VODIČ:

CENTAR ZA PREVENCIJU IKT RIZIKA - CERT

SHARE FOUNDATION - 2017

VODIČ: CENTAR ZA PREVENCIJU IKT RIZIKA - CERT
SHARE FONDACIJA, MAJ 2017.
UREDNICI: ĐORĐE KRIVOKAPIĆ I VLADAN JOLER
AUTORI: DANILO KRIVOKAPIĆ, ANDREJ PETROVSKI,
BOJAN PERKOV I SONJA MALINOVIĆ
OBRADA TEKSTA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ: 200

PODRŠKA PROJEKTU:

Kingdom of the Netherlands

Министарство трговине, туризма
и телекомуникација

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад
004.738.5:351.083.8(036)
CENTAR za prevenciju IKT rizika - CERT : vodič / [autori Danilo Krivokapić ... [et al.] ; urednici Đorđe Krivokapić, Vladan Joler]. - Novi Sad : Share fondacija, 2017 (Novi Sad : NS press). - 31 str. ; 24 cm

Tiraž 200. - Napomene i bibliografske reference uz tekst.

ISBN 978-86-89487-12-1
1. Кривокапић, Данило
а) Интернет - Заштита података - Водичи
COBISS.SR-ID 314376711

ŠTA JE TO CERT?

ŠTA JE TO CERT?

Centri za prevenciju rizika u informaciono-komunikacionim sistemima ustanovljeni su po uzoru na slične organizacije posvećene zaštiti informacione bezbednosti u svetu (eng. Computer Emergency Response Team, CERT), i mogu delovati na nacionalnom nivou ali i u specifičnim sektorima kao što su finansijski sistem, državni organi, pa čak i u okviru samo jednog pravnog subjekta. Alternativno, ove organizacije se zovu CSIRT (Computer Security Incident Response Team), CIRT (Computer Incident Response Team), ili slično. U zavisnosti od lokalnog pravnog okvira, uloga CERT-a može biti edukativna, savetodavna, preventivna i istraživačka, što između ostalog podrazumeva praćenje incidenata na nacionalnom nivou, pružanje ranih upozorenja i informacija o rizicima i incidentima u oblasti informacione bezbednosti, ali i promociju bezbednosne kulture među građanima, u državnim institucijama i privatnom sektoru.

Prvom organizacijom ove vrste smatra se CERT koordinacioni centar (CERT/CC) Instituta za softverski inženjering na Karnegi Melon univerzitetu u Pitsburgu, SAD. CERT/CC je osnovan 1988. godine, nakon incidenta sa tzv. Moris crvom, jednim od prvih kompjuterskih virusa distribuiranih preko interneta. Virus je onesposobio na hiljade povezanih kompjutera, razotkrivajući ranjivost mreže. Razvoj interneta od tada podrazumeva sve bolju zaštitu, ali se istovremeno unapređuju i tehnike za narušavanje bezbednosti mreže. Tako je CERT/CC postao deo CERT odeljenja Instituta za softverski inženjering, čija su dodatna polja delovanja edukacija i sprovođenje treninga, istraživanje i razvoj, podizanje svesti, forenzika, organizaciona bezbednost i uspostavljanje globalnih odnosa.[1]

Već 1990. godine nacionalne organizacije su osnovale međunarodnu koaliciju FIRST (Forum of Incident Response and Security Teams),[2] koja danas broji više od 350 članica iz 80 država sveta. Među njima su brojni nacionalni CERT-ovi, kao i CERT-ovi komercijalnog sektora (Cisco Systems CSIRT), akademske zajednice (Akademski CERT Izraela) i banaka (CERT nemačke Komerc banke).[3]

01 Česta pitanja o CERT odeljenju [na engleskom] https://www.cert.org/faq/index.cfm
02 O Forumu [na engleskom] https://www.first.org/about
03 Članice Foruma [na engleskom] https://www.first.org/members/map

CERT U DOMAĆOJ REGULA-TIVI

CERT U DOMAĆOJ REGULATIVI

Zakon o informacionoj bezbednosti (ZIB), usvojen 2016, u članovima 14-19 definiše i bliže uređuje pojam i ulogu:

- Nacionalnog CERT-a;
- Posebnih CERT-ova;
- CERT-a Republičkih organa i
- CERT-ove samostalnih operatora IKT sistema.

Iako Zakon koristi englesku skraćenicu CERT, ona ne predstavlja pravi akronim u našem pravnom sistemu, budući da označava Centar za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalni i Posebni CERT) ili Centar za bezbednost IKT sistema (Ostali). Zakonodavac se odlučio da zadrži međunarodno prihvaćenu skraćenicu, dobro poznatu među stručnjacima za informacionu bezbednost, kako bi se izbegla konfuzija stvaranjem novih akronima ili upotrebom predugih naziva.

Ovim Zakonom ustanovljen je, s jedne strane, Nacionalni CERT čija se nadležnost prostire na sve IKT sisteme u Republici Srbiji, kao i na sve incidente i događaje koji ugrožavaju bezbednost IKT sistema, dok s druge strane svi ostali CERT-ovi zapravo obavljaju poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično.

ŠTA JE NACIONALNI CERT?

ŠTA JE NACIONALNI CERT?

Nacionalni CERT je telo koje obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou. Ovakvo telo postoji u 102 zemlje sveta, uključujući gotovo sve evropske zemlje. Nacionalni CERT u Sloveniji, na primer, osnovan je pre 20 godina. Nadležnosti nacionalnih CERT-ova se razlikuju među državama, u zavisnosti od specifičnosti infrastruktutre, ali je to uvek ekspertska organizacija čija je glavna nadležnost koordinacija i komunikacija na nacionalnom i međunarodnom nivou, radi prevenicije i upravljanja rizicima u ovoj oblasti. Za poslove Nacionalnog CERT-a u Republici Srbiji nadležna je Regulatorna agencija za elektronske komunikacije i poštanske usluge (RATEL).

Nacionalni CERT je nadležan da prati incidente na nacionalnom nivou, da pruža rana upozorenja, uzbune i najave, te da informiše relevantna lica o rizicima i incidentima. Takođe, Nacionalni CERT reaguje po prijavljenim, ili na drugi način otkrivenim incidentima, tako što pruža savete na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja. Ovo telo kontinuirano izrađuje analize rizika i incidenata, podiže svest kod građana, privrednih subjekata i organa javne vlasti o značaju informacione bezbednosti, te vodi evidenciju Posebnih CERT-ova.

Budući da su njegove nadležnosti pre svega preventivne, Nacionalni CERT najčešće neće biti u poziciji da reaguje i pomogne IKT sistemima u kriznim i hitnim situacijama.

ŠTA JE POSEBAN CERT?

ŠTA JE POSEBAN CERT?

Posebni CERT-ovi takođe obavljaju poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima, pa zapravo imaju sličnu ulogu i nadležnosti kao Nacionalni CERT. Ipak, njihova specifičnost se ogleda u tome što su specijalizovani za određenu oblast ili grupu pravnih subjekata kao što su, na primer, različite grane privrede, finansijske institucije, državni organi, civilni sektor, akademski sistem i slično, te stoga prate stanje i reaguju u slučaju incidenata samo u toj oblasti ili grupi. Na ovaj način, posebni CERT-ovi vremenom stiču specifična znanja i iskustva u svojoj oblasti i spremni su da pruže specijalizovanu pomoć svojim korisnicima.

U skladu sa Zakonom, Poseban CERT može biti pravno lice ili organizaciona jedinica u okviru pravnog lica. Ovaj status se formalno stiče upisom u evidenciju posebnih CERT-ova na osnovu prijave Nacionalnom CERT-u, odnosno RATEL-u. Sam postupak registracije je regulisan Pravilnikom o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u infromaciono-komunikacionim sistemima (''Službeni glasnik RS'', broj 12/17).

SHARE CERT je prvi Poseban CERT registrovan u Republici Srbiji u skladu sa Zakonom, 3. aprila 2017. godine. Specijalizovan za pružanje pravne i tehničke podrške onlajn i građanskim medijima u Srbiji koji su pretrpeli tehničke napade, SHARE CERT je formiran na osnovu iskustva stručnog tima SHARE Fondacije u pružanju ovakve vrste podrške u više desetina slučajeva proteklih godina. Tim SHARE CERT-a godinama se aktivno bavi istraživanjem i sistematizacijom znanja iz oblasti informacione bezbednosti onlajn i građanskih medija, publikovanjem priručnika, organizovanjem javnih diskusija u saradnji sa nadležnim državnim institucijama, kompanijama i organizacijama civilnog društva, kao i treninga i radionica na temu informacione bezbednosti u Srbiji i inostranstvu.

