ZAŠTITITE SVOJU FIRMU I ZAPOSLENE

UPUTSTVO ZA PRIJAVU INCIDENTA

PRIJAVITE SVAKI INCIDENT
NA NAŠEM PORTALU

SRB-CERT

UPUTSTVO ZA PRIJAVU INCIDENTA

Incident je svaki događaj koji ima stvaran negativan uticaj na bezbednost mrežnih i informacionih sistema. Svi operatori IKT sistema od posebnog značaja odgovaraju za bezbednost IKT sistema i dužni su da u tom cilju primenjuju mere zaštite propisane Zakonom o informacionoj bezbednosti.

U cilju ostvarivanja strateškog cilja Vlade Republike Srbije- razvoja i unapređenja informacione u Republici Srbiji, Nacionalni CERT vrši prevenciju i zaštitu od rizika putem razmene informacija, praćenja aktuelnih rizika i podizanja svesti građana, privrednih subjekata i organa vlasti o značaju informacione bezbednosti.

Prijavljivanje incidenata koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti predviđena je Zakonom o informacionoj bezbednosti, te je operatorima IKT sistema od posebnog značaja propisana obaveza prijavljivanja incidenata. Imajući u vidu da je informaciona bezbednost sastavni deo sveukupne bezbednosti, i da je njeno očuvanje u funkciji ostvarivanja i poštovanja prava, sloboda i interesa građana, privrede i države svi društveni činioci treba da budu svesni rizika povezanih sa upotrebom tehnologije. Ta svest se, između ostalog, ogleda i u efikasnoj reakciji na incidente, odnosno njihovom prijavljivanju nadležnom organu.

IKT sistemi od posebnog značaja su sistemi koji se koriste u obavljanju poslova u organima javne vlasti, za obradu podataka o ličnosti, u obavljanju delatnosti od opšteg interesa u oblastima proizvodnje i distribucije električne energije, proizvodnja i prerada uglja, istraživanje, proizvodnja, prerada transport i distribucija nafte i tečnog gasa, promet nafte i naftnih derivata, železničkog, poštanskog i vazdušnog saobraćaja, zdravstvena zaštita, vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama, upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta, razmene internet saobraćaja, upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži, upravljanje, zaštita i unapređenje dobara od opšteg interesa, kao što su vode, putevi, mineralne sirovine, šume, plovne reke,jezera, obale, banje, divljač, zaštićena područja, usluge informacionog društva, elektronska komunikacija, izdavanje službenog glasila RS, upravljanje nuklearnim objektima, korišćenje, proizvodnja, promet i prevoz naoružanja i vojne opreme, upravljanje otpadom, komunalne delatnosti, poslovi finansijskih institucija, usluge informacionog društva namenjene drugim pružaocima usluga informacionog društva u cilju omogućavanja pružanja njihovih usluga.

Dakle, IKT sistemi od posebnog značaja su sistemi, mreže, objekti ili njihovi delovi, čiji prekid funkcionisanja ili prekid isporuke roba odnosno usluga može imati ozbiljne posledice na nacionalnu bezbednost, zdravlje i živote ljudi, imovinu, životnu sredinu, bezbednost građana, ekonomsku stabilnost, odnosno ugroziti funkcionisanje Republike Srbije.

Operatori IKT sistema od posebnog značaja su obavezni da o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti dostave obaveštenja o incidentima:

1) koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga;

2) koji utiču na veliki broj korisnika usluga;

3) koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanja usluga, koji utiču na obavljanje poslova i vršenje usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost;

4) koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;

