Organizačný poriadok

Centra pre riešenie kybernetických bezpečnostných incidentov

Fakulty elektrotechniky a informatiky
Slovenskej technickej univerzity v Bratislave

Dátum: 03.02.2025

Organizačný poriadok Centra pre riešenie kybernetických bezpečnostných incidentov

Článok 1
Úvodné ustanovenia

1. Tento organizačný poriadok upravuje obsah a rozsah činností, spôsob riadenia a organizačné usporiadanie Akademického Centra pre riešenie kybernetických bezpečnostných incidentov (ďalej len „CSIRT Centrum“) v súlade so Štatútom Fakulty elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave (ďalej len „Štatút FEI STU“) a Organizačným poriadkom Fakulty elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave (ďalej len „Organizačný poriadok FEI STU“). Skrátený názov centra je CSIRT FEI.
2. Anglický názov centra je Cyber Security Incident Response Center. Skrátený anglický názov centra je CSIRT FEI.

Článok 2
Postavenie CSIRT Centra a jeho riadenie

1. CSIRT Centrum je špeciálne účelové zariadenie Fakulty elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave (ďalej len „FEI STU“), ktoré realizuje odborné činnosti, súvisiace s reakciou na bezpečnostné incidenty namierené na Informačné technológie FEI STU.
2. Hlavnou úlohou CSIRT Centra je zabezpečenie služieb spojených so zvládaním bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci FEI STU.
3. CSIRT Centrum poskytuje služby preventívneho a vzdelávacieho charakteru. Zároveň poskytne aj cenné poznatky a dáta nevyhnutné pre realizáciu výskumu v oblasti IT a kybernetickej bezpečnosti.
4. Predstaviteľom CSIRT Centra je riaditeľ, ktorý centrum riadi a koná v jeho mene. Riaditeľ CSIRT Centra nie je vedúcim zamestnancom FEI STU, vymenúva a odvoláva ho dekan. Za svoju činnosť riaditeľ zodpovedá dekanovi v zmysle čl. 8 ods. 3 Organizačného poriadku FEI STU. Anglickým prekladom funkcie „riaditeľ“ je „director".
5. V čase neprítomnosti riaditeľa CSIRT Centra na pracovisku ho zastupuje zástupca riaditeľa. Zástupca riaditeľa môže zastupovať riaditeľa aj na dlhšie obdobie, a to v presne vymedzených činnostiach a na presne definované obdobie. Vymedzené činnosti a rozsah právomocí zástupcu riaditeľa musia byť uvedené v menovacom dekréte na funkciu zástupcu riaditeľa. Zástupcu riaditeľa vymenúva a odvoláva dekan na základe návrhu riaditeľa CSIRT Centra. Dekan môže návrh riaditeľa na vymenovanie a odvolanie zástupcu riaditeľa zamietnuť. Zástupca riaditeľa nie je vedúcim zamestnancom FEI STU. Počas neprítomnosti riaditeľa CSIRT Centra je zástupca riaditeľa oprávnený konať v jeho mene s výnimkou rozhodovania v oblasti pracovnoprávnych vzťahov a mzdových záležitostí. Anglickým prekladom funkcie „zástupca riaditeľa“ je „deputy director“.

Článok 3
Základné úlohy CSIRT Centra

1. CSIRT Centrum bude podporovať správcov IT systémov v rámci FEI STU v rámci svojho sektoru pôsobnosti.
2. CSIRT Centrum bude informovať, vo svojom sektore pôsobnosti, o potenciálnych zraniteľných miestach a tam, kde je to možné, bude informovať o takýchto zraniteľnostiach skôr, ako budú aktívne zneužité.
3. CSIRT Centrum bude spolupracovať s ďalšími organizáciami v oblasti počítačovej bezpečnosti. Táto spolupráca tiež zahŕňa a často vyžaduje výmenu vysoko dôležitých informácií týkajúcich sa bezpečnostných incidentov a zraniteľných miest.
4. CSIRT Centrum bude pôsobiť v rámci obmedzení uložených slovenským právom a právom EÚ. Ide o starostlivé zaobchádzanie s osobnými údajmi v zmysle všeobecného nariadenia o ochrane údajov a o zaobchádzanie s incidentmi v zmysle platnej legislatívy SR.

5. CSIRT Centrum bude propagovať osvedčené postupy súvisiace s bezpečnosťou a ochranou proti kybernetickým útokom.
6. CSIRT Centrum bude prispievať ku zvyšovaniu bezpečnostného povedomia a procesu vzdelávania zamestnancov STU v oblasti kybernetickej bezpečnosti.
7. CSIRT Centrum bude v spolupráci s ďalšími výskumnými centrami v oblasti kybernetickej bezpečnosti, ktoré realizujú iné CSIRT centrá alebo univerzity, realizovať vedecký výskum v oblastiach kybernetickej bezpečnosti.

Článok 4
Organizácia CSIRT Centra

1. CSIRT Centrum sa vnútorne člení na:
   a) v prípade potreby viacero oddelení, ktoré zabezpečujú aktivity podľa článku 3 tohto organizačného poriadku,
   b) administratívno-hospodársky útvar, ktorý zabezpečuje administratívnu, organizačnú, informačnú a hospodársku činnosť.
2. Oddelenia zriaďuje alebo ruší riaditeľ CSIRT Centra so súhlasom dekana. Pri zriadení oddelenia riaditeľ určí jeho slovenský a anglický názov; anglickým prekladom „oddelenie“ je „department“.
3. Ak CSIRT Centrum obsahuje viacero oddelení, ich zoznam tvorí prílohu tohto organizačného poriadku.
4. Oddelenia sú vedené vedúcimi oddelenia. Anglickým prekladom funkcie vedúci oddelenia je „department chair“. Vedúcich oddelení vymenúva a odvoláva dekan na návrh riaditeľa centra. Vedúci oddelenia vedie oddelenie v rozsahu vymedzenom riaditeľom centra a nie je vedúcim zamestnancom FEI STU.
5. Administratívno-hospodársky útvar je riadený riaditeľom CSIRT Centra. Administratívno-hospodársky útvar zabezpečuje organizačnú a hospodársku činnosť CSIRT Centra. Administratívno-hospodársky útvar centra je metodicky riadený tajomníkom FEI STU.
6. Riaditeľ zodpovedá za zabezpečenie dosahovania odbornej úrovne v oblasti spolupráce, dohliada na odbornú stránku realizácie úloh, ich kvality a časového harmonogramu, navrhuje ďalšie ciele, rozvoj a smerovanie a plánuje činnosti v súlade so stanovenými cieľmi.
7. Riaditeľ ďalej zodpovedá za administratívne záležitosti CSIRT Centra, personálne otázky, hospodárenie a reprezentáciu centra a podporu a rozvoj ďalšej externej spolupráce v témach centra.
8. Riaditeľ CSIRT Centra je priamo podriadený dekanovi FEI STU a pri výkone svojej činnosti sa riadi jeho pokynmi. Riaditeľ pri výkone svojej činnosti musí zohľadňovať aj odporúčania osoby zodpovednej za plnenie Memoranda o spolupráci uzatvoreného s Kompetenčným a certifikačným centrom kybernetickej bezpečnosti NBÚ za FEI STU.
9. Riaditeľ ako riadiaci pracovník CSIRT Centra zodpovedá za zabezpečenie schopnosti poskytovať nasledovné služby:
   a) spolupráca s lokálnymi a medzinárodnými partnermi a organizáciami pri zastúpení FEI STU v oblasti informačnej bezpečnosti na národnej a medzinárodnej úrovni,
   b) zabezpečenie plnenia úloh vyplývajúcich z poslania CSIRT Centra,
   c) školiace činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti fakulty,
   d) príprava a školenie nových členov CSIRT Centra v špecializovanom laboratóriu CSIRT Centra.

Článok 5
Hospodárenie CSIRT Centra

1. CSIRT Centrum efektívne hospodári s pridelenými finančnými prostriedkami a majetkom STU, ktorý používa na svoju činnosť v súlade s vnútornými predpismi FEI STU a STU, najmä so Štatútom Slovenskej technickej univerzity v Bratislave a Organizačným poriadkom Slovenskej technickej univerzity v Bratislave, Štatútom FEI STU a Organizačným poriadkom FEI STU a v súlade so všeobecne platnými právnymi predpismi.

2. CSIRT Centrum môže vykonávať za úhradu doplnkové činnosti nadväzujúce na jeho vzdelávaciu, vedeckú, výskumnú alebo ďalšiu tvorivú činnosť alebo činnosť slúžiacu k účelnejšiemu využitiu ľudských zdrojov a majetku.

Článok 6
Členovia tímu CSIRT Centra

1. Úplný zoznam členov CSIRT Centra nie je verejne dostupný, ale zoznam bude uložený v kancelárii dekana FEI STU a každý mesiac bude zoznam aktualizovaný. Za úplný a správny zoznam zodpovedá riaditeľ CSIRT Centra. Členovia tímu dajú o sebe vedieť v konkrétnych situáciách, ako je hlásenie incidentov, reakcia, koordinácia, podpora.

Článok 7
Charta CSIRT Centra

1. Sektor zodpovednosti CSIRT Centra sú študenti, zamestnanci, spolupracovníci Fakulty elektrotechniky a informatiky STU v Bratislave a ďalšie inštitúcie zapojené do siete FEI STU. Predmetom monitorovania bude infraštruktúra a informačné systémy FEI STU, ktoré budú definované v prílohe, ktorá je neoddeliteľnou súčasťou tohto organizačného poriadku.
2. CSIRT Centrum zabezpečuje koordináciu a stanovuje postup riešenia bezpečnostných incidentov. Je oprávnené vykonávať:
   a) riešenie bezpečnostných incidentov a počiatočné opatrenia týkajúce sa bezpečnostných incidentov v kooperácii s VS FEI STU,
   b) navrhovať, a v príslušnej miere (v súlade s úlohami CSIRT Centra aplikovať bezpečnostné opatrenia na odstránenie incidentov, pokrytie identifikovaných rizík (ošetrenie rizika),
   c) monitorovanie a zber relevantných informácií o toku siete a procesoch v monitorovaných informačných systémoch, vytváranie, uchovávanie a analýza logov z koncových zariadení, informačných systémov a ich komponentov, serverov a sieťovej infraštruktúry, zber a analýza dodatočných dôkazov pri vyšetrovaní kybernetických incidentov,
   d) detekciu bezpečnostných zraniteľností súvisiacich s univerzitným prostredím,
   e) zvýšenie bezpečnosti sieťovej infraštruktúry, serverov a zariadení koncových používateľov,
   f) vyhľadávanie zraniteľných miest, pravidelne podávať správy o nových zraniteľnostiach dekanovi, riaditeľovi VS a poverenej osobe za IT na FEI STU raz za mesiac,
   g) monitorovanie informačných zdrojov o hrozbách relevantných pre FEI STU a STU,
   h) prevádzkovanie bezpečnostných a monitorovacích nástrojov v kooperácii s VS FEI STU.
3. Monitorovanie incidentov v sektore zodpovednosti CSIRT Centra bude minimálne v rozsahu:
   a) monitorovanie toku siete,
   b) analýza logov z koncových zariadení, informačných systémov, ako celkov alebo ich komponentov a sieťovej infraštruktúry,
   c) zber dát a informácií o incidentoch pre potreby ich analýzy a využitia pre výskum.
4. Detekcia a reakcia na incidenty v sektore zodpovednosti CSIRT Centra bude minimálne v rozsahu:
   a) počiatočné opatrenia týkajúce sa bezpečnostných incidentov,
   b) koordinácia reakcie na incidenty a riešenie incidentov,
   c) analýza a triedenie (klasifikovanie) incidentov.
5. CSIRT Centrum bude zabezpečovať aktivity potrebné pre zvýšenie bezpečnostného povedomia a pre minimalizáciu incidentov pomocou nasledovných činnosti:
   a) výber a nasadenie nástrojov na skenovanie a testovanie bezpečnosti softvérových a hardvérových komponentov prevádzkovaných v sieti FEI STU,
   b) príprava a vytvorenie bezpečnostných smerníc,
   c) propagácia osvedčených postupov súvisiacich s bezpečnosťou IT formou vzdelávacieho webového portálu, diskusií na mieste, workshopov a školení v oblasti kybernetickej bezpečnosti,

d) vyhľadávanie zraniteľných miest, pravidelné informovanie o nových zraniteľnostiach,
e) príprava bezpečnostnej dokumentácie fakulty vrátane analýzy rizík,
f) testovanie riešení navrhnutých výskumnými tímami a nasadenie overených vlastných nástrojov, ktoré vzniknú ako výsledok výskumných projektov.

6. CSIRT Centrum bude systematicky realizovať detekciu bezpečnostných zraniteľností súvisiacich s fakultným prostredím.
7. CSIRT Centrum bude pravidelne revidovať a realizovať zvyšovanie bezpečnosti sieťovej infraštruktúry, serverov a zariadení koncových používateľov.
8. CSIRT Centrum bude pravidelne revidovať a implementovať monitorovanie informačných zdrojov o hrozbách relevantných pre FEI STU.
9. Bezpečnostné a monitorovacie nástroje CSIRT Centra budú v prevádzke s vysokou dostupnosťou.
10. Členovia CSIRT Centra sa budú podieľať aj na príprave a výučbe kurzov súvisiacich s kybernetickou bezpečnosťou.

Článok 8
Zásady

1. CSIRT Centrum ako súčasť Fakulty elektrotechniky a informatiky STU v Bratislave musí dodržiavať vnútorné predpisy Slovenskej technickej univerzity v Bratislave, FEI STU a dodržiavať pravidlá používania siete SANET.
2. CSIRT Centrum tiež uznáva a používa najlepšie postupy formulované Európskou komunitou CSIRT (TF-CSIRT a Trusted Introducer) a ENISA, Agentúrou EÚ pre sieťovú a informačnú bezpečnosť, napríklad TI's CSIRT Code of Practice.
3. CSIRT Centrum sa týmto tiež zaväzuje, že jeho zamestnanci alebo členovia budú dodržiavať kódex správania a dodržiavať záväzky mlčanlivosti a rešpektovať príslušné legislatívne akty SR a EÚ.
4. CSIRT Centrum bude aktivity deklarované v článku 7, ktoré je oprávnený vykonávať v prostredí FEI STU vykonávať na základe upresňujúcich smerníc pre dané aktivity, kde budú zároveň upresnené podrobnosti a postupy pre vykonávanie danej aktivity, alebo súboru aktivít a tiež spôsob kooperácie s ostatnými organizačnými jednotkami FEI STU.

Článok 9
Typy incidentov a úroveň podpory

1. CSIRT Centrum je oprávnené riešiť všetky typy počítačových bezpečnostných incidentov, ktoré sa vyskytujú alebo hrozí, že sa vyskytnú v jeho sektore zodpovednosti (v zmysle čl. 7, odst.2.). Presná definícia typov incidentov, postupov a spôsobu kooperácie budú definované samostatnou smernicou pre postup riešenia počítačových incidentov pre CSIRT Centrum.
2. Úroveň podpory poskytovanej CSIRT Centrom sa bude líšiť v závislosti od typu a závažnosti incidentu alebo problému, typu zložky, veľkosti dotknutej používateľskej komunity a zdrojov CSIRT Centra v danom čase. Osobitná pozornosť sa bude venovať otázkam ovplyvňujúcim kritickú infraštruktúru.
3. Koncovým používateľom nebude poskytnutá priama podpora; očakáva sa, že požiadajú o pomoc svojho správcu systému a/alebo siete na organizačnej jednotke. CSIRT Centrum bude podporovať daných správcov systémov v spolupráci s VS FEI STU.
4. CSIRT Centrum sa zaväzuje informovať v rámci svojho sektora zodpovednosti o potenciálnych zraniteľných miestach a tam, kde to bude možné, bude o zraniteľnostiach informovať komunitu skôr, ako budú aktívne zneužité.