Organizacija, dakle, može obavljati poslove Posebnog CERT-a i pre formalne registracije, međutim, upis u registar pruža dodatnu vidljivost, olakšava korisnicima kontakt sa Posebnim CERT-om i unapređuje saradnju Posebnog i Nacionalnog CERT-a, kao i između posebnih CERT-ova. Konačno, upis u registrar istovremeno predstavlja potvrdu o ispunjavanju propisanih uslova, svojevrsnu sertifikaciju da je organizacija sposobna da obavlja poslove CERT-a.

ZNAČAJ SARAD-NJE

ZNAČAJ SARADNJE

Komunikacija različitih CERT-ova unapređuje operativnu bezbednost u tehničkom smislu, ali i razvoj poverenja među akterima, što je od naročitog značaja kada je reč o saradnji Nacionalnog i posebnih CERT-ova. Redovna komunikacija neophodna je akterima za optimizaciju kapaciteta, dok blagovremena razmena informacija istovremeno omogućava efikasne reakcije u slučaju incidenta.

Jedna od Zakonom definisanih uloga Nacionalnog CERT-a jeste vođenje evidencije posebnih CERT-ova. Tako ovo telo postaje centralna tačka povezivanja postojećih CERT-ova u državi, posredujući u saradnji javnog i privatnog sektora. Budući da su posebni CERT-ovi, pored razvoja u svojoj oblasti, dužni da grade kapacitete za saradnju sa postojećim CERT-ovima, Nacionalni CERT služi kao platforma za prikupljanje i usmeravanje informacija, znanja i dobrih praksi među različitim akterima. Primarna saradnja posebnih CERT-ova, bez obzira na to da li su javni ili privatni, treba da se odvija na tehničkom i stručnom nivou. Osim na principu deljenja resursa između CERT-ova koji imaju različite kapacitete i polja stručnosti, njihova saradnja se zasniva i na razmeni znanja, relevantnih i aktuelnih informacija i iskustva. Bez obzira da li će i kako u daljoj primeni novih zakonskih rešenja država svojim resursima pomagati formiranje posebnih CERT-ova kako bi se pokrila svaka oblast sistema, javno-privatno partnerstvo može poslužiti kao dobar mehanizam, posebno na nivou tehničke i stručne saradnje u pravcu racionalizacije resursa.

U slučaju sajber incidenta na nacionalnom nivou, privatni sektor i posebni CERT-ovi mogu odigrati važnu ulogu u reagovanju i prevazilaženju njegovih posledica. U procesu digitalizacije državne administracije, na primer, posebni CERT-ovi mogu značajno da doprinesu svojim znanjem, iskustvom i razvijenim standardima u izgradnji mehanizama za odbranu od sajber incidenata. Zbog toga je neophodno blagovremeno omogućiti saradnju javnog i privatnog sektora.

Sledeći stepen saradnje posebnih CERT-ova može se odvijati na nivou internih politika. Mada je proces formiranja posebnih CERT-ova tek počeo, treba razmotriti mogućnost udruživanja posebnih CERT-ova, odnosno formalizovanja saradnje na kreiranju i promociji zajedničkih politika, kao i preporuka za poboljšanje formalnog i tehničkog aspekta rada. Time bi se, ujedno, obezbedila lakša saradnja sa državom na nivou politika i omogućio zajednički nastup, zasnovan na konkretnom iskustvu i praksi razvijenoj u posebnim CERT-ovima, kao i na predlozima politika zasnovanim na zajedničkim interesima.

Ovakav razvoj predstavlja prirodnu evoluciju saradnje koja, počevši od tehničkog nivoa, vremenom obuhvata i druge aspekte informacione bezbednosti, prevencije i reagovanja na rizike, sve do nivoa politika. Istovremeno, dublji nivo saradnje omogućava nerivalsku razmenu znanja javnih i privatnih aktera, stimulišući opšti napredak izvan granica puke tehničke saradnje propisane Zakonom.[4]

04 Vodič kroz informacionu bezbednost u Republici Srbiji, 2016 https://www.ceas-serbia.org/images/2016/09/Vodic _ kroz _ informacionu _ bezbednost _ SRB _ Web _ 1.pdf

