredstvo za regulaciju tržišta. Međutim, ukoliko ne postoji učinkovito tržišno natjecanje, nacionalna regulatorna tijela moraju djelovati, između ostalog, nametanjem obveza operaterima koji imaju značajnu tržišnu snagu.

Cilj je uspostaviti okvire koji će potaknuti konkurenciju i razvoj komunikacijskih usluga i mreža te osigurati da sva uska grla na tržištu ne ograničavaju nastanak inovativnih usluga koje bi mogle biti od koristi krajnjim korisnicima. Ovaj pristup je tehnološki neutralan, tj. direktiva ne namjerava uvesti pravila koja bi mogla ugroziti tehnološki napredak, već joj je umjesto toga namjera uspostaviti principe rješavanja problema na tržištu.

Direktiva se primjenjuje na sve oblike komunikacijskih mreža koji nude javno dostupne komunikacijske usluge. To uključuje fiksne i mobilne telekomunikacijske mreže, mreže za zemaljsko emitiranje, kabelske TV mreže, satelitske mreže i Internet koji se koristi za prijenos govora, slika, podataka i ostalo.

O ovoj direktivi je moguće više saznati na sljedećoj adresi:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:NOT

4.1.6. Direktiva 2002/58/EZ

Direktiva 2002/58/EZ Europskog parlamenta i Vijeća izadana je 12. srpnja 2002. godine i u vezi je s obradom osobnih podataka i zaštitom privatnosti na području elektroničkih komunikacija.

Ova direktiva čini dio paketa obredaba o telekomunikacijama i poznata je kao Direktiva o privatnosti i elektroničkim komunikacijama (eng. *Directive on privacy and electronic communications*). Prvenstveno se odnosi na obradu osobnih podataka prilikom isporuke komunikacijske usluge.

Davatelji usluga elektroničke komunikacijske usluge moraju štititi sigurnost svojih usluga sljedećim mjerama:

- osiguravanjem osobnih podataka, a pristup tim podacima dozvoliti samo ovlaštenim osobama,
- zaštitom osobnih podataka kako se ne bi uništili, izgubili ili bili promijenjeni,
- osiguravanjem provedbe sigurnosne politike na području obrade osobnih podataka.

U slučaju povrede sigurnosti osobnih podataka, davatelj usluga mora obavijestiti zainteresirane osobe, kao i nadležno regulatorno tijelo.

U direktivi je navedeno da države članice moraju, kao i prema svojim nacionalnim zakonima, osigurati tajnost komunikacije koja se odvija preko javne elektroničke komunikacijske mreže. Slušanje, snimanje i skladištenje komunikacijskih podataka mora biti izričito zabranjeno osobama koje nisu korisnici bez pristanka navedenih korisnika.

Direktiva određuje da se podaci o prometu i lokacijski podaci moraju brisati ili učiniti anonimnima kada više nisu potrebni za održavanje komunikacije ili za obračun, osim ako je pretplatnik dao svoj pristanak za drugu uporabu.

Također je navedeno kako korisnici moraju dati svoju suglasnost ukoliko žele primati neželjenu komercijalnu elektroničku poštu (eng. *spam*). Takav pristup se naziva *opt-in*, tj. opcionalan je.

Direktiva kaže da korisnici moraju dati svoj pristanak za informacije koje se mogu spremiti na njihovu informacijsku opremu i da se mora omogućiti pristup takvim informacijama. Kako bi bili u mogućnosti to učiniti, korisnicima moraju biti dostupne jasne i sveobuhvatne informacije o namjeni skladištenja tih informacija. Namjena ovih odredaba je zaštitita informacijskog sustava korisnika od zlonamjernih programa, poput virusa, ali primjenjuju se i na kolačiće (eng. *cookies*).

Također je navedeno kako europski građani moraju dati prethodnu suglasnost za javno objavljivanje telefonskih brojeva (fiksnih ili mobilnih), adresa elektroničke pošte i poštanskih adresa.

Cjelokupan sadržaj ove direktive može se pronaći na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

4.2. Propisi s područja zaštite podataka, autorskih i srodnih prava

4.2.1. Direktiva 95/46/EZ

Europski parlament i Vijeće donijeli su 24. listopada 1995. godine direktivu 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i o slobodnom kretanju takvih podataka. Ova direktiva poznata je kao Direktiva o zaštiti osobnih podataka.

Primjenjuje se na podatke obrađene automatiziranim sredstvima (npr. računalna baza podataka kupaca) i podatke koji su sadržani ili namjeravaju biti sadržani u neautomatiziranom sustavu pohrane podataka (tradicionalni papirnati dokumenti).

Direktiva je usmjerena na zaštitu prava i sloboda osoba na području obrađivanja osobnih podataka kada je obrada podataka dopuštena.

Smjernice se odnose na:

- kvalitetu podataka: osobni podaci moraju biti obrađeni na pravičan i zakonit način, a prikupljeni za određene, izričite i zakonite svrhe. Oni također moraju biti točni i, prema potrebi, ažurirani,
- legitimnost obrade podataka: osobni podaci mogu se obrađivati samo ako je nositelj podataka nedvojbeno dao svoj pristanak ili ako je to nužno:
    - za izvršenje ugovora u kojem je nositelj podataka ugovorna stranka,
    - za usklađivanje sa zakonskom obvezom,
    - u cilju zaštite vitalnih interesa nositelja podataka,
    - za obavljanje zadataka koji su javni interes,
    - radi zakonitih interesa koje ostvaruje nadzorno tijelo,
- posebne kategorije za obradu: zabranjeno je obrađivati osobne podatke koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, sindikalno članstvo te obradu podataka vezanih za zdravlje ili spolni život. Ova odredba dolazi s određenim odstupanjima, npr. slučajevi u kojima je to nužno radi zaštite vitalnih interesa nositelja podataka ili za potrebe preventivne medicine i medicinske dijagnoze,
- informacije koje moraju biti pristupačne ispitaniku: nadzorno tijelo mora osigurati ispitaniku o kojem se prikupljaju određene informacije podatke koji se odnose na njega samog (npr. identitet nadzornika, svrha prikupljanja podataka, primatelji podataka i sl.),
- nositelja podataka koji ima pravo pristupa podacima: svaki ispitanik treba imati pravo dobiti podatke od nadzornika:
    - podatke o načinu obrade podataka koji se odnose na njega i obavijest je li obrada podataka u tijeku,
    - ispravak, brisanje ili blokiranje podataka ukoliko obrada nije u skladu s odredbama ove direktive, bilo zbog nepotpunosti ili netočnosti podataka, te obavijest o promjenama trećim osobama kojima se podaci moraju dostaviti,
- izuzeća i ograničenja: opseg zahtjeva koji se odnose na kvalitetu podataka, informacije koje se daju nositelju podataka, pravo pristupa i publicističku obradu može se ograničiti u cilju očuvanja nacionalne sigurnosti, obrane, javne sigurnosti, kaznenog progona zbog kaznenih djela, važnoga gospodarskog ili financijskog interesa države članice Europske unije, ili zaštite nositelja podataka,
- pravo prigovora na obradu podataka: nositelj podataka bi trebao imati pravo prigovora temeljem pravne osnove na obradu podataka koji se odnose na njega. On bi također trebao imati pravo prigovora na zahtjev i bez naknade, na obradu osobnih podataka koji su predviđeni za korištenje u svrhu izravnog marketinga. Trebao bi biti informiran prije nego se osobni podaci daju trećim stranama u svrhu izravnog marketinga te bi trebao imati pravo prigovora na takva objavljivanja,

- povjerljivost i sigurnost obrade: bilo koja osoba koja djeluje pod nadležnosti nadzornika ili korisnika podataka koja ima pristup osobnim podacima ne smije ih obrađivati, osim uz dozvolu nadzornog tijela. Osim toga, nadzorno tijelo mora provesti odgovarajuće mjere zaštite osobnih podataka protiv slučajnog ili nezakonitog uništenja, slučajnog gubitka, izmjene, neovlaštenog odavanja ili pristupa podacima,
- obavijest o obradi podataka koja se daje nadzornom tijelu: nadzornik obrade mora obavijestiti državno nadzorno tijelo prije obavljanja bilo kakve radnje obrade. Potrebno je provesti provjeru kako bi se utvrdili specifični rizici za prava i slobode nositelja podataka koje provodi nadzorno tijelo nakon primitka obavijesti. Mjere koje treba poduzeti kako bi se osiguralo da su načini obrade podataka objavljeni i javni te nadzorna tijela moraju voditi zapisnik o poslovanju prijavljenih organizacija koja obavljaju obradu.

Važno je napomenuti kako nadzornik ili nadzorno tijelo u ovoj direktivi opisujeu fizičku ili pravnu osobu, javnu vlast, agenciju ili drugi organ koji samostalno ili zajedno s drugima utvrđuje svrhu i način obrade osobnih podataka, gdje se cilj i način obrade utvrđuju zakonima ili propisima europskih država ili Europske unije. Posebni kriteriji za njegovo imenovanje mogu se utvrditi nacionalnim zakonima ili zakonima Europske unije.

Tekst ove direktive može se pronaći na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

4.2.2. Uredba 45/2001

Uredba 45/2001 Europskog parlamenta i Vijeća izdana je 18. prosinca 2000. godine i odnosi se na područje zaštite pojedinaca u pogledu obrade osobnih podataka u ustanovama i tijelima Europske unije te o slobodnome protoku takvih podataka.

Ova uredba sadrži odredbe kojima je cilj zaštita osobnih podataka koje obrađuju institucije i tijela Europske unije. Njihov je cilj osigurati visoku razinu zaštite osobnih podataka kojima upravljaju u ustanovama i tijelima Unije. Konkretno, ti podaci moraju biti:

- obrađeni pravilno i zakonito,
- prikupljani za određene, izričite i zakonite svrhe te se ne smiju obrađivati na način nespojiv s tim svrhama,
- odgovarajući, mjerodavni i ne suvišni u odnosu na svrhu za koju su prikupljeni i obrađeni,
- točni i prema potrebi ažurirani (potrebno je poduzeti određene korake kako bi se osiguralo da su podaci koji su netočni ili nepotpuni za svrhu zbog koje su prikupljeni, odnosno za koje se dalje obrađuju, obrisani ili uklonjeni),
- čuvani u obliku koji dopušta identifikaciju ispitanika ne duže nego što je potrebno za svrhe za koje su podaci prikupljeni, odnosno za koje se dalje obrađuju.

Ova uredba povezana je s direktivom 95/46/EZ i zajedno omogućuju zaštitu osobnih podataka i zakonski okvir za protok tih podataka.

Također predviđa osnivanje Europskog nadzornog tijela za zaštitu podataka (eng. *European Data Protection Authority*), nezavisnog tijela Unije koje je odgovorno za nadzor pravilne primjene propisa o zaštiti podataka koju moraju provesti institucije i tijela EU.

Više o ovoj uredbi može se saznati na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:NOT

4.2.3. Direktiva 2001/29/EC

Direktiva 2001/29/EC Europskog parlamenta i Vijeća od 22. svibnja 2001. godine odnosi se na usklađivanje određenih aspekata zaštite autorskog prava i srodnih prava u informacijskom društvu.

Osim ako nije drugačije određeno, direktiva se primjenjuje u slučaju:

- pravne zaštite računalnih programa,
- prava u vezi iznajmljivanja i posudbe te prava u vezi s autorskim pravima na području intelektualnog vlasništva,
- autorskih i srodnih prava koja se primjenjuju na emitiranje programa putem satelita i prijenos putem kabela,
- pojašnjavanja i korištenja pojma zaštite autorskog i srodnih prava,
- pravne zaštite baza podataka.

Direktiva se bavi trima glavnim područjima:

- reprodukcijskim pravima,
- pravima koja se odnose na komunikaciju,
- pravima koja se odnose na distribuciju.

Države članice moraju osigurati isključivo pravo na dozvolu ili zabranu, izravno ili neizravno, privremeno ili trajno, reprodukciju bilo kojim sredstvima i u bilo kojem obliku, u cijelosti ili djelomično:

- autorima za izvornike i kopije svojih djela,
- izvođačima za snimke njihovih izvedbi,
- proizvođačima fonograma za njihove fonograme,
- producentima filmova za izvornik i kopije svojih filmova,
- organizacijama za radiodifuziju za snimke svojih emisija bez obzira na metodu prijenosa.

Države članice moraju osigurati autorima isključivo pravo na odobravanje ili zabranu korištenja primjeraka svojih djela u javnosti, uključujući stavljanje na raspolaganje javnosti njihovih djela na način da im se može pristupiti s mjesta i u vrijeme koje odgovara pojednicima. Isto vrijedi i za stavljanja na raspolaganje javnosti zaštićenih djela na način da im pojednici mogu pristupiti s mjesta i u vrijeme koje im odgovara.

Direktiva usklađuje autorska prava i prava distribucije u javnosti orginalnih radova ili umnoženih primjeraka. Ovo pravo prestaje biti važeće prilikom prve prodaje ili drugim prijenosom vlasništva gdje je prijenos vlasništva obavio nositelj prava ili je to omogućeno uz njegov pristanak.

Više o ovim pravima može se saznati na sljedećoj adresi:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML

4.3. Propisi na području Interneta, mrežnih aktivnosti te informacijskih i komunikacijskih standarda

4.3.1. Uredba 733/2002

Europski parlament i Vijeće 22. travnja 2002. godine izdali su uredbu 733/2002 o osnivanju i uvođenju .eu domene koja je najveće razine (eng. *Top-level Domain, TLD*) na području Europske unije.

Ova uredba ima za cilj utvrditi uvjete osnivanja i korištenja domene .eu, a posebno osigurati uspostavu registra mrežnih stranica (eng. *Registry*) i općenitog političkog okvira unutar kojeg će Registar djelovati.

