HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Europska politika mrežne i informacijske sigurnosti

CCERT-PUBDOC-2005-06-124

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Povećanje vrijednosti informacija te briga o sigurnosti mreža i informacijskih sustava utječu na sve veći značaj i brigu oko mrežne i informacijske sigurnosti. Problem mrežne i informacijske sigurnosti jedno je od strateških pitanja Europske unije (u nastavku EU) a samim tima i razlog kreiranja europske politike mrežne i informacijske sigurnosti. Osnovna namjena sigurnosne politike EU je zaštita integriteta, dostupnosti i tajnosti informacija te informacijskih sustava.
Vijeće EU (engl. *Council of the European Union*) glavna je zakonodavna institucija Europske unije. Vijeće EU usvojilo je konvencije, europske sporazume i pripadajuće protokole, te preporuke kojima se nastoji regulirati pitanje mrežne i informacijske sigurnosti. 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.
Dokument daje prikaz europske politike sigurnosti kroz osnovne definicije mrežne i informacijske sigurnosti te opseg politike. Obzirom da je klasifikacija informacija temelj mrežne i informacijske sigurnosti u EU, najveći naglasak stavljen je upravo na opisivanje klasifikacije i označavanja informacija, nakon čega slijedi opis minimalnih sigurnosnih standarda. Na kraju je dat kratki osvrt za obveze zemalja članica EU pri organiziranju sigurnosti te zaključak.

2. Opseg Europske politike

Europska politika mrežne i informacijske sigurnosti razmatra se u kontekstu postojećih telekomunikacijskih politika, politika zaštite podataka i politika kibernetičkog kriminala (engl. *cybercrime*). Povezanost spomenutih politika prikazana je na slici (Slika 1).

Slika 1: Interakcija politika

Odlukom Vijeća EU o prihvaćanju sigurnosne politike definiraju se specifične aktivnosti u području mrežne i informacijske sigurnosti za zemlje članice, a to su:

- podizanje svijesti putem javnog informiranja, razvijanjem edukacijskih promocija i edukacije,
- učinkovit odgovor na sigurnosne incidente putem CERT (engl. *Computer Emergency Response Team*) organizacija zemalja članica s ciljem unapređenja i koordiniranog rada istih,
- tehnološka podrška za istraživanja i razvoj sigurnosti povezana sa strategijom unapređenja mrežne i informacijske sigurnosti,
- pružanje podrške i promocija standardizacije i certifikacije temeljem postojećih sigurnosnih standarda,
- harmonizacija pozitivnih propisa na nacionalnoj razini,
- međunarodna suradnja na području mrežne i informacijske sigurnosti.

Svakako je potrebno naglasiti da je sigurnosna politika namijenjena trima glavnim skupinama:

1. **građanima** kojima se mora osigurati zaštita osobnih podataka koja predstavlja osnovni uvjet individualne slobode u demokratskoj državi,
2. **tvrtkama** koje trebaju štiti intelektualno vlasništvo i osobne podatke građana, poštivati konkurentnost i osiguravati produktivnost, a što se sve vrlo često temelji na kompleksnim informacijskim sustavima,
3. **državnim aparatima** koji su odgovorni za zaštitu osjetljivih i klasificiranih informacija kao i za osiguranje kontinuiranog poslovanja državnih institucija i infrastrukture.

Sve navedene skupine imaju zajednički cilj, a to je sigurnost informacija ispunjavanjem relevantnih tehničkih, operacijskih i zakonskih uvjeta. Sigurnosna politika, može se reći, predstavlja kompromis između zaštite individualnih sloboda i implementacije restriktivnih sigurnosnih kontrola te alokacije materijalnih i ljudskih resursa.

3. Definiranje mrežne i informacijske sigurnosti

Generički sigurnosnih zahtjevi postavljeni pred organizaciju mrežne i informacijske sigurnost sastoje se od već spomenutog osiguranja slijedećih međusobno povezanih karakteristika:

- dostupnosti informacija,
- integriteta informacija,
- tajnosti informacija.

Mrežna i informacijska sigurnost definiraju se kao sposobnost obrane mreže i informacijskog sustava od gubitka dostupnosti, narušavanja integriteta i kompromitiranja tajnosti informacija koje su spremljene ili koje se prenose uporabom određenih servisa, a koji mogu biti ugroženi nenamjernim događajima ili malicioznim akcijama.

Mrežna i informacija sigurnost ima glavne ciljeve, a to su:

- zaštita klasificiranih informacija od špijunaže, kompromitiranja ili neautoriziranog otkrivanja,
- zaštita informacija koje se razmjenjuju putem mreža i informacijskih sustava od narušavanja integriteta i gubitka dostupnosti,
- zaštita informacija od sabotaže i malicioznih akcija,
- ograničavanje posljedica i usvajanje potrebnih dopunskih mjera u slučaju ugrožavanja (napada).

Osnovi principi sigurnosnih mjera su:

- osigurati dostupnost, integritet i tajnost informacija,
- osigurati da se informacijama pristupa na temelju načela „*need-to-know*“,
- spriječiti bilo kakvu vrstu neovlaštenog pristupa klasificiranim informacijama,
- osigurati identifikaciju osoba čiji položaj može ugroziti sigurnost klasificiranih informacija.

4. Klasifikacija i označavanje informacija

Obzirom na činjenicu da je klasifikacija informacija temelj za sigurnost, posebna se briga treba posvetiti pravilnoj klasifikaciji informacija prema određenim razinama klasifikacije, a ne pretjeranoj ili nedostatnoj klasifikaciji informacija. Sigurnosna politika EU primjenjuje se za EU klasificirane informacije. Pod pojmom `EU klasificirane informacije` shvaća se bilo koja informacija i materijal čije neovlašteno otkrivanje može uzrokovati štetu interesima EU ili bilo kojoj od zemalja članica.

U europskoj sigurnosnoj politici dokumentima se definiraju 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:

1. TRÈS SECRET UE / EU TOP SECRET: ova oznaka pridaje se informacijama i materijalima čije neovlašteno otkrivanje može izazvati *izuzetno ozbiljnu štetu* interesima Europske unije ili bilo kojoj od zemalja članica,

2. SECRET UE: ova oznaka pridaje se informacijama i materijalima čije neovlašteno otkrivanje može izazvati *ozbiljnu štetu* interesima Europske unije ili bilo kojoj od zemalja članica,
3. CONFIDENTIEL UE: ova oznaka pridaje se informacijama i materijalima čije neovlašteno otkrivanje može izazvati *štetu* interesima Europske unije ili bilo kojoj od zemalja članica,
4. RESTREINT UE: ova oznaka pridaje se informacijama i materijalima čije neovlašteno otkrivanje može *biti nepogodno* za interese Europske unije ili bilo koje od zemalja članica.

Jednom klasificirana informacija treba prolaziti ponovni pregled. Sve ustanove koje rade s klasificiranim informacijama trebaju slijediti standardiziran način klasifikacije te standardiziran način zaštite iste razine klasificiranih informacija.

Zahtjevi europske politike pri upravljanju klasificiranjem informacija su:

- informacije treba klasificirati samo kada je to nužno i na način da su opravdano i jednoznačno označene, a klasifikacijska oznaka treba važiti onoliko dugo koliko je to realno potrebno,
- za klasifikaciju informacija odgovoran je vlasnik (informacija),
- za klasifikaciju informacija treba postojati procedura,
- broj osoba koje imaju pristup EU TOP SECRET klasificiranim informacijama treba biti što je manji.

Prilikom primjene klasifikacije informacija treba voditi računa o tome da se klasifikacija oznaka dodjeljuje sukladno definicijama razina klasifikacija informacija (od 1 do 4). Ukoliko se unutar jednog dokumenta pojavi određeni dio koji ima različitu razinu klasifikacije, tada se taj dio mora tako i označiti, a cjelokupni dokument dobiva onu razinu klasifikacije koja je jednaka najvišoj razini barem jednog dijela dokumenta.

Dokumenti koji su jednom klasificirani određenom razinom mogu se deklasificirati te im se može smanjiti razina klasifikacije, no taj postupak mora biti popraćen pismenim dokazom. U slučaju da postoji mogućnost smanjivanja razine klasifikacije dokumenta te njegove deklasifikacije, tada je prilikom prve klasifikacije dokumenta preporučljivo unijeti datum ili vremenski interval važenja trenutne razine klasifikacije.

5. Minimalni sigurnosni standardi

Sigurnosna politika EU propisuje minimalne sigurnosne standarde koje trebaju zadovoljiti zemlje članice. Minimalni sigurnosni standardi obuhvaćaju slijedeća područja:

- ljudski resursi,
- fizička sigurnost,
- sigurnost informacija,
- sigurnost informacijskih sustava,
- razmjena informacija s trećim stranama.

5.1. Ljudski resursi

Pod sigurnosnim standardima vezanim uz ljudske resurse podrazumijeva se sigurnosna provjera osoblja kao predradnja dodjeljivanju ovlaštenja u obavljanju poslova. Osobe koje po svojim ovlaštenjima imaju pristup informacijama koje su klasificirane kao CONFIDENTIEL UE moraju biti provjerene na odgovarajući način prije nego li im se omogući pristup takvim informacijama. Sigurnosna provjera osoblja treba se provoditi i u slučaju kada osoba ima zaduženja koja uključuju tehničke operacije ili održavanje komunikacijskih i informacijskih sustava, a sadrže klasificirane informacije. Postupak treba biti oblikovan tako da se osiguraju provjere zadovoljava li pojedinac slijedeće kriterije:

- neupitnu lojalnost,
- diskreciju i integritet pri rukovanju klasificiranim informacijama.

Lojalnost, povjerljivost, pouzdanost i vjerodostojnost karakteristike su pojedinca kojem se može dati ovlaštenje za pristup povjerljivim informacijama, a da to ne predstavlja neprihvatljiv rizik za sigurnost informacija.

Posebnu pažnju treba posvetiti procedurama koje propisuju temeljitu provjeru osoba koje:

- imaju pristup EU TOP SECRET informacijama,

- obavljaju poslove koje uključuju konstantan pristup većem broju SECRET UE informacija,
- izvršavaju dužnosti koje zahtijevaju pristup kritičkim komunikacijskim ili informacijskim sustavima te imaju mogućnost ostvariti neovlašten pristup velikom broju klasificiranih informacija ili mogu nanijeti veliku štetu svojim akcijama ili tehničkom sabotažom.

Sve ustanove, tijela i servisi koji rukuju klasificiranim informacijama ili održavaju kritične komunikacijske i informacijske sustave moraju održavati zapise o sigurnosnoj provjeri osoblja te ovlaštenjima koja su dodijeljena pojedincu.
Sve osobe na funkcijama koje omogućuju pristup klasificiranim informacijama trebaju biti detaljno upućene u posao koji obavljaju. Upute se trebaju ponavljati u određenim vremenskim intervalima kako bi se osigurala sigurnost provođenja procedura za izvršenje posla. Preporučljivo je uključiti proceduru prema kojoj je osoblje dužno vlastoručnim potpisom potvrditi potpuno razumijevanju sigurnosnih odredbi koji se odnose na obavljanje poslova.
Dužnost uprave je nadgledati osoblje koje ima pristup klasificiranim informacijama te pristup kritičnim komunikacijskim ili informacijskim sustavima. Također, uprava mora nadgledati i podnositi izvješća o svakom incidentu ili uočenim ranjivostima.

5.2. Fizička sigurnost

Fizička sigurnost obuhvaća primjenu fizičkih i tehničkih mjera zaštite na mjestima na kojima se nalaze klasificirane informacije. Uvjeti koji moraju biti zadovoljeni po pitanju fizičke sigurnosti odnose se na obim fizičkih i tehničkih mjera zaštite kojima se štite klasificirane informacije proporcionalno stupnju klasifikacije, obimu te prijetnjama informacijama. Glavni cilj fizičkih sigurnosnih mjera jest spriječiti neovlašteni pristup klasificiranim informacijama.
Pod fizičkom sigurnošću prije svega shvaća se zaštita informacija implementacijom sustava za kontrolu ulaza i izlaza u i iz prostora u kojem se nalaze klasificirane informacije, za radnoga vremena, ali i nakon radnog vremena. Osim pristupa prostorima u kojima se radi s klasificiranim informacijama, fizička sigurnost obuhvaća i zaštitu zgrada u kojima su smještene informacije ili komunikacijski i informacijski sustavi.
Prilikom određivanja razine fizičke sigurnosti u razmatranje treba uzeti slijedeće kriterije:

- klasifikaciju informacija,
- obim i format informacija,
- fizičku prirodu i lokaciju zgrade u kojoj se nalaze informacije.

Osim navedenih kriterija, prilikom dizajna fizičke sigurnosti u razmatranje treba uzeti i procjenu vrijednosti resursa kao i prijetnje i ranjivosti prema identificiranim resursima.
Prema europskoj politici mrežne i informacijske sigurnosti sigurnosne mjere iz područja fizičke sigurnosti obuhvaćaju:

- sigurne zone za sve razine klasificiranih informacija osim RESTREINT UE,
- administrativne zone za RESTREINT UE razinu informacija,
- kontrolu ulaza i izlaza u sigurne zone,
- stražarske službe za sigurne zone van radnog vremena,
- sigurnosne kontejnere za spremanje klasificiranih informacija,
- zaključavanje, kontrolu ključeva i kombinacija za zaključavanje,
- uređaje za kontrolu pristupa,
- provjerenu sigurnosnu opremu,
- fizičku zaštitu aparata za kopiranje i telefax uređaja.

5.3. Sigurnost informacija

Sigurnost informacija u EU odnosi se na identifikaciju i klasifikaciju informacija i primjenu odgovarajućih sigurnosnih mjera s ciljem zaštite tajnosti, integriteta i dostupnosti informacija koje se obrađuju, spremaju ili prenose. Kako bi se zaštitio pristup klasificiranim informacijama od strane neovlaštenih korisnika, osigurao pristup informacijama ovlaštenim korisnicima te spriječila modifikacija ili brisanje informacija od strane neovlaštenih osoba trebaju se poduzeti odgovarajuće sigurnosne mjere.

Za pristup informacijama, prema europskoj politici mrežne i informacijske sigurnosti, koristi se načelo „*need-to-know*". Prema ovom načelu pristup informacijama osigurava se prema potrebama posla koji se obavlja, a ne prema hijerarhijskoj razini.

5.4. Sigurnost informacijskih sustava

Sigurnost informacijskih sustava unutar EU poznata je pod nazivom INFOSEC i ona podrazumijeva nekoliko ostalih tipova sigurnosti:

1. sigurnost podataka na elektroničkim medijima i računalima (COMPUSEC),
2. sigurnost podataka u sustavima za prijenos podataka (COMSEC),
3. sigurnost informacijske infrastrukture u posebnim kategorijama prostora od različitih vrsta prisluškivanja (TECSEC).

Sigurnost informacijskih sustava uključuje nadgledanje informacijskih sustava kako bi se spriječile špijunaža, sabotaža, terorizam i ostale subverzivne aktivnosti. Sigurnost informacijskih sustava podrazumijeva i uzajamno djelovanje svih strana uključenih u rad informacijskog sustava: projektanata informacijskog sustava, odgovornih za implementaciju i operativnost informacijskog sustava kao i korisnika informacijskog sustava.

5.5. Razmjena informacija s trećim stranama

Trećim stranama smatraju se zemlje članice ili međunarodne organizacije. U postupku razmjene informacija između Vijeća EU 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 razmjeni informacija.

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

6. Osvrt na organizaciju sigurnosti u zemljama članicama

Organi EU pretpostavljaju opću odgovornost za harmonizaciju i vođenje prilikom podizanja svijesti o sigurnosti kao i prilikom uspostavljanja koherentnog zakonske regulative kroz postupak usvajanja direktiva i okvirnih odluka. Zemlje članice EU imaju obvezu prilagoditi svoje nacionalne pozitivne propise direktivama EU. Njihova obveza je implementirati operacijske i praktične okvire i osigurati njihovo provođenje.

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

- održavanje sigurnosti klasificiranih informacija koje su u posjedu nacionalnog tijela, agencije, javne ili privatne ustanove, u zemlji ili inozemstvu,
- autorizacija uspostavljanja EU TOP SECRET registra,
- periodična inspekcija svih sigurnosnih postavki koje imaju za cilj zaštitu klasificiranih informacija,
- uspostavljanje postupka sigurnosne provjere osoblja bez obzira na nacionalnost unutar nacionalnih tijela ukoliko imaju pristup informacijama klasificiranim kao EU TOP SECRET, SECRET UE i CONFIDENTIEL UE,
- osmišljavanje sigurnosnih planova koji će sprečavati neautorizirani pristup klasificiranim informacijama.

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 temeljenu na sigurnosnom standardu ISO/IEC 17799 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.

7. Zaključak

Na sve veću važnost sigurnosti informacija i informacijskih sustava ukazuju dvije bitne činjenice. Prva činjenica jest da su NATO i EU potpisale NATO-EU Pakt o sigurnosti u Ateni još 14. ožujka 2003. godine, a jedan od ciljeva bio je otvaranje sigurne razmjene klasificiranih informacija između organizacija.
Druga činjenica je ta da je EU početkom 2004. godine osnovala Europsku agenciju za mrežnu i informacijsku sigurnost (engl. *European Network and Information Security Agency*, ENISA) čiji je glavni cilj promovirati i razvijati kulturu mrežne i informacijske sigurnosti unutar EU.
Ono što je zadaća EU i zemalja članica u području mrežne i informacijske sigurnosti jest približavanje sigurnosne politike EU te nacionalnih sigurnosnih politika zemalja članica. Ambiciozan koncept izgradnje sigurnog informacijskog sustava EU temelji na politikama te preporučuje uporabu internacionalnih standarda iz područja informacijske sigurnosti (ISO/IEC 17799, ISO/IEC 15408).
Republika Hrvatska, kao zemlja kandidatkinja, nailazi na sigurnost kao preduvjet punog razvoja informacijskog društva, a kojeg postavlja EU. Po pitanju sigurnosti, Središnji državni ured za *e*-Hrvatsku, odnosno Stručna skupina za informacijsku sigurnost, kreirala je Nacionalni program informacijske sigurnosti Republike Hrvatske čiji je prijedlog obavljen u siječnju 2005. godine. Program definira ciljeve informacijske sigurnosti na razini Republike Hrvatske, nadležnosti i poslove pojedinih institucija u području informacijske sigurnosti. To je samo jedan korak prema sigurnom informacijskom sustavu koji je zahtjevan od EU, ali i potreba modernog informacijskog društva.

8. Reference

[1] COUNCIL DECISION 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

[2] Communication from The Commision of the Council, The European Parliament, The European Economic and Social Committee and The Committee of the Regions: : Network and Information Security: Proposal for a European Policy Approach, COM(2001)298 final
http://www.usdoj.gov/criminal/cybercrime/intl/netsec_comm.pdf

[3] Esterle, Alain: Information security, A new challenge for the EU, Chaillot Paper, no. 76
http://www.iss-eu.org/chaillot/chai76.pdf

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

[5] ENISA
http://www.enisa.eu.int/