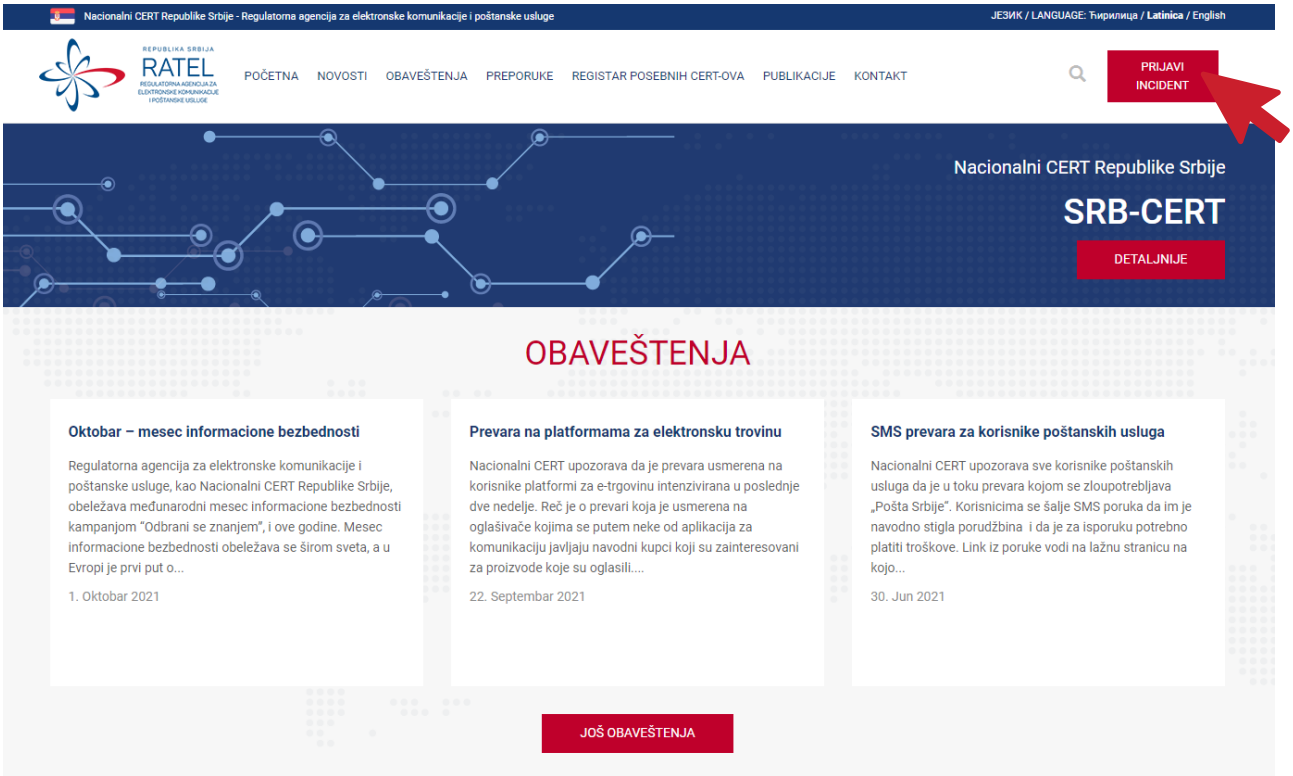
5) koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnos;

6) koji su nastali kao posledica incidenta u IKT sistemu koji se koristi u pružanju usluga informacionog društva, kada IKT sistem od posebnog značaja koristi informacione usluge IKT sistema koji pruža usluge informacionog društva.

Prijava incidenata vrši se putem imejla na info@cert.rs kao i preko veb sajta www.cert.rs klikom na polje „Prijavi incident“ i tom prilikom unose se podaci lica koje prijavljuje incident, kao i podaci o incidentu, odnosno atributi neophodni za dalju analizu, tip i opis incidenta.

U slučaju da ne postoji mogućnost prijave incidenta putem interneta, isti se može prijaviti i pozivom na broj telefona 062/20-20-30.

Incident je moguće prijaviti u bilo koje vreme tokom 24 sata svim danima u nedelji.



Na sve mejlove primljene preko portala ili imejla odgovora se automatski. Odgovor sadrži link preko koga je potrebno izvršiti verifikaciju prijave, i na taj način potvrditi prijavu incidenta. Nakon verifikacije prijave, licu koje je prijavilo incident dostavlja se potvrda sa identifikacionim brojem i porukom da je prijava incidenta evidentirana.

Operatori IKT sistema od posebnog značaja su u obavezi da ove incidente prijave bez odlaganja, a najkasnije narednog radnog dana od dana saznanja o nastanku incidenta. Preporuka Nacionalnog CERT-a je prijavljivanje u sledećom rokovima:

Opis incidenta	Rok za prijavu
Incidenti koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanja usluga	Prvi naredni radni dan
Incidenti koji utiču na veliki broj korisnika usluga ili traju duži vremenski period	Prvi naredni radni dan
Incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga, koji utiču na obavljanje poslova i pružanje usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost	Isti dan
Incidenti koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije	Isti dan
Incidenti koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose	Isti dan
Incidenti koji su nastali kao posledica incidenta u IKT sistemu koji se koristi u pružanju usluga informacionog društva, kada IKT sistem od posebnog značaja koristi informacione usluge IKT sistema koji pruža usluge informacionog društva	Prvi naredni dan

Osnovni tipovi incidenata propisani su Uredbom o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja [1]:

LISTA INCIDENATA PREMA VRSTAMA		
Grupa incidenata	Vrsta incidenta	Opis incidenta
Instaliranje zlonamernog softvera u okviru IKT sistema (malver, engl. „malware")	Virus	Računarski virus je deo zlonamernog kompjuterskog kôda čiji je cilj da se širi sa računara na računar tako što napada izvršne datoteke i dokumenta i može prouzrokovati namensko brisanje datoteka sa hard diska i sličnu štetu.
	Crv (engl. „worm")	Računarski crv je program koji sadrži zlonamerni kôd koji se širi preko mreže, tako što se samostalno umnožava i prenosi, odnosno ne zavisi od datoteka hosta. Crvi se šire na adrese elektronske pošte sa liste kontakta žrtve ili iskorišćavaju ranjivosti mrežnih aplikacija i zbog velike brzine širenja služe za prenos ostalih tipova zlonamernog softvera.
	Ransomver (engl. „ransomware")	Ransomver je tip malvera, odnosno zlonamerni softver koji šifrira informacije na uređajima ili mrežama, a za pristup i otključavanje datoteka zahteva plaćanje otkupa. Čest je slučaj da datoteke čak i nakon plaćanja otkupa ostaju zaključane.
	Trojanac	Računarski trojanci (trojanski konji) su pretnja koja pokušava da se predstavi korisnicima kao da su korisni programi i na taj način ih prevari da ih pokrenu. Ovi programi mogu da preuzmu druge pretnje sa interneta, ubacuju druge tipove malvera na ugrožene računare, komuniciraju sa udaljenim napadačima, i beleže sve što se kuca na tastaturi i šalju napadačima.
	Špijunski softver (engl. „spyware")	Špijunski softver delimično presreće ili preuzima kontrolu nad računarom bez znanja ili dozvole korisnika. Sam naziv sugeriše da je reč o programima koji nadgledaju rad korisnika tako što snimaju i preuzimaju informacije sa računara poput navika pretraživanja veba, elektronske pošte, kredencijala i sl. i te podatke prenose napadaču.

[1] Uredbom o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja („Službeni glasnik RS", broj 11/20)

