



COMPUTER SECURITY
INCIDENT RESPONSE TEAM



COMPUTER SECURITY INCIDENT RESPONSE TEAM (BEZPEČNOSTNÍ
TÝM PRO ŘEŠENÍ POČÍTAČOVÝCH BEZPEČNOSTNÍCH INCIDENTŮ)
OSTRAVSKÉ UNIVERZITY

Výročná správa 2018

CSIRT OU
Ostravská univerzita
30. dubna 22, 701 03 Ostrava
cisrt@osu.cz | csirt.osu.cz

30.1.2018



Obsah

1	Vymedzenie a členovia CSIRT OU	2
2	Úvod a stručný „historický“ súhrn	3
3	Oblasti pôsobnosti CSIRT OU	4
4	Realizované aktivity CSIRT OU	5
4.1	Riešenie kybernetických bezpečnostných incidentov	5
4.2	Edukačná činnosť	6
4.3	Výskum	7
4.4	Národná a medzinárodná spolupráca	7
4.5	Pomoc s implementáciou legislatívy	9
5	Rámcový plán na rok 2019	10

1 Vymedzenie a členovia CSIRT OU

- CSIRT OU má štatút pracovnej skupiny podľa opatrenia rektora 39/2018 (OU-13358/90-2018).
- Webová stránka CSIRT OU: csirt.osu.cz, anglická verzia: csirt.osu.eu.
- Kontaktný e-mail: csirt@osu.cz
- Hlásenie kybernetických bezpečnostných incidentov: csirt@helpdesk.osu.cz
- Telefonické kontakty:
Hlásenie incidentov, bežná agenda: +420 734 163 004
Urgentné náležitosti: +420 734 163 003
- Členmi skupiny CSIRT OU sú:
 - RNDr. Matej Zuzčák (predseda),
 - Ing. Pavel Smolka, Ph.D,
 - RNDr. Tomáš Sochor, CSc.,
 - Mgr. Milan Zenka.
- CSIRT OU nemá vlastný rozpočet, drobné financie pre možnosť základného fungovania poskytuje Katedra informatiky a počítačů (KIP).
- CSIRT OU nemá výkonné právomoci a pri riešení bezpečnostných incidentov môže pôsobiť len v roli koordinátora, realizovať edukačné či výskumné aktivity, zaisťovať národnú i medzinárodnú spoluprácu a pomáhať s implementáciou legislatívy.
- Detailný popis činností CSIRT OU obsahuje dokument RFC 2350¹.
- CSIRT OU má status „Listed“² v medzinárodnej organizácii združujúcej CSIRT tímy najmä v EÚ.

¹dokument RFC 2350– <https://dokumenty.osu.cz/csirt/CSIRT-OUrfc2350.txt>

²status „Listed“ v organizácii TF-CSIRT pre CSIRT OU <https://www.trusted-introducer.org/directory/teams/csirt-ou.html>

2 Úvod a stručný „historický“ súhrn

Kybernetická bezpečnosť sa stáva v súčasnosti neustále viac skloňovaným pojmom. Deje sa tak vo všetkých oblastiach – od výskumnej resp. akademickej sféry, cez bežných používateľov systémov až po obranné a vojenské prostredie i geo-politiku, výnimkou samozrejme nie je ani komerčný sektor cielený na koncových užívateľov a firmy.

V rôznych organizáciách je potrebné budovať kapacity pre zvládanie potenciálnych bezpečnostných incidentov a hrozieb, ale zároveň budovať i preventívne opatrenia - vrátane vzdelávania tak, aby sa pokiaľ možno čo najviac dokázalo takýmto incidentom predchádzať. Jednotky, ktoré túto činnosť zabezpečujú sa zvyčajne označujú ako *Computer Security Incident Response Team (Bezpečnostný tím pro řešení počítačových bezpečnostních incidentů)* skrátené *CSIRT*.

CSIRT OU vznikol ako iniciatíva členov *Katedry informatiky a počítačů (KIP)* na *Přírodovědecké fakulte (PřF)* Ostravskej univerzity. Cesta k jeho oficiálnemu založeniu a formalizovaniu bola neľahká. Členovia katedry vedený RNDr. Matejom Zuzčákom sa prvý raz stretli s pánom rektorom prof. MUDr. Janom Latom, CSc. v lete 2017. Tomuto stretnutiu predchádzala už viac než ročná zdĺhavá a náročná intenzívna diskusia s *Centrom informačních technologií (CIT)* OU, ale i diskusia v rámci KIP, kde celý projekt veľmi zásadne podporilo vedenie KIP a to najmä vedúci tejto katedry doc. RNDr. PaeDr. Hashim Habiballa Ph.D, PhD., ale následne i dekan PřF doc. RNDr. Jan Hradecký Ph.D. Po kladnom stanovisku pána rektora pokračovalo jednanie s vedením OU najmä s pani kancelárkou Mgr. Monikou Šumberovou a na konci februára 2018 bolo prijaté opatrenie rektora 39/2018 (OU-13358/90-2018), ktoré CSIRT OU formalizovalo ako pracovnú skupinu.

Boli poverení členovia a predseda tejto skupiny. O niekoľko týždňov neskôr bol zriadený i web csirt.osu.cz, na ktorom členovia CSIRT OU aktívne pracovali a stále i pracujú a CSIRT OU bol začlenený do Helpdesku OU, zriadený bol e-mailový a telefonické kontakty, čo umožnilo zahájiť reálne pilotné fungovanie tejto skupiny. Táto správa v súlade s opatrením rektora sumarizuje v podstate necelý prvý rok fungovania CSIRT OU. Išlo o neľahké obdobie, ktoré sprevádzali najmä zložité jednanie na rôznych úrovniach o samotnom vzniku a rámci pre ďalšie fungovanie, avšak skupine sa podaril v relatívne krátkom čase aj úspech v podobe získania statusu *Listed* v medzinárodnej organizácii združujúcej CSIRT tímy - *TF-CSIRT*. Rozvinutá bola tiež edukačná činnosť, riešených bolo niekoľko bezpečnostných incidentov a pripravili sme i niekoľko možností na vzájomné diskusie jednotlivých subjektov OU, ktoré majú čo povedať do budovania ICT v rámci OU. Tieto diskusie sa podarilo i zrealizovať a zvyčajne sa viedli vo veľmi konštruktívnom duchu.

Postupom času CSIRT OU rozvinul spoluprácu i s ďalšími subjektmi OU napr. marketingovým oddelením, poverencom GDPR, či referátom bezpečnosti práce. V CSIRT OU veríme, že spolupráca i realizácia ďalších aktivít bude napredovať i v roku 2019.

3 Oblasti pôsobnosti CSIRT OU

CSIRT OU pôsobí primárne v piatich oblastiach:

- **Vzdelávacia činnosť**

CSIRT OU realizuje systematické vzdelávanie a jednorazová odborné školenia pre technikov CIT, pre zamestnancov OU (napr. v rámci školenia bezpečnosti práce), pre študentov (napr. v rámci kurzov úvode do štúdia). V prípade výskytu aktuálnej kybernetickej hrozby vydáva odporúčania (best practices), prípadne vykonáva ciele školenia.

- **Výskumná činnosť**

V intenzívnej spolupráci s Katedrou informatiky a počítačov Prírodovedeckej fakulty OU CSIRT OU vykonáva vedecký výskum založený napr. na technickej a štatistickej analýze zachytených kybernetických incidentov. Podieľa sa na publikovaní vedeckých článkov. Podľa aktuálnej situácie kybernetických hrozieb tiež vydáva proaktívnu, alebo preventívne odporúčania a rady, prípadne analytické správy, ktoré popisujú zaznamenané kybernetické hrozby v rámci OU a opatrení, ako sa im v budúcnosti vyhýbať.

- **Riešenie kybernetických bezpečnostných incidentov**

V spolupráci s CIT rieši kybernetické bezpečnostné incidenty, ktoré môžu vzniknúť v rámci ISAS OU. CSIRT OU poskytuje v prípade potreby odbornú konzultačnú pomoc pracovníkom CIT a ďalším zamestnancom OU. CSIRT OU okrem toho analyzuje a vyhodnocuje incidenty, ku ktorým v rámci OU došlo a odporúča preventívne opatrenia.

- **Medzinárodná spolupráca**

CSIRT OU intenzívne rozvíja medzinárodnú spoluprácu predovšetkým s inými CSIRT tímami v rámci ČR a Európskej únie prostredníctvom komunity TF-CSIRT. Zúčastňuje sa stretnutí na národnej úrovni (napr. česká a slovenská komunita) a medzinárodnej úrovni (napr. stretnutie skupiny TF-CSIRT).

- **Pomoc s implementáciou národnej a európskej legislatívy**

CSIRT OU poskytuje svoje analýzy, rady a návrhy pri uvádzaní interných procesov OU do súladu s povinnosťami vyplývajúcimi zo súčasnej a novoprijatej národnej aj nadnárodnej legislatívy (najmä zákon o kybernetickej bezpečnosti).

4 Realizované aktivity CSIRT OU

4.1 Riešenie kybernetických bezpečnostných incidentov

Rok 2018 bol najmä rokom nábehovým, kedy CSIRT OU zahájil svoju pôsobnosť v prostredí, kde ho zatiaľ užívatelia univerzitnej siete - zamestnanci a študenti OU príliš nepoznali. Členovia CSIRT OU intenzívne pracovali a stále i pracujú na tom, aby užívatelia bezpečnostné incidenty vnímali a CSIRT OU ich aktívne hlásili. Aj napriek počiatočnému nízkemu povedomiu boli riešených niekoľko incidentov, možno ich rozdeliť do niekoľkých skupín ako napr.:

- **Phishing a spam**

Viacero incidentov, ktoré boli hlásené CSIRT OU sa týkali obťažujúcich nevyžiadanych elektronických správ (spamu) a správ, ktoré sa javili ako podvodné tzv. phishing. Kliknutím na odkaz, alebo otvorením prílohy v takejto správe si užívateľ mohol infikovať svoj počítač. Všetky preposlané správy tohto druhu boli analyzované a užívatelia boli informovaní čomu sa vyvarovať v budúcnosti. Užívateľom, ktorí sa obrátili na CSIRT OU nevznikli žiadne škody, za poskytnuté rady vyjadrili takmer vždy vďaku.

- **Prevádzkové pravidlá siete**

Jednalo sa o sťažnosti, ktoré adresovalo OU najmä združenie CESNET, napr. vedenie privátnych doménových názvov na servery OU. Okamžite bola zjednaná náprava.

- **Osobné údaje**

V rámci monitoringu bezpečnostných incidentov bol CSIRT OU informovaný i o závažnejšom incidente, kedy došlo k zverejneniu osobných údajov zamestnancami jednej z fakúlt cez nedostatočne zabezpečenú webovú stránku mimo web a portál OU, ktorý spravovala samotná fakulta. Incident primárne riešilo CIT a poverenec GDPR na OU. Dabá webová stránka bola zrušená.

- **Technické problémy portal.osu.cz a e-mailového servera student.osu.cz súvisiace s bezpečnosťou**

CSIRT OU zaevidoval incident, kedy dvaja pracovníci OU s rovnakými priezviskami mohli vidieť určitý obsah, ktorý bol určený výhradne len danému pracovníkovi. Na problém bolo upozornené patričné oddelenie CIT a problém bol odstránený. V decembri 2018 bolo tiež identifikovaných niekoľko bezpečnostných zraniteľností vrátane vysoko rizikovej zraniteľnosti *Heartbleed* (CVE-2014-0160) na serveri student.osu.cz, ktorý je používaný pre príjem, odosielanie a ukladanie študentskej univerzitnej elektronickej pošty. Po vysvetlení nebezpečnosti situácie bol daný systém zo strany CIT aktualizovaný a zraniteľnosti odstránené.

- **Pracovné stanice infikované malwarom**

CSIRT OU zaznamenal za uplynulý rok i niekoľko incidentov, kedy došlo, alebo existovalo vysoké riziko infekcie pracovnej stanice vo vlastníctve OU škodlivým kódom (malware). Náprava bol zjednaná v spolupráci s patričnými technikmi zodpovednými za danú budovu/zložku OU. V prípade hrozby šíriacej sa sieťou OU e-mailom bola vydaná i správa³, ktorá upozorňovala na toto riziko a zároveň ho i analyzovala.

³Správa o šírení nebezpečného e-mailu sieťou OU – <https://www.osu.cz/23091/nebezpecny-e-mail/>

4.2 Edukačná činnosť

CSIRT OU považuje vzdelávanie všetkých troch skupín v rámci OU - zamestnanci, študenti, technici CIT za jednu z hlavných priorít, nakoľko prevencia je najefektívnejšia v zabránení vzniku potenciálnych hrozieb. Počas krátkej existencie CSIRT OU sme stihli zrealizovať niekoľko vzdelávacích aktivít a ďalšie naplánovať na rok 2019.

- **Vzdelávanie študentov v rámci kurzu Úvod do štúdia**

CSIRT OU sa zapojil do vzdelávania študentov o základoch bezpečného používania ICT a kybernetickej bezpečnosti v rámci kurzu Úvod do štúdia už v roku 2017 ako súčasť predmetu INPOG pre bšety obory Pedagogické fakulty a Fakulty sociálnych štúdií a pre študentov Katedry informatiky a Katedry informatiky a počítačov Přírodovědecké fakulty. V roku 2018 CSIRT OU ponúkol možnosť podobného kurzu viacerým fakultám no žiaľ zareagovala opäť iba Pedagogická fakulta a Fakulta sociálnych štúdií v rámci predmetu INPOG a tiež Katedry informatiky a počítačov. Študentky a študenti boli počas kurzu oboznámení napr. o tom, ako by si mali zabezpečiť počítač či mobil, ako byť ostražitý pri používaní WiFi sietí, šifrovaného HTTPS spojenia, a pri práci s e-mailovými správami, kde na nich číha nebezpečenstvo phishingu. Ďalej boli poučení aj o tom, aké pravidlá platia pre používanie univerzitných informačných systémov a sietí a ako nahlásiť bezpečnostné incident v prípade, že sa s ním stretnú. Viac informácií je možné nájsť v osobitej správe⁴.



Obr. 1: Študenti počas prednášky CSIRT OU v rámci predmetu INPOG.

- **Vzdelávanie technikov CIT**

Ešte na jeseň roku 2017 bol zrealizovaný pilotný workshop pre vybraných technikov CIT o kybernetickej bezpečnosti, phishingu, ransomware a detekcii či odstraňovaní malware. V školeniach sa bude pokračovať po dohode CIT i v roku 2019, pravdepodobne v marci, alebo apríli 2019.

⁴Správa o zapojení sa CSIRT OU do vzdelávania v predmete INPOG – <https://www.osu.cz/22751/csirt-ou-vzdelaval-nastupujici-studenty-o-zakladnich-zasadach-bezpecneho-pouzivani-ict/>

- **Príspevky a návody na webe csirt.osu.cz**

Na webovej stránke csirt.osu.cz bolo publikovaných niekoľko praktických článkov a návodov pre zamestnancov a študentov OU i verejnosť napr. výstraha a analýza⁵ škodlivej správy, ktorá sa šírila sieťou OU.

Ďalej návod⁶, ako posilať a prijímať zabezpečené e-mailové správy, ktoré dokážu jasne preukázať autenticitu resp. to, že ich odoslala skutočne osoba, od ktorej prišli, prípadne ich aj šifrovať. Za účelom sprehľadnenia takýchto návodov vznikla na webovej stránke CSIRT OU i osobitá sekcia „Praktické rady“.⁷

- 18.10.2018 sa vedúci CSIRT OU - RNDr. Matej Zuzčák stretol so zástupcami PR oddelenia OU - Mgr. Adamom Soustružníkom a Mgr. Janom Fricom, kde rozoberali ďalšie možnosti spolupráce a propagácie CSIRT OU. