V súčasnosti sa informácie v čoraz väčšej miere spracovávajú v elektronickej forme pomocou počítačov a iných informačných a komunikačných technológií. Potenciálna možnosť narušenia týchto informácií, či už priamo alebo prostredníctvom útoku na technické zariadenie alebo prostredie, v ktorom sa informácia spracováva, sa nazýva hrozba. Existuje množstvo činiteľov, ktoré môžu ohroziť alebo spôsobiť znefunkčnenie informačných a komunikačných technológií a znehodnotenie informácií, ktoré sú v nich spracovávané. Sú to napríklad prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus, ktoré by mohli spôsobiť vážne bezpečnostné problémy.

Cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru Slovenskej republiky.

Informačná bezpečnosť

musí zohľadňovať záujmy vlastníkov a potreby používateľov informačných a komunikačných technológií, ako aj práva fyzických osôb a právnických osôb, ktorých údaje sa v systémoch spracovávajú. Z hľadiska používateľov sú pri spracovaní informácie najdôležitejšie faktory, a to účel a obsah informácií, presnosť, aktuálnosť, prístupnosť, autenticita, usporiadanie a kvalita informácií. Z hľadiska vlastníkov a prevádzkovateľov je najdôležitejšia dostupnosť informačných zdrojov, podľa možnosti s prístupom on-line, a ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému.

Nezabezpečenie informácií môže mať za následok nenahraditeľné straty a narušenie dôveryhodnosti organizácie a štátu. Vzhľadom na to, že štát je garantom kritických procesov, má úlohu starať sa o celkovú úroveň konkurencieschopnosti spoločnosti, a tým chrániť národné bohatstvo, ktorého súčasťou sú aj znalosti a informácie, a preto si nemôže dovoliť mať nízke kritériá úrovne bezpečnosti.

Computer Security Incident Response Team Slovakia – CSIRT.SK bol zriadený ako špecializovaný útvar DataCentra (rozpočtovej organizácie Ministerstva financií SR) s cieľom zabezpečiť primeranú úroveň ochrany národnej informačnej a komunikačnej infraštruktúry - NIKI, kritickej informačnej infraštruktúry a jej technologických prvkov.

CSIRT.SK

zabezpečuje služby spojené so zvládnutím bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci NIKI v spolupráci s vlastníkmi a prevádzkovateľmi NIKI, telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a prípadne inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy), podieľa sa na budovaní a rozširovaní poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti, aktívne kooperuje so zahraničnými organizáciami a reprezentuje SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni.

Služby

pre klientov definované uznesením vlády č. 479/2009:

Aktívne služby:

- varovania / upozornenia na bezpečnostné riziká,
- reakcia na incidenty,
- analýza incidentov,
- tvorba manuálov pre riešenie najčastejšie sa vyskytujúcich incidentov,
- koordinácia činností pri reakcií na incidenty,
- analýza bezpečnostných rizík a zraniteľností,
- reakcia na škodlivý softvér,
- analýza škodlivého softvéru.

Proaktívne služby:

- oznámenia,
- technologický dozor,
- vzdelávanie a budovanie všeobecného povedomia v oblasti informačnej bezpečnosti,
- konfigurácia a údržba bezpečnostných nástrojov, aplikácií a infraštruktúry,
- služby detekcie prienikov,
- distribúcia informácií týkajúcich sa bezpečnosti,
- monitorovanie stavu hrozieb v oblasti IKT,
- konzultačná činnosť v oblasti informačnej bezpečnosti.

Komunikačné kanály:

e-mail: incident@csirt.gov.sk a info@csirt.gov.sk (s možnosťou šifrovania),
telefonický kontakt publikovaný na http://www.csirt.gov.sk/kontakty-7db.html,
elektronické formuláre na webovom sídle pre:
hlásenie incidentu: http://www.csirt.gov.sk/formular-na-zadanie-incidentu-7ed.html
hlásenie zraniteľnosti: http://www.csirt.gov.sk/formular-na-zadanie-incidentu-7ee.html
webové sídlo www.csirt.gov.sk s privátnou sekciou pre registrovaných používateľov,
mailing list a RSS vybraných sekcií web stránky http://www.csirt.gov.sk/aktualne/mailing-list-822.html,
sekcia web stránky s údajmi pre registrovaných používateľov (https),
tiketovací systém RTIR (prepojený na nahlasovacie on-line formuláre).

V súčasnosti je pripravené

poskytovanie služieb

pre vlastníkov a správcov informačných systémov inštitúcií verejnej správy najmä v oblastiach:

- konzultácie a súčinnosť pri riešení počítačových incidentov,
- konzultácie pri tvorbe a udržiavaní systému riadenia informačnej bezpečnosti alebo vybraných častí bezpečnostnej dokumentácie podľa ISO 2700x,
- analýza zraniteľností webového sídla a návrh opatrení,
- forenzná analýza desktopových staníc (Windows, Linux), obnova dát po incidente,
- informovanie o nových zraniteľnostiach pre vybrané hardvérové a softvérové platformy,
- zabezpečenie školení a seminárov na požadované témy z oblasti informačnej bezpečnosti,
- asistencia a zaškolenie pri budovaní vlastných tímov pre riešenie počítačových incidentov.

Školenia

poskytované špecializovaným útvarom CSIRT.SK:

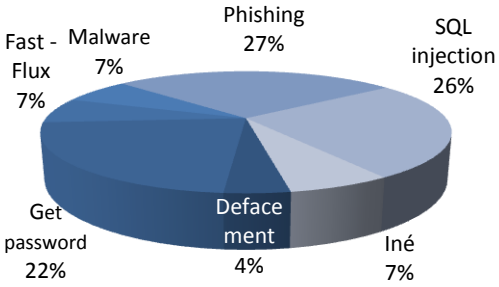
- Tvorba a prevádzka CSIRT/CERT tímov:
  - Tvorba CSIRT/CERT tímov, organizačné zabezpečenie, procesy CSIRT/CERT tímov.
  - Operačné zabezpečenie CSIRT/CERT tímov (nástroje, postupy, procesy).
  - Varovania a vydávanie varovaní .
  - Správa incidentov, riešenie incidentov, manažment zraniteľností a prevencia.
  - Vzdelávanie špecialistov CSIRT/CERT tímov.
- Princípy bezpečnostných slabín a ich prevencia
- Forenzná analýza – princípy a prostriedky
- Forenzná analýza
  - Forenzná analýza – pracovné stanice (Windows/Linux)
  - Forenzná analýza – servery (Linux/Unix/Windows)
  - Sieťová forenzná analýza – netflow a event based.
- ENISA cvičenia – návrh a realizácia
- Business continuity manažment a súvis s CSIRT/CERT

Uvedené školenia môže CSIRT.SK poskytovať na základe absolvovania školení TRANSIT training organizovaných inštitúciou TERENA.

V prípade záujmu vieme zabezpečiť aj ďalšie témy školení.

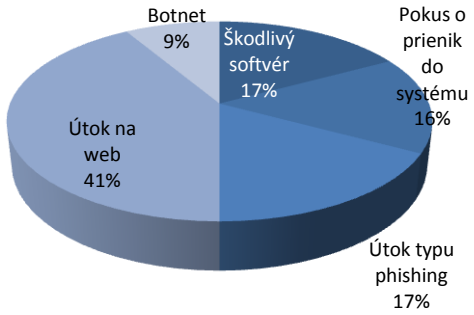
Počet a zastúpenie typov závažných incidentov riešených CSIRT.SK v období 1.1.2012 - 31.12.2012

Defacement	5
Get password	27
Fast - Flux	8
Malware	8
Phishing	33
SQL injection	31
Iné	8
Incidenty spolu	**120**



Počet a zastúpenie typov závažných incidentov riešených CSIRT.SK v období 1.1.2011 - 31.12.2011

Škodlivý softvér	12
Pokus o prienik do systému	11
Útok typu phishing	12
Útok na web	29
Botnet	6
Incidenty spolu	**70**



CSIRT.SK funguje ako národný **kontaktný bod** pre nahlasovanie bezpečnostných počítačových incidentov v SR.

V máji 2011 bol CSIRT.SK plne akreditovaný združením **TF-CSIRT** a stal sa tak ako jediný v SR plnohodnotným členom komunity európskych tímov CSIRT/CERT. Aktívne spolupracuje so zahraničnými tímami CSIRT/CERT Rakúska, Maďarska, Českej republiky, Poľska a ďalších krajín v oblasti prijímania hlásení o incidentoch zo zahraničia, zdieľanie informácií, skúseností a overených postupov (best practices) pri ich riešení.

Útvar CSIRT.SK sa taktiež zaslúžil o aktívnu podporu SR zo strany Európskej agentúry pre bezpečnosť sietí a informácií – ENISA. Pri plnení úloh Akčného plánu k dokumentu Národná stratégia pre informačnú bezpečnosť v SR sa špecializovaný útvar CSIRT.SK, ako národný koordinátor, zúčastnil medzinárodných **cvičení** riešenia rozsiahlych počítačových incidentov CyberEurope 2010 a na spoločnom EÚ – USA cvičení Cyber Atlantic 2011 zameraných na preverenie pripravenosti a budovanie medzinárodnej spolupráce v oblasti ochrany kritickej informačnej infraštruktúry.

CSIRT.SK v spolupráci s MF SR pripravil a realizoval národné cvičenia na ochranu kritickej informačnej infraštruktúry Slovak Information Security Exercise 2011 – SISE 2011 a **SISE 2012**. Do cvičení, ktoré sa konali v novembri 2011 a 2012 sa aktívne zapojilo viacero inštitúcií štátnej správy ako aj zahraničné jednotky typu CSIRT/CERT. Primárnym cieľom cvičení SISE bolo preveriť schopnosť zúčastnených inštitúcií reagovať na rozsiahle počítačové incidenty v prostredí IKT a s tým súvisiacich aktivít akými sú preverenie efektívnosti medzirezortnej komunikácie, funkčnosti interných procesov a postupov, havarijných plánov, plánov obnovy činnosti po rozsiahlom incidente a pod.

CSIRT.SK
DATACENTRUM
CINTORÍNSKA 5
814 88 BRATISLAVA
INCIDENT@CSIRT.GOV.SK
INFO@CSIRT.GOV.SK
02 / 59278 454
02 / 59278 514
02 / 52926 870 (FAX)
WWW. CSIRT.GOV.SK

CSIRT.SK PGP KEY FINGERPRINT:
DFB9 E47B 4304 CB18 AF97
E49D EC51 77D3 E4E1 1CE2

CSIRT.SK
www.csirt.gov.sk

ibrožúra