Stvaranje ove domene jedan je od ciljeva navedenih u akcijskom planu eEurope 2002 kako bi se ubrzao razvoj elektroničke trgovine i promicala upotreba Interneta. Ova domena će biti dodatak te neće zamijeniti one koje već postoje unutar EU čime će se korisnicima pružiti mogućnost stvaranja pan-europskog Internet identiteta (npr. mrežne stranice ili adrese e-pošte).

Provedba uredbe 733/2002 ispunjava sljedeće ciljeve:

- promicanje korištenja Interneta i povećanje izbora prilikom registracije domene, pružajući dopunsku registraciju domene na domenu više razine ili globalnu registraciju na generičke domene najveće razine,
- poboljšanje interoperabilnosti europskih poslužitelja osiguravanjem dostupnosti domene .eu svim poslužiteljima,
- povećanje vidljivosti europskog unutarnjeg tržišta na svjetskoj Internetskoj mreži i promicanje pozitivne slike o Europskoj uniji na globalnim informacijskim mrežama.

Europska komisija je odgovorna za donošenje javne politike i pravila koja se odnose na provedbu i funkcije domene .eu te pravila o registraciji. Ta pravila obuhvaćaju osobito:

- način rješavanja sukoba,
- javne politike o nepravilnoj i neovlaštenoj registraciji imena domena,
- pravila o mogućem ukidanju ili mijenjanju imena domena,
- pitanja jezika i geografskih pojmova,
- zaštitu intelektualnog vlasništva i drugih srodnih prava.

Tekst uredbe može se pronaći na sljedećoj adresi:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R0733:EN:NOT

4.3.2. Odluka Vijeća 87/95/EEC

Odluka Vijeća 87/95/EEC od 22. prosinca 1986. godine odnosi se na provođenje normizacije na području informacijske i komunikacijske tehnologije i telekomunikacija.

Ova odluka ima za cilj uvođenje i primjenu politike EU o normizaciji na području informacijske i komunikacijske tehnologije i telekomunikacija.

Cilj normizacija je olakšavanje razmjene informacija u cijeloj Europskoj uniji. Normizacija smanjuje prepreke stvorene nekompatibilnošću informacijskih sredstava i oblika informacija. Konkretne mjere su predložene za:

- promicanje normizacije u Europi,
- izrađivanje i primijenu standarda iz područja informacijske i komunikacijske tehnologije,
- izrađivanje i primijenu funkcionalne specifikacije u području telekomunikacija.

Ovom odredbom cilj je izraditi i uspostaviti europske standarde i funkcionalne specifikacije te europska normizacijska i tehnička tijela koja će se baviti informacijskim tehnologijama i telekomunikacijskim sektorom te će svoj rad temeljiti na međunarodnim standardima. Ova tijela također pripremaju tehničke specifikacije koje će formirati osnovu europskih standarda.

4.3.3. Uredba 460/2004

Uredbom 460/2004 Europskog parlamenta i Vijeća donesenom 10. ožujka 2004. godine osnovana je Europska agencija za informacijsku i mrežnu sigurnost (eng. *European Network and Information Security Agency, ENISA*).

Kako su informacijski sustavi i mreže postali sastavni dio svakodnevnog života europskih građana, neizbježno se postavlja pitanje njihove sigurnosti koja je postala predmet rastućeg interesa za društvo. Na slici 4 može se vidjeti logo agencije ENISA-e.

Slika 4. Logo ENISA-e
Izvor: iwar.org.uk

Zbog sve većeg broja prijetnji informacijskoj i mrežnoj sigurnosti, osnovana je Europska agencija za informacijsku i mrežnu sigurnost. Cilj agencije je povećati sposobnost Europske unije, zemalja članica i poslovne zajednice kako bi se identificiralo, spriječilo i odgovorilo na izazove koji se pojavljuju na području sigurnosti mreža i informacija.

Osim toga, ENISA pruža pomoć i daje savjete Europskoj komisiji i zemljama članicama. Također može biti pozvana kao pomoć Komisiji u pripremanju tehničkih projekata za osuvremenjivanje, modernizaciju i razvoj Europske unije. Nadalje, ENISA olakšava i unapređuje suradnju između različitih sudionika koji djeluju u javnom i privatnom sektoru kako bi se postigla dovoljno visoka razina sigurnosti u zemljama EU.

Uloga ENISA-e među ostalima je:

- prikupljanje odgovarajućih podataka za analizu tekućih i novih rizika, a rezultate svojih istraživanja mora dati na uvid zemljama EU i Komisiji,
- davanje savjeta i, po potrebi, pomoći Europskom parlamentu, Europskoj komisiji i nadležnim europskim i nacionalnim tijelima u pitanjima informacijske i mrežne sigurnosti,
- poboljšavanje suradnje između različitih sudionika u tom području (npr. putem konzultacija i umrežavanja),
- olakšavanje suradnje između Europske komisije i zemalja Europske unije u razvoju zajedničkih metodologija za sprečavanje sigurnosnih problema,
- doprinos podizanju svijesti i dostupnost brzih, objektivnih i sveobuhvatnih informacija o mrežnim sigurnosnim pitanjima i informacijama za sve korisnike (npr. promicanje razmjene najboljih načela i praksi, uključujući metode uzbunjivanja korisnika te traženje sinergije između javnog i privatnog sektora),
- pomaganje Komisiji i zemljama članicama u dijalogu s industrijom pri riješavanju problema vezanih uz sigurnost sklopovskih i programskih proizvoda,
- praćenje razvoja standarda za sigurnost proizvoda i usluga te promicanje procjene i upravljanja sigurnosnim rizicima i aktivnostima,
- doprinos nastojanjima članica EU prilikom suradnje s ne-EU zemaljama i međunarodnim organizacijama za promicanje globalnog pristupa sigurnosnim pitanjima,
- davanje svojih zaključaka, smjernica i savjeta.

ENISA obuhvaća:

- upravni odbor sastavljen od predstavnika zemalja članica Europske unije i predstavnika Komisije, kao i predstavnika gospodarstva, akademika i korisnika bez prava glasa,
- izvršnog direktora koji imenuje upravu na temelju popisa predloženih kandidata koju predlaže Europska komisija,

- stalnu skupinu sudionika koju osniva izvršni direktor. Skupina je sastavljena od predstavnika stručnjaka s područja informacijskih i komunikacijskih tehnologija, tvrtki, potrošača i akademskih stručnjaka. Na taj način ENISA ima pristup najnovijim informacijama koje su dostupne te može odgovoriti na sve informacijske i mrežne sigurnosne izazove.

Više o ovoj uredbi može se pročitati na sljedećoj adresi:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:NOT

4.3.4. Odluka 92/242/EEC

Odluku 92/242/EEC je 31. ožujka 1992. godine donijelo Europsko vijeće na području informacijske sigurnosti.

Ovom odlukom odobrava se i potiče djelovanje na području sigurnosti informacijskih sustava, a uključuje dvije komponente:

- postavljanje akcijskog plana za početno 24-mjesečno razdoblje. Iznos od 12 milijuna eura smatra se nužnim za provedbu akcije za ovo početno razdoblje,
- postavljanje Odbora s dugoročnim mandatom koji će pomagati Komisiji u akcijama koje treba poduzeti na području sigurnosti informacijskih i mrežnih sustava.

Akcijski plan kao svoj cilj mora imati razvoj ukupne strategije čiji je cilj osigurati korisnicima i vlasnicima informacija koje su elektronički pohranjene, obrađene ili prenošene da budu na odgovarajući način zaštićene od slučajnih ili namjernih prijetnji. Akcijski plan će se provoditi u uskoj suradnji sa svim sudionicima na tom području. U obzir će se uzeti i nadopuniti normizacijske aktivnosti u tijeku na ovom području koje se odvijaju širom svijeta. To će uključivati sljedeće linije djelovanja:

- razvoj strategije informacijske sigurnosti,
- utvrđivanje zahtjeva korisnika i davatelja usluga koje su potrebne za sigurnost informacijskih sustava,
- rješenja za neposredne i privremene potrebe korisnika, dobavljača i davatelja usluga,
- specifikacija, standardizacija i certifikacija informacijske sigurnosti,
- tehnološki i operacijski razvoj informacijske sigurnosti unutar opće strategije,
- pružanje sigurnosti informacijskih sustava.

Cjelokupan tekst odluke nalazi se na sljedećoj poveznici:

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Decision&an_doc=1992&nu_doc=242

4.3.5. Odluka 2005/222/JHA

Okvirna odluka Europskog vijeća 2005/222/JHA donesena je 24. veljače 2005. godine te se odnosi na napade na informacijske sustave. Cilj ove odluke je borba protiv računalnog kriminala i promicanje informacijske sigurnosti te poboljšavanje suradnje između pravosudnih i drugih nadležnih tijela kroz približavanje pravila o kaznenom pravu u području napada na informacijske sustave.

Glavne vrste kaznenih djela obuhvaćenih ovom odlukom su napadi na informacijske sustave kao što su piratstvo, virusi i drugi zlćudni programi te napadi uskraćivanja usluga (eng. *Denial of Service, DoS*).

Ovo novo kazneno djelo, koje ne poznaje granice, može biti spriječeno na način da se:

- poveća sigurnost informacijskih infrastruktura,
- omogući tijelima pravosudne vlasti sredstva za djelovanje.

U tom smislu, ovom okvirnom odlukom predlaže se usklađivanje kaznenopravnih sustava i poboljšanje suradnje između pravosudnih tijela prilikom djela koja se tiču:

- protuzakonitog pristupa informacijskim sustavima,
- protuzakonitog ometanja rada sustava,
- protuzakonitog ometanja protoka podataka.

U svim slučajevima kazneno djelo mora biti namjerno. Poticanje, pomaganje i pokušaj bilo kojeg od navedenih djela također će biti procesuirano.

Na sljedećoj poveznici može se saznati više o ovoj odluci:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT

4.3.6. Odluka 1351/2008/EC

Odluka 1351/2008/EC Europskog parlamenta i Vijeća o uspostavi višegodišnjeg programa EU za zaštitu djece putem Interneta i drugih komunikacijskih tehnologija donesena je 16. prosinca 2008. godine.

Program "Sigurniji Internet" ima za cilj poboljšanje sigurnosti djece u mrežnom okruženju i usredotočuje se na dva cilja:

- povećati znanje o uporabi novih tehnologija u djece i mladih,
- identificirati rizike kojima su izloženi i osigurati načine suočavanja s njima.

Program je namijenjen ne samo za ilegalne i štetne sadržaje, već i za štetno ponašanje, a provodi se kroz sljedeća četiri načina djelovanja:

- podizanje razine javne svijesti. Ovakve akcije posebno su usmjerene prema djeci, njihovim roditeljima i nastavnicima. Omogućuju širenje informacija među velikim brojem korisnika i informiraju ih o rizicima i načinima kako ih spriječiti. Ove radnje obuhvaćaju razvoj i širenje alata namjenjenih podizanju svijesti i omogućuju ljudima dobivanje savjeta o tim pitanjima,
- borba protiv ilegalnih sadržaja i štetnog ponašanja. Ove aktivnosti imaju za cilj smanjiti količinu ilegalnog sadržaja i riješiti problem mrežnog seksualnog zlostavljanja i maltretiranja djece. Program pruža smjernice za osnivanje javno dostupnih organizacija na europskoj razini koje bi se učinkovito bavile ovom vrstom zlostavljanja. Također imaju za cilj istraživanje štetnog ponašanja i psiholoških i sociološkiх aspekta takvog ponašanja. Nadalje, program promiče suradnju na nacionalnoj, europskoj i međunarodnoj razini te potiče relevantne sudionike na razmjenu informacija i međusobnih iskustava,
- promicanje sigurnijeg mrežnog okruženja. Glavni ciljevi su osmišljeni kako bi potakli sudjelovanje djece u oblikovanju sigurnijeg mrežnog okruženja,
- uspostava baze znanja. Ova baza znanja će biti sastavljena od poznatih i novih načina korištenja mreže kod djece te o rizicima i posljedicama svojstvenim uporabi Interneta. Ova baza znanja će se sastaviti u suradnji sa stručnjacima iz područja mrežne sigurnosti djece na europskoj razini.

Više o ovoj odluci može se saznati na sljedećoj poveznici:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D1351:EN:NOT

4.4. Konvencija o računalnom kriminalu

Konvencija je prvi međunarodni ugovor o zločinima počinjenima putem interneta i drugih računalnih mreža. Posebno se bavi kršenjem autorskih prava, računalnim prijevarama, dječjom pornografijom i povredama sigurnosti mreže. Ona također sadrži niz ovlasti i postupaka za povećanje razine informacijske i mrežne sigurnosti. Izdana je 23. studenog 2001. Godine u Budimpešti, a stupila na snagu 1. srpnja 2004. godine.

Glavni cilj konvencije je nastavak zajedničke kaznene politike usmjerene na zaštitu društva od kibernetičkog (eng. *cyber crime*) kriminala, posebno usvajanje odgovarajućeg zakonodavstva i jačanje međunarodne suradnje. Konvencija je proizvod četiriju godina rada stručnjaka Vijeća Europe, ali i stručnjaka Sjedinjenih Američkih Država, Kanade, Japana i drugih zemalja koje nisu članice Organizacije. Nadopunjena je dodatnim protokolom koji svako objavljivanje i promidžbu rasizma i ksenofobije putem računalnih mreža označava kao kazneno djelo.

Deset godina nakon njezinog usvajanja, Budimpeštanska konvencija još uvijek predstavlja jedini prihvaćeni međunarodnih ugovor za zaštitu sloboda, sigurnosti i ljudskih prava na Internetu. Postalo je jasno da je uspostava učinkovitih pravila potrebna kako bi se povećala sloboda i smanjio rizik prilikom korištenja Interneta.

Do danas, 55 zemalja je potpisalo, ratificiralo ili je pozvano da pristupi Konvenciji. Više od 120 zemalja surađuje s Vijećem Europe kako bi ojačale svoje zakonodavstvo i kapacitet za rješavanje kibernetičkog kriminala. Konvencija je imala globalni utjecaj, a rezultirala je strožim i prihvaćenim pravilima o računalnom kriminalu u zakonodavstvima širom svijeta te učinkovitijoj međunarodnoj suradnji u istrazi i procesuiranju kaznenih djela počinjenih na Internetu.

Ciljevi Konvencije su:

- usklađivanje nacionalnih kaznenih zakona, elementa kaznenih djela i povezanih odredbi u području računalnog kriminala,
- omogućavanje nacionalnoj sudskoj vlasti ovlasti potrebnih za istrage i kazneni progon tih djela, kao i drugih kaznenih djela počinjenih pomoću računalnog sustava ili koja su u svezi s dokazima u elektroničkom obliku,
- postavljanje brzog i djelotvornog načina međunarodne suradnje.

Sljedeća kaznena djela definirana su u Konvenciji:

- ilegalni pristup informacijskim i mrežnim resursima,
- nezakonito presretanje i ometanje prijenosa informacija,
- narušavanje integriteta podataka,
- ometanje informacijskog i mrežnog sustava,
- zloupotreba uređaja,
- korištenje računala za potrebe krivotvorenja,
- računalna prijevara,
- kaznena djela u svezi s dječjom pornografijom,
- kaznena djela koja se odnose na autorska i srodna prava.

Konvencija također određuje načine postupanja u slučaju povreda čuvanih i pohranjenih podataka, spremanja i otkrivanja mrežnih podataka, pretrage i privremenog oduzimanja računalnih podataka, prikupljanja mrežnog prometa u stvarnom vremenu i presretanja sadržaja podataka.

Tekst Konvencije može se naći na sljedećoj poveznici:

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

5. Zaključak

Informacijska i mrežna sigurnost je postala predmet rastućeg interesa za društvo. Sve veći broj slučajeva narušavanja informacijske i računalne sigurnosti već je ostvario znatnu financijsku štetu, potkopao povjerenje korisnika te nanio štetu razvoju e-trgovine. Napadi na ključne informacijske sustave mogu imati velike posljedice za pružanje usluga bitnih za dobrobit europskih građana. Omogućivanje brze internetske veze i povećanje umreženosti čine sve veće zahtjeve na sigurnosne uvjete. Zbog toga je donesen velik broj međunarodnih akata i odluka unutar Europske unije.

Modeliranje sigurnosnog okruženja i donošenje zakonodavnog okvira kako bi se to okruženje ostvarilo predstavlja jedan od vodećih problema kojima se bavi sigurnosna politika Europske unije u području informacijske sigurnosti. Ovdje se misli na modeliranje prijetnji, ranjivosti i općenito sigurnosnog okruženja (organizacijska obilježja, osoblje i sl.). Kombiniranje usklađenih sigurnosnih kriterija kao i modeliranje sigurnosnog okruženja, ukazuju na namjeru politike EU koja sve više pažnje priklanja rastućem računalnom kriminalu. Pojedinci, javne uprave i poduzeća su reagirali na povećanje sigurnosnih prijetnji te uveli i počeli primjenjivati sigurnosne tehnologije i procedure osiguravanja koje će doprinijeti visokoj razini računalne sigurnosti. Sve više se razvija i sustavna prekogranična suradnja među zemljama Europske unije kako bi se zajedničim snagama mogle oduprijeti novim izazovima na području informacijske i mrežne sigurnosti.

Europska unija posljednjih godina sve više pažnje daje razvijanju sigurnog okruženja i sigurnosti informacija. Zbog toga je stvoren zakonodavni okvir EU koji se odnosi na identifikaciju i klasifikaciju informacija i primjenu odgovarajućih sigurnosnih mjera s ciljem zaštite tajnosti, integriteta i dostupnosti informacija koje se obrađuju, spremaju ili prenose. Razvoj područja upravljanja informacijskom sigurnošću danas je uglavnom usmjeren prema višedimenzijonalnom shvaćanju politike informacijske sigurnosti. Takav pristup podrazumijeva međupovezanost različitih područja politike informacijske sigurnosti, ali i povezanost s korporativnom razinom poslovnog upravljanja te s tijelima javne vlasti.

.

6. Leksikon pojmova

Napad uskraćivanjem usluga (eng. Denial of Service)

Vrsta napada u kojem se obično namjernim generiranjem velike količine mrežnog prometa nastoji zagušiti mrežna oprema i poslužitelji. Isti postaju toliko opterećeni da više nisu u stanju obrađivati promet što na kraju dovodi do onemogućavanja mrežnih usluga.

en.wikipedia.org/wiki/Denial-of-service_attack

Direktiva (eng. Directive)

Direktiva je, uz uredbu, najvažniji pravni akt Europske unije. Direktiva obvezuje u pogledu rezultata koji se njome ostvaruje, ali nacionalnim vlastima prepušta izbor forme i metode provedbe. Za razliku od uredbe, direktiva služi približavanju, a ne potpunomu ujednačivanju prava država članica Unije. Zato se direktivom zadaje cilj koji se mora postići, dok su države članice obvezne prenijeti direktivu u svoj nacionalni sustav, birajući pritom formu (zakon, podzakonski akt i sl.)

http://en.wikipedia.org/wiki/Directive_%28European_Union%29

Uredba (eng. Regulation)

Uredbe u pravu Europske unije imaju opću primjenu, u potpunosti su obvezujuće i izravno primjenjive u svim državama članicama Europske unije. Zajedno s direktivama, uredbe su najčešći i najbitniji tipovi akata kojima se usklađuju nacionalna prava država članica EU. Dok uredbe u potpunosti unificiraju pravo, tj. zamijenjuju do tada postojeće interne norme jednom, potpuno istovjetnom europskom normom, direktive ostavljaju prostora za donekle različita rješenja u različitim državama članicama.

http://en.wikipedia.org/wiki/Regulation_%28European_Union%29

7. Reference

[1] General legislative framework: http://europa.eu/legislation_summaries/information_society/legislative_framework/index_en.htm, pristupljeno u travnju 2012.

[2] Središnji državni ured za e-Hrvatsku, Stručna skupina za informacijsku sigurnost: Nacionalni program informacijske sigurnosti Republike Hrvatske: http://www.ehrvatska.hr/ehrvatska/modules/Downloads/upload/Nacionalni%20program%20informacijske%20sigurnosti%20u%20RH.pdf, pristupljeno u travnju 2012.

[3] Council decidion of 19 March 2001 adopting the Council's security regulations (2001/264/EC): http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_101/l_10120010411en00010066.pdf, pristupljeno u travnju 2012.

[4] Klaić A.: Minimalni sigurnosni kriteriji i upravljanje rizikom informacijske sigurnosti, seminarski rad, travanj 2010, http://os2.zemris.fer.hr/ISMS/rizik/2010_klajic/SeminarskiRad_SRS_042010_AK.pdf, pristupljeno u travnju 2012.

[5] Convention on Cybercrime:http://en.wikipedia.org/wiki/Convention_on_Cybercrime, pristupljeno u travnju 2012.

[6] The Body of European Regulators for Electronic Communications: http://europa.eu/legislation_summaries/information_society/legislative_framework/si0015_en.htm, pristupljeno u travnju 2012.

[7] Regulatory framework for electronic communications: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm, pristupljeno u travnju 2012.

[8] Authorisation of electronic communications networks and services: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24164_en.htm, pristupljeno u travnju 2012.

[9] Universal service and users' rights: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24108h_en.htm, pristupljeno u travnju 2012.

[10] Access to electronic communications networks: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24108i_en.htm, pristupljeno u travnju 2012.

[11] Data protection in the electronic communications sector: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm, pristupljeno u travnju 2012.

[12] Protection of personal data: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm, pristupljeno u travnju 2012..

[13] Data protection by Community institutions and bodies: http://europa.eu/legislation_summaries/information_society/data_protection/l24222_en.htm, pristupljeno u travnju 2012..

[14] Copyright and related rights in the information society: harmonisation of certain aspects: http://europa.eu/legislation_summaries/information_society/data_protection/l26053_en.htm, pristupljeno u travnju 2012.

[15] The ".eu" top-level domain: http://europa.eu/legislation_summaries/information_society/internet/l24228_en.htm, pristupljeno u travnju 2012.

[16] Information security: http://europa.eu/legislation_summaries/information_society/internet/l24121_en.htm, pristupljeno u travnju 2012.

[17] European Network and Information Security Agency (ENISA): http://europa.eu/legislation_summaries/information_society/internet/l24153_en.htm, pristupljeno u travnju 2012.

[18] Attacks against information systems:
http://europa.eu/legislation_summaries/information_society/internet/l33193_en.htm
pristupljeno u travnju 2012.

[19] Safer Internet programme 2009-13:
http://europa.eu/legislation_summaries/information_society/internet/l24190d_en.htm,
pristupljeno u travnju 2012.

[20] Standardisation: information technology and telecommunications:
http://europa.eu/legislation_summaries/information_society/internet/l24106_en.htm,
pristupljeno u travnju 2012.