CERT U SVETU

CERT U SVETU

Kao vodeće organizacije za unapređenje standarda informacione bezbednosti, CERT-ovi imaju veliki značaj i za kulturu bezbednosti informacionih sistema. Budući da su u svetu čitavi sistemi javne uprave, obrazovanja, bankarstva, nauke i trgovine, svoje poslovanje najvećim delom preneli u digitalno okruženje, bezbednost postaje vitalno pitanje ne samo ovih sistema, već i samog društva. Stoga, pored nacionalnih CERT-ova koji prate stanje informacione bezbednosti na nivou cele države, postoje i posebni CERT timovi specijalizovani za pojedine oblasti, od čije brzine i efikasnosti često zavisi funkcionalnost sistema, kao i opšti nivo bezbednosne kulture u zajednici. Međunarodna saradnja nacionalnih i posebnih CERT-ova u tome može imati ključni značaj.

CERT-EU, EVROPSKA UNIJA

Posle jednogodišnjeg pilot programa, institucije Evropske unije su u septembru 2012. odlučile da formiraju Centar za prevenciju bezbednosnih rizika u informacionim sistemima Evropske unije (CERT-EU). Ovaj regionalni CERT čine stručnjaci za informacionu bezbednost iz vodećih institucija EU: Evropske komisije, Generalnog sekretarijata Saveta EU, Evropskog parlamenta, Komiteta regiona i Evropskog ekonomskog i socijalnog komiteta. CERT-EU aktivno sarađuje sa CERT-ovima država članica EU, kao i sa specijalizovanim kompanijama za IT bezbednost. [5]

US-CERT, SJEDINJENE AMERIČKE DRŽAVE

CERT federalnih organa SAD je najpre formiran kao Federalni centar za računarske incidente (Federal Computer Incident Response Center, FedCIRC) ranih 2000-ih, kada je informaciona infrastruktura federalnih organa počela da biva sve češće na meti napada. Nakon uspostavljanja Ministarstva za nacionalnu bezbednost, FedCIRC 2003. godine menja ime u US-CERT. Njegove glavne aktivnosti uključuju:

- Pružanje sajber-bezbednosne zaštite federalnim civilnim organima;
- Razvoj i distribuciju obaveštenja ministarstvima i agencijama, organima vlasti saveznih država, te lokalnim, plemenskim i teritorijalnim administracijama, vlasnicima i rukovaocima kritične infrastrukture, privatnoj industriji i međunarodnim organizacijama;
- Reagovanje na incidente i analiziranje podataka o novim pretnjama u sajber prostoru;
- Saradnju sa stranim državama i međunarodnim telima. [6]

CERT-IN, INDIJA

Indijski nacionalni CERT je osnovan 2004. godine i nalazi se u okviru Ministarstva elektronike i informacione tehnologije Vlade Indije. Čine ga eksperti iz indijske sajber-bezbednosne zajednice, a između ostalog se bavi sakupljanjem, analizom i diseminacijom informacija o sajber napadima, uzbunjivanjem i koordinacijom aktivnosti prilikom bezbednosnih incidenata. CERT-In poseduje veliku bazu znanja koju čine preporuke, analitički izveštaji i statistike u vezi sa bezbednosnim incidentima u sajber prostoru Indije. [7]

AUSCERT, AUSTRALIJA

Jedan od najstarijih CERT-ova u svetu je AusCERT, koji se nalazi na Univerzitetu Kvinslend u Australi-

05 CERT-EU [na engleskom] https://cert.europa.eu/cert/plainedition/en/cert_about.html
06 US-CERT [na engleskom] https://www.us-cert.gov/about-us
07 CERT-In [na engleskom] http://www.cert-in.org.in/

ji. Osnovan je 1993. godine i ulogu nacionalnog CERT-a za Australiju vršio je do 2010. kada je federalna vlada osnovala drugi. AusCERT pruža savete u oblasti informacione bezbednosti članovima svoje mreže, što uključuje i sektor visokog obrazovanja. Takođe, AusCERT održava brojne kontakte sa CERT-ovima u Severnoj Americi, Britaniji, Evropi i Aziji radi razmene ranih upozorenja o globalnim pretnjama. [8]

CERT-BUND, NEMAČKA

CERT-Bund je formiran u okviru Savezne kancelarije za informacionu bezbednost kao centralna tačka kontakta za mere prevencije i reakcije na bezbednosne incidente u IKT sistemima saveznih agencija Nemačke. Njegovi poslovi, između ostalog, obuhvataju:

- Objavljivanje preporuka i preventivnih mera;
- Informisanje o bezbednosnim propustima u hardveru i softverskim prozvodima;
- Predlaganje mera za rešavanje poznatih propusta;
- Pružanje podrške javnim službama u reagovanju na bezbednosne incidente u IKT sistemima;
- Predlaganje mera za ublažavanje posledica incidenata.

U okviru CERT-Bunda deluje i Nacionalni centar za IT incidente. Iako prvenstveno pruža usluge državnim organima, kroz projekat "CERT za građane" CERT-Bund informiše širu javnost o rizicima i merama za unapređenje lične digitalne bezbednosti.[10]

SI-CERT, SLOVENIJA

SI-CERT je nacionalni CERT zadužen za bezbednosne incidente u okviru mreža i informacionih sistema na teritoriji Slovenije. Radi pod okriljem Akademsko-istraživačke mreže Slovenije (ARNES), neprofitne institucije koju finansira Direktorat za informaciono društvo Ministarstva obrazovanja, nauke i sporta. Kroz svoje aktivnosti, SI-CERT ostvaruje aktivnu saradnju i partnerstvo sa svim relevantnim akterima na polju informacione bezbednosti, kao što su internet provajderi i organi vlasti. Od 2010. godine, odlukom Vlade Slovenije, SI-CERT je proglašen Centrom za odgovore na bezbednosne incidente u IKT sistemima državnih organa.[11]

08 AusCERT [na engleskom] https://www.auscert.org.au/about
09 CERT-Bund [na engleskom] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund _ node.html
10 Bürger-CERT [na nemačkom] https://www.buerger-cert.de/
11 SI-CERT [na engleskom] https://www.cert.si/en/detailed-information-rfc-2350/

MEĐU-NARODNE ORGANI-ZACIJE

MEĐUNARODNE ORGANIZACIJE

TRUSTED INTRODUCER

Sistem "Trusted Introducer" ustanovila je evropska CERT zajednica 2000. godine u cilju izgradnje servisne infrastrukture i pružanja specifičnih usluga samim CERT-ovima.[12] Ovaj servis je istovremeno svojevrsni klirinški zavod koji garantuje ispunjenje obaveza, ažurira informacije i posreduje u komunikaciji. Servis ima oko 300 upisanih članica iz zemalja Evrope i sveta, uz dvostepenu kategorizaciju dodatnih usluga za akreditovane i seritifkovane timove. Deo usluga dostupan je i široj javnosti kroz pretragu direktorijuma članica, njihovih podataka i kontakata.[13]

Status akreditovanog, odnosno sertifkovanog tima stiče se na osnovu utvrđene procedure, uz godišnju nadoknadu. U "Trusted Introducer" direktorijumu dva tima iz Srbije imaju status upisanih članova, CSIRT Akademske mreže Srbije (od 2011) i CERT Ministarstva unutrašnjih poslova (od 2016).

FIRST

Od nastanka Foruma timova za odgovor na incidente i bezbednost (Forum of Incident Response and Security Teams, FIRST) 1990. godine, njegovi članovi se bave rešavanjem neprekidnog niza pretnji i napada na računarske mreže i sisteme povezane preko interneta. Forumu je pristupio širok spektar timova koji se bave bezbednosnim pretnjama, uključujući timove iz komercijalnog, akademskog i državnog sektora.

FIRST okuplja preko 350 timova iz 80 različitih država, u statusu punopravnih ili pridruženih članova.[14] Punopravno članstvo podrazumeva pravo glasanja i predlaganja novih pridruženih i punopravnih članova. Srbija nema svoje predstavnike u Forumu, dok su iz regiona zastupljeni Slovenija i Crna Gora sa svojim nacionalnim organizacijama, te Hrvatska sa nacionalnim i CERT-om državnih tela.

12 Trusted Introducer [na engleskom] https://www.trusted-introducer.org
13 Direktorijum TI [na engleskom] https://www.trusted-introducer.org/directory/teams.html
14 FIRST članovi [na engleskom] https://www.first.org/members/teams#

ITU

Međunarodna telekomunikaciona unija (ITU), specijalizovana agencija pri Ujedinjenim nacijama, bavi se komunikacionim i informacionim tehnologijama. U okviru posebnog CIRT programa, ITU sarađuje sa državama članicama UN, kao i regionalnim organizacijama, na izgradnji kapaciteta za koordinisane odgovore na sajber napade. Takođe, ITU pruža podršku u procesu planiranja, implementacije i operativnosti nacionalnih CERT-ova. U okviru ovog programa, ITU sprovodi procenu spremnosti država za uspostavljanje nacionalnih timova koja je, između ostalih, sprovedena i u državama regiona, i to u Crnoj Gori, Albaniji, Makedoniji i Srbiji.

ITU mrežu čine 102 nacionalna CERT-a.[15]

15 ITU mreža [na engleskom] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT _ Status.pdf

ŠTA RADI POSEBAN CERT?

ŠTA RADI POSEBAN CERT?

Pored nacionalnih CERT-ova koji se sveobuhvatno bave bezbednosnim incidentima u IKT sistemima na nacionalnom nivou, širom sveta postoji veliki broj posebnih CERT-ova, fokusiranih na unapređenje informacione bezbednosti u okviru jedne društvene oblasti, grupe subjekata, pa čak i unutar samo jedne kompanije. Recimo, gigant onlajn prodaje, Amazon ima svoj tim za bezbednosne incidente (Amazon SIRT) koji je član koalicije FIRST.[16] Imajući u vidu složenost i specifičnost određene zajednice ili grupe subjekata (akademske institucije, banke, i slično), odnosno poverljivu prirodu informacija kojima kompanije upravljaju, posebni CERT-ovi sa svojim visoko specijalizovanim stručnjacima svakako su najkompetentnija adresa za zaštitu od sajber-bezbednosnih incidenata i uspostavljanje preventivnih mera.

Jedan takav primer je ICS CERT (Industrial Control Systems Cyber Emergency Response Team) kompanije "Kasperski labs", poznatog proizvođača anti-virus softvera.[17] ICS CERT je nekomercijalni projekat kompanije i pruža različite usluge zainteresovanim akterima u industriji. Drugim rečima, ICS CERT besplatno deli informacije i ekspertizu sa mrežom partnera iz više oblasti:

- Analiza usklađenosti sa standardima bezbednosti IKT sistema.
- Informisanje o najčešćim propustima proizvoda koji se koriste u industrijskim informacionim sistemima.
- Pružanje informacija o malveru i drugim vrstama pretnji po bezbednost IKT sistema.
- Daljinska detekciju pretnji, tj. procena ljudskog faktora i lanca povezanih aktera (npr. kompanija podizvođača).
- Opšta procena bezbednosti IKT sistema.
- Testiranje otpornosti IKT sistema na napade.
- Analiza malicioznih fajlova.
- Analiza drugih predmeta iz IKT sistema (radnih stanica, mrežnih uređaja, eksternih memorija).
- Koordinacija postupaka prilikom napada.[18]

Akademske institucije koje često dele informacionu infrastrukturu, poput Akademske mreže Srbije - AMRES, takođe imaju specifične potrebe u zaštiti informacione bezbednosti. Radi što bolje koordinaci-

16 Amazon SIRT [na engleskom] https://www.first.org/members/teams/amazon _ sirt

17 Kaspersky Lab ICS CERT [na engleskom] https://ics-cert.kaspersky.com/

18 Usluge ICS CERT [na engleskom] https://ics-cert.kaspersky.com/services/

je prilikom bezbednosnih incidenata i odgovora na njih, osnivaju se posebni CERT-ovi i za akademske zajednice. Primer takvog posebnog CERT-a jeste IUCC CERT akademske mreže Izraela, koji je član FIRST koalicije CERT-ova od 1995. godine. IUCC CERT je zadužen za bezbednost mreže mreže osam univerziteta širom Izraela.[19]

Centar za bezbednosne incidente (Service Center for Security Incidents - CAIS) Akademske mreže Brazila osnovan je 1997. godine s ciljem da sačuva bezbednost mreže, otkrije, upravlja i spreči bezbednosne rizike. Do sada, Centar je dokumentovao više od milion slučajeva, a među uslugama koje pruža nalaze se i katalog prevara, razvoj akademskih CSIRT-ova na univerzitetima u Brazilu, podizanje svesti i edukacija o informacionoj bezbednosti i rešavanje bezbednosnih incidenata. [20]

19 IUCC CERT [na engleskom] https://cert.iucc.ac.il/

20 Brazilska nacionalna istraživačka i obrazovna mreža [na engleskom] https://www.rnp.br/en/services/security

OSNOVNI PROCE-SI U RADU CERT OR-GANI-ZACIJA

OSNOVNI PROCESI U RADU CERT ORGANIZACIJA

Zadatak svake CERT organizacije je da prati i analizira pretnje po bezbednost IKT sistema, pruža pomoć u prepoznavanju pretnji i prevenciji napada, osnažuje aktere za adekvatne odgovore na napad, obezbeđuje pravnu asistenciju u procesuiranju sajber incidenata, održava komunikaciju sa nadležnim institucijama, i drugo.

Da bi CERT organizacija mogla uspešno da realizuje svoje aktivnosti neophodno je da, za početak, definiše viziju, misiju i ciljeve. Ukoliko su jasno i precizno utvrđeni, vizija, misija i ciljevi predstavljaju osnovni okvir poslovanja i razvoja organizacije i pružaju fokus organizacionom timu. U slučaju CERT organizacija to može biti, između ostalog, oporavak sistema od posledica napada, analiza potencijalnih pretnji i napada na bezbednost IKT sistema, koordinacija informacija, sprovođenje istraga kompjuterskog kriminala i monitoring sistema za detekciju upada.

Osnovne usluge CERT organizacija podrazumevaju izveštavanje, analizu i tehičku podršku. One se detaljnije mogu opisati u svetlu svoja četiri osnovna procesa: trijaža, razrešavanje, izdavanje obaveštenja i davanje povratnih informacija korisnicima. Svaki od ovih procesa je potrebno interno dokumentovati, u okviru CERT organizacije, u vidu jasnih opisa.[21]

- Proces trijaže predstavlja osnovnu tačku kontakta i podrazumeva prihvatanje, prikupljanje, sortiranje i prosleđivanje dobijenih informacija. Kada deo CERT tima koji se bavi trijažom dobije neku informaciju ili prijavu problema, šalje se potvrda pošiljaocu da je poruka primljena, a zatim se informacija sortira, prioritizuje, dodaje joj se jedinstveni idenitifikator i prosleđuje se drugim procesima u okviru implementiranih servisa.[22]
- Proces razrešavanja incidenata podrazumeva analizu prijavljenih bezbednosnih incidenata ili pretnji i davanje odgovora na njih. Tokom analize se utvrđuje uzrok, analiziraju se dokazni materijali, utvrđuje se ko je uključen u incident, kao i koja vrsta podrške i u kojoj meri je potrebna. Kakav će odgovor biti zavisi od CERT-ovih misija, ciljeva i definicija usluga, ali i od postavljenih prioriteta.
- Proces izdavanja obaveštenja predstavlja obaveštavanje u različitim formatima, kao što su:

21 Studija izvodljivosti izgradnje Nacionalnog CERT-a, RATEL, 2016. http://www.ratel.rs/upload/documents/Studije/Studija%20izvodljivosti%20izgradnje%20Nacionalnog%20CERT-a.pdf

22 Ibid.

1. najave
2. upozorenja
3. saveti
4. kratka obaveštenja
5. smernice
6. tehničke procedure

Glavni cilj ove funkcije je da se korisnicima proslede informacije koje će im pomoći u zaštiti njihovih sistema, ili da bi se pronašli tragovi potencijalnog napada davanjem informacija o mogućim, tekućim ili nedavnim pretnjama. Dodatno, sugerišu se metode za prevenciju, otkrivanje ili oporavak od incidenata. Kada se objavljuju informacije u vezi sa napadom određenog tipa, treba obezbediti da je nivo informacija koje se otkrivaju dovoljan da korisnici razumeju prirodu napada i mogu da provere da li su postali žrtve tog napada, ali ne toliko detaljne da bi mogle da se upotrebe kao uputstvo za sprovođenje napada.[23]

- Proces davanja povratnih informacija predstavlja komunikaciju sa korisnicima i entitetima, bilo na zahtev ili u regularnoj formi (npr. u formi izveštaja). Zahtevi koje članovi CERT-a uobičajeno dobijaju mogu se podeliti u četiri kategorije: opšti zahtevi na temu informacione bezbednosti, zahtevi medija, ostali zahtevi i pitanja, zahtevi van okvira delovanja CERT-a.
- Proces saradnje podrazumeva sve vrste interakcija koje CERT tim ima sa drugim entitetima. Poželjno je redovno održavanje postojećih i ostvarivanje novih kontakata sa lokalnim i regionalnim partnerima i klijentima, kao i kreiranje adekvatnih baza podataka. Međutim, tokom sva četiri osnovna procesa dolazi do razmene informacija, zato je važno pažljivo izabrati partnerske organizacije kako bi se očuvao integritet, poverljivost i raspoloživost podataka.
- Proces upravljanja informacijama veoma je važan deo osnovnog procesa. Informacije je potrebno prikupljati i evidentirati, nakon toga verifikovati, kategorizovati i na kraju čuvati. Neke informacije se mogu i objaviti, kako bi se dale smernice ili podrška zainteresovanim stranama, ali tokom čitavog procesa bezbednost svih informacija u okviru CERT organizacije mora biti na najvišem nivou.

23 Ibid.

KAKO REGI-STROVA-TI POSE-BAN CERT U SRBIJI

KAKO REGISTROVATI POSEBAN CERT U SRBIJI

Delatnosti i poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima može obavljati i organizacija koja nije registrovana kao poseban CERT, ali formalna registracija svakako može poboljšati odnos sa korisnicima kao i saradnju sa drugim CERT-ovima i sličnim organizacijama.

Postupak registracije je regulisan Pravilnikom o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbedonosnih rizika u infromaciono-komunikacionim sistemima.[24] Ovim dokumentom propisani su osnovni uslovi koje organizacija treba da ispunjava kako bi mogla biti registrovana i upisana u Evidenciju posebnih CERT-ova:

- da ima sedište na teritoriji Republike Srbije;
- da je pravno lice ili organizaciona jedinica u okviru pravnog lica;
- da obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično.

Registraciona prijava se podnosi Nacionalnom CERT-u koji vodi ovu evidenciju i to na propisanom obrascu koji je dat u prilogu Pravilnika. U registracionoj prijavi potrebno je popuniti sledeće podatke o posebnom CERT-u:

- Naziv subjekta (pravnog lica) koji podnosi prijavu
- Naziv posebnog CERT-a
- Sedište (mesto, ulica i broj)
- Matični broj
- Poresko-identifikacioni broj (PIB)
- Broj telefona
- Broj faksa
- Adresa internet strane
- Adresa elektronske pošte

Prijava treba da sadrži i podatke o odgovornom licu u posebnom CERT-u:

- Ime i prezime
- Funkcija
- Broj službenog telefona
- Službena adresa elektronske pošte

24 Pravilnik o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbedonosnih rizika u infromaciono-komunikacionim sistemima http://www.ratel.rs/upload/documents/Novosti/Pravilnik%20o%20blizim%20uslovima%20za%20upis%20u%20evidenciju%20posebnih%20CERT-ova.pdf

Uz registracionu prijavu se mora dostaviti i dokaz o obavljanju poslova prevencije i zaštite od bezbednosnih rizika u IKT sistemima. Podnosiocu se ostavlja sloboda da odluči na koji način će dokazivati da obavlja ove poslove, pa tako može podneti izvod iz statuta ili normativnog akta podnosioca koji uređuje i opisuje obavljanje poslova posebnog CERT-a, izvod iz sistematizacije radnih mesta ili ugovora o radu kojima je za određene zaposlene uvtrđeno obavljanje pomenutih poslova, neki drugi akt pravnog lica ili bilo koja druga dokumentacija kojom podnosilac dokazuje da se bavi obavljanjem ovih poslova.

Prijava se može podneti u pisanom obliku, neposredno u prostorijama Nacionalnog CERT-a ili poštom, a moguće je podneti je i elektronskim putem na internet strani Nacionalnog CERT-a. Ipak, u slučaju da se prijava podnosi elektronskim putem neophodno je u roku od pet dana podneti papirnu dokumentaciju, tj. obrazac i dokaze, osim ukoliko je prilikom podnošenja elektronskim putem ova dokumentacija bila potpisana kvalifikovanim elektronskim potpisom ovlašćenog lica.

Na osnovu podnete prijave i u slučaju da su ispunjeni uslovi propisani Zakonom i Pravilnikom, Nacionalni CERT donosi rešenje kojim se uvrđuje ispunjenost ovih uslova i posebni CERT se formano upisuje u Evidenciju posebnih CERT-ova.

SHARE FOUNDATION - 2017