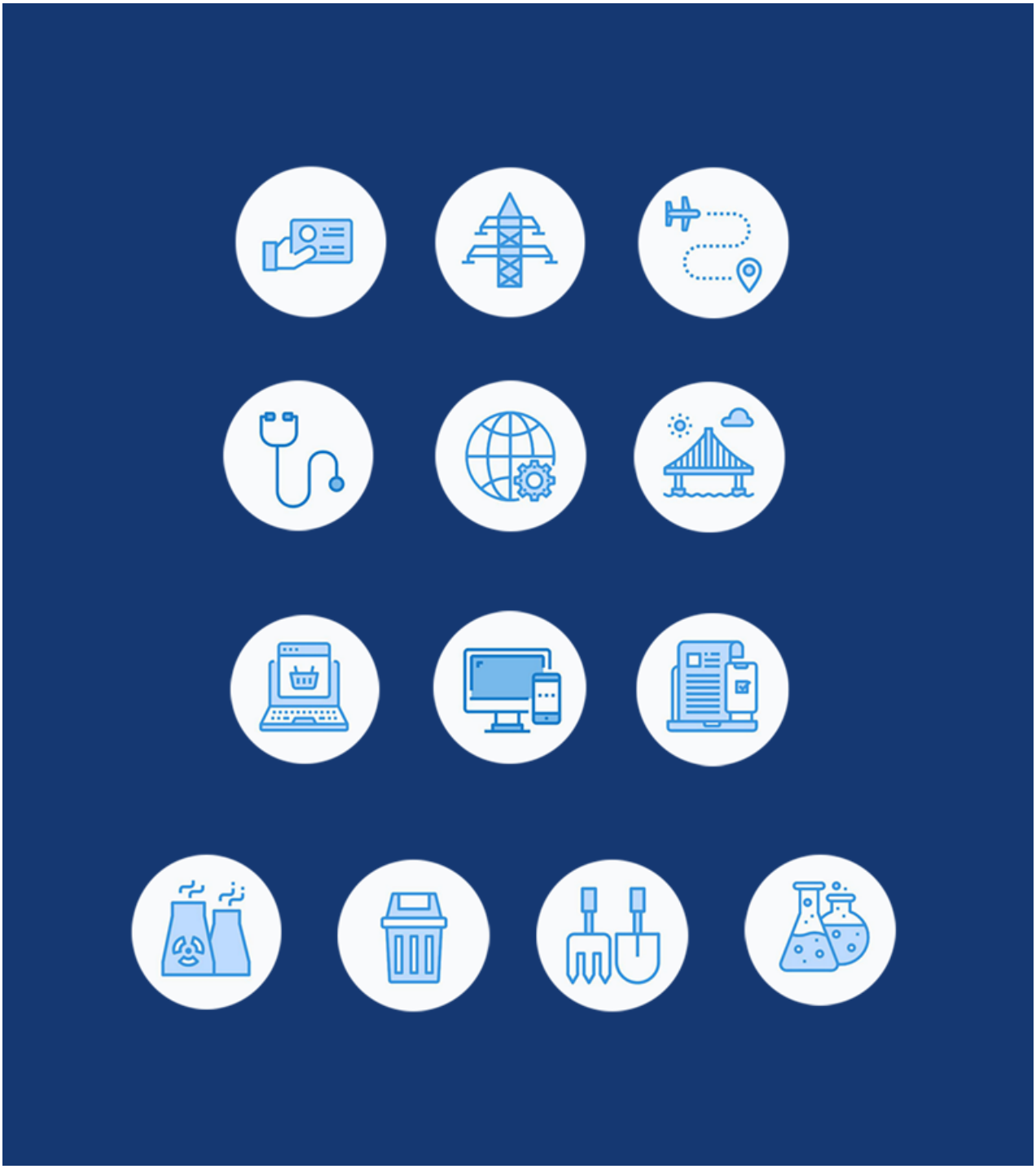
LISTA INCIDENATA PREMA VRSTAMA		
Grupa incidenata	Vrsta incidenta	Opis incidenta
	Rutkit (engl. „rootkit")	Rutkit je softver koji omogućava privilegovan daljinski pristup računaru, krijući svoje prisustvo od administratora sistema. Omogućava napadaču da se sakrije u toku neovlašćenog pristupa i održava privilegovan pristup računaru zaobilaženjem uobičajenog načina autentifikacije i mehanizama autorizacije.
Neovlašćeno prikupljanje podataka	Skeniranje portova	Skeniranje portova je napad koji šalje zahteve klijenata na niz adresa portova servera hosta, sa ciljem otkrivanja komunikacionih kanala koji se mogu iskoristiti, odnosno pronalaska otvorenog porta i iskorišćavanja njegove ranjivosti.
	Presretanje podataka između računara i servera (engl. „sniffing")	Snifer napad podrazumeva korišćenje aplikacija za nadgledanje i analizu mrežnog saobraćaja u cilju preuzimanja mrežnih paketa. Na ovaj način napadač analizira mrežu i pribavlja informacije kojim je može kompromitovati.
	Socijalni inženjering (lažno predstavljanje i drugi oblici)	Napadi socijalnog inženjeringa obično koriste ljudsku psihologiju i podložnost manipulacijama kako bi naveli žrtve na otkrivanje osetljivih podataka ili kršenje bezbednosnih mera koje će omogućiti napadaču pristup mreži.
	Kompromitovanje ili curenje podataka (engl. „data breaches")	Povreda podataka podrazumeva uspešan zlonameran pokušaj koji je doveo do izmene ili gubitka podataka.
Prevara	Fišing (engl. „phishing")	Fišing je sajber napad koji se vrši uz pomoć elektronske pošte, koja sadrži zlonamerni prilog ili link koji vodi ka zaraženom sajtu ili dokumentu. Napadač koristi socijalni inženjering da bi se predstavio kao neko poznat i tako naveo žrtvu da otvori elektronsku poštu. Ovaj napad je često povezan i sa napadima poput malvera, mreže botova i sajber špijunaže.

LISTA INCIDENATA PREMA VRSTAMA		
Grupa incidenata	Vrsta incidenta	Opis incidenta
	Neovlašćeno korišćenje resursa (engl. „cryptojacking " i drugi oblici)	Kriptodžeking (poznat i kao kriptomajning) odnosno „otimanje" je novi termin koji se odnosi na programe koji koriste snagu centralne procesorske jedinice (70% do 80% neiskorišćene snage procesora) bez pristanka žrtve, da bi „rudarili" kripto valute za sticanje lične koristi
	Pokušaj iskorišćavanja ranjivosti sistema	Pokušaj iskorišćavanja ranjivosti sistema je napad na računarski sistem, kojim napadač koristi određenu ranjivost sistema. Ovaj napad koristi ranjivost operativnog sistema, aplikacije ili bilo kojeg drugog softverskog koda, uključujući dodatke aplikacija ili biblioteke softvera.
Pokušaji upada u IKT sistem	Pokušaj otkrivanja kredencijala (engl. „brute force attack", „dictionary attack" i sl.)	Brute Force napad podrazumeva pokušaj pristupa sistemu žrtve neprekidnim logovanjem različitim kombinacijama slova, brojeva i simbola sa ciljem identifikacije korisničkog imena i lozinke.
Upad u IKT sistem	Otkrivanje ili neovlašćeno korišćenje privilegovanih naloga (engl. „privileged account	Korišćenje privilegovanih naloga omogućava napadačima da se neprimećeno kreću kroz IKT sistem ili mrežu i pristupe osetljivim podacima.
	Otkrivanje ili neovlašćeno korišćenje neprivilegovanih naloga (engl. „unprivileged account compromise")	Korišćenje neprivilegovanih naloga omogućava napadačima da se neprimećeno kreću kroz ograničeni deo IKT sistema ili mreže, sa mogućnošću dalje kompromitacije IKT sistema ili mreže i pristupanja osetljivim podacima.
	Neovlašćeni pristup aplikaciji	Neovlašćeni pristup aplikaciji je pristup veb lokaciji, programu, serveru, servisu ili drugom sistemu pomoću tuđeg naloga ili drugih metoda.

LISTA INCIDENATA PREMA VRSTAMA		
Grupa incidenata	Vrsta incidenta	Opis incidenta
	Mreža zaraženih uređaja (engl. „botnet“)	Mreža botova je automatizovani napad koji je skenira mrežne adrese i širi zaraze na ranjivim računarima, što omogućava hakerima da preuzmu kontrolu nad zaraženim računarima i pretvore ih u botove. Na taj način se stvara mreža botova koja se koristi za napade onemogućavanja usluga (DDoS), kao i za izvršavanje zadataka bez znanja žrtve (slanje elektronske pošte, virusa ili krađe ličnih podataka).
Nedostupnost ili ograničena dostupnost IKT sistema	Napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. „denial -of -service attack” – DoS)	DoS napad je pokušaj napadača da onemogući pristup serveru ili servisima koji su namenjeni krajnjim korisnicima.
	Distribuirani napad sa ciljem onemogućavanja ili ometanja funkcionisanja IKT sistema (engl. „distributed denial-of-service attack” – DDoS)	DDoS je višestruki napad koji ima za cilj da se poremeti normalan saobraćaj servera, usluge ili mreže preplavljujući infrastrukturu većom količinom internet saobraćaja. DDoS napadi postižu efikasnost koristeći više kompromitovanih računarskih sistema kao izvora saobraćaja.
	Sabotaža	Sabotaža kao napad se koristiti u svrhu sabotiranja sistema ili mreže i nanošenja štete. Mogući su različiti oblici sabotaže u zavisnosti od oblasti poslovanja napadnute infrastrukture.
	Prekid u funkcionisanju sistema ili dela sistema (engl. „outage”)	Prekid rada sistema prouzrokovan prekidom u isporuci električne energije, zbog loših vremenskih uslova ili hardverske greške koja je nastala kao posledica neispravne opreme.
Ugrožavanje bezbednosti podataka	Neovlašćen pristup podacima	Neovlašćeni pristup podacima je napad pomoću kog se kršenjem mera zaštite pristupa podacima sistema ili mreže u cilju njihove zloupotrebe.

LISTA INCIDENATA PREMA VRSTAMA		
Grupa incidenata	Vrsta incidenta	Opis incidenta
	Neovlašćena izmena ili brisanje podataka	Neovlašćena izmena podataka je napad pomoću kog se kršenjem mera zaštite pristupa podacima sistema ili mreže i vrši njihova izmena, a u cilju njihove zloupotrebe.
	Kriptografski napad	Kriptografski napad je metod zaobilaženja mera zaštite kriptografskog sistema pronalaženjem slabosti u kodu, šifri, algoritmu, kriptografskom protokolu ili šemi upravljanja ključevima. Ovaj proces se takođe naziva „kriptoanaliza“.
Operativni incidenti	Otkazivanje hardverskih komponenti	Otkazivanje hardverskih komponenti se odnosi na zastoj u radu koji se dogodio zbog otkazivanja hardverskih komponenti. Ukoliko je problem bilo jednostavno rešiti, ali je ometao redovan proces rada i doveo do pomeranja rokova izvršavanja radnih zadataka, odnosno onemogućavanja pružanja usluga, smatra se da se dogodio incident.
	Problemi u radu sa softverskim komponentama	Problemi u radu sa softverskim komponentama se odnose na sve one probleme koji su doveli do zastoja u radu i poslovnom procesu, koji zahtevaju angažovanje lica za rukovanje tim komponentama, nove instalacije, kao i nove nabavke. Problemi koji se rešavaju restartovanjem programa koje traje toliko da ne izaziva pomeranje rokova ili nemogućnost pružanja usluga na uobičajen način, može se izostaviti iz broja incidenta.
Incidenti fizičko-tehničke bezbednosti	Krađa hardverskih komponenti	Svi incidenti koji su nastali kao posledica krađe hardverskih komponenti koje su sastavni deo IKT sistema.
	Požar	Svi incidenti koji su nastali kao posledica požara u IKT sistemu.
	Poplava	Svi incidenti koji su nastali kao posledica poplave u IKT sistemu.
Ostali incidenti	Incidenti koji ne spadaju u gore navedene kategorije	

Zahvaljujući ostvarenoj međunarodnoj saradnji sa drugim nacionalnim CERT-ovima, kao i članstvu u međunarodnim organizacijama Nacionalni CERT je pouzdani koordinator informacija o incidentima i posebno ukazuje na značaj prijavljivanja incidenata.



REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

SRB-CERT