Článok 10
Spolupráca, interakcia a sprístupnenie informácií

1. CSIRT Centrum spolupracuje s ďalšími organizáciami v oblasti počítačovej bezpečnosti. Táto spolupráca tiež zahŕňa a často si vyžaduje výmenu dôležitých informácií týkajúcich sa bezpečnostných incidentov a slabých miest. V takýchto prípadoch CSIRT Centrum využíva protokol TLP (Information Sharing Traffic Light Protocol).
2. CSIRT Centrum pôsobí v rámci obmedzení uložených slovenským právom a právom EÚ. Ide o starostlivé zaobchádzanie s osobnými údajmi v zmysle všeobecného nariadenia o ochrane údajov a zaobchádzanie s incidentmi v zmysle zákona o kybernetickej bezpečnosti SR (zákon č. 69/2018 Z. z.).

Článok 11
Komunikácia a autentifikácia

1. Pre bežnú komunikáciu, ktorá neobsahuje citlivé informácie, CSIRT Centrum použije konvenčné metódy ako nešifrovaný e-mail alebo telefón.
2. Pre bezpečnú komunikáciu bude použitý zabezpečený-šifrovaný mail. Ak je potrebné autentifikovať osobu pred komunikáciou, možno to urobiť buď prostredníctvom existujúcich sietí dôvery (napr. Trusted Introducer) alebo inými metódami, ako je spätné volanie, spätný e-mail alebo dokonca osobné stretnutie, ak je to potrebné.
3. Pre bezpečnú sieťovú komunikáciu budú použité príslušné sieťové protokoly pre zabezpečenú sieťovú komunikáciu v aktuálnych verziách, pričom ich aktuálnosť (použitá verzia) bude priebežne overovaná. Prechod na novú verziu protokolu bude realizovaný bezodkladne, s prioritizáciou podľa posúdenia rizika, spolu s aplikovaním súvisiacich potrebných bezpečnostných opatrení v rámci procesu riadenia zmien CSIRT.
4. Pre bezpečnú online komunikáciu bude použitá aplikácia zabezpečujúca „end-to-end šifrovanie“.

Článok 12
Etický kódex a kódex správania

1. Okrem vyššie uvedeného Kódexu postupov sú členovia CSIRT Centra viazaní aj Etickým kódexom študentov Slovenskej technickej univerzity v Bratislave a Etickým kódexom zamestnanca Slovenskej technickej univerzity v Bratislave v platnom znení.

Článok 13
Služby - reakcia na incident

1. CSIRT Centrum napomáha fakultným administrátorom z VS FEI STU pri riešení technických a organizačných aspektov incidentov. Poskytuje pomoc alebo rady týkajúce sa:
   a) analýzy a triedenia incidentov,
   b) koordinácie reakcie na incidenty, návrhu reaktívnych bezpečnostných opatrení,
   c) riešenia incidentov,
   d) návrhu preventívnych bezpečnostných opatrení.
2. CSIRT Centrum tiež zbiera štatistiky o incidentoch v rámci svojho sektora zodpovednosti.
3. CSIRT Centrum zvyčajne neposkytuje reakciu na incidenty na mieste.
4. Presná definícia spôsobu poskytovania pomoci a kooperácii bude definovaná v samostatnej smernici pre postup riešenia kybernetických bezpečnostných incidentov pre CSIRT Centrum.

Článok 14
Upozornenia, varovania, oznámenia

1. CSIRT Centrum bude aktívne získavať a vyhodnocovať informácie z dôveryhodnej globálnej siete pre CSIRT tímy a iných dôveryhodných zdrojov o aktuálnych udalostiach a hrozbách a bude reagovať, ak tieto môžu ovplyvniť infraštruktúru IT FEI STU alebo ich používateľov.

2. Na základe očakávaného dopadu vydáva CSIRT Centrum výstrahy, varovania alebo oznámenia prostredníctvom vhodných kanálov na poskytovanie týchto informácií v rámci určeného sektoru zodpovednosti.

Článok 15
Manipulácia s artefaktmi

1. Ak analýza incidentu ukáže, že môže ísť o neznámy alebo sofistikovaný útok alebo je cieľ opakovane napadnutý, CSIRT Centrum skontroluje artefakty nájdené počas riešenia incidentu, aby účinne zabránil ďalším útokom.
2. Postup analýzy a kontroly a definícia typov útokov, pri ktorých sa zber artefaktov bude vykonávať, bude definovaný samostatnou smernicou.

Článok 16
Vzdelávanie, školenie, budovanie povedomia

1. CSIRT Centrum propaguje osvedčené postupy súvisiace s bezpečnosťou IT formou vzdelávacieho webového portálu, diskusií na mieste, workshopov a školení v oblasti kybernetickej oblasti. Členovia CSIRT Centra sa podieľajú aj na príprave a výučbe kurzov súvisiacich s kybernetickou bezpečnosťou.

Článok 17
Výskum

1. Fakulta elektrotechniky a informatiky STU v Bratislave realizuje vedecký výskum v doméne kybernetickej bezpečnosti v týchto oblastiach:
   a) detekcia a sledovanie incidentov,
   b) zdieľanie poznatkov o incidentoch.
2. Prebiehajúci výskum zameraný na včasnú detekciu incidentov, analýzu incidentov a zdieľanie poznatkov o incidentoch sa v CSIRT Centre bude synergicky rozvíjať, rovnako ako aj iné výskumné aktivity a zároveň činnosť CSIRT Centra poskytne cenné poznatky a dáta pre realizáciu výskumu.

Článok 18
Pomoc so systémom riadenia informačnej bezpečnosti

1. CSIRT Centrum poskytuje analýzy, poradenstvo a návrhy súvisiace s implementáciou povinností vyplývajúcich zo súčasnej a novozavedenej legislatívy SR a EÚ v oblasti ochrany osobných údajov, informačnej bezpečnosti a kybernetickej bezpečnosti.

Článok 19
Hlásenie incidentov

1. Incidenty sa nahlasujú prostredníctvom formulárov zverejnených na stránke CSIRT Centra. Incident je možné nahlásiť aj inou cestou, pomocou e-mailu, alebo telefonicky cez kontaktné údaje uverejnené na stránke CSIRT Centra (https://csirt.fei.stuba.sk/).
2. V prípade kybernetického bezpečnostného incidentu, ktorý naplnil kritériá závažného kybernetického incidentu podľa Zákona č. 69/2018 o kybernetickej bezpečnosti a Vyhlášky č. 165/2018, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov sa postupuje v súlade s uvedenou legislatívou.

Článok 20
Vylúčenie zodpovednosti

1. Aj keď sa pri príprave informácií, oznámení a upozornení prijmú všetky preventívne opatrenia, CSIRT Centrum nepreberá žiadnu zodpovednosť za chyby alebo opomenutia z prebraných a inými stranami preukázateľne dodaných informácií, ani za škody vyplývajúce z použitia informácií v nich obsiahnutých.

Článok 21
Prechodné a záverečné ustanovenia

1. Tento organizačný poriadok nadobúda platnosť dňom 03.02.2025 a účinnosť dňom 03.02.2025.

V Bratislave, 03.02.2025

prof. Ing. Vladimír Kutiš, PhD., v. r.
dekan FEI STU

Príloha č. 1 Predmet monitorovania CSIRT Centra

V zmysle čl. 7 ods. 1 Organizačného poriadku CSIRT Centra stanovujem, že predmetom monitorovania CSIRT Centra bude infraštruktúra a informačné systémy siete vytvorenej na tento účel. Táto sieť bude izolovaná virtuálna sieť alebo fyzicky oddelená lokálna sieť s prístupom na internet.

V Bratislave, 03.02.2025

prof. Ing. Vladimír Kutiš, PhD.,v.r.
dekan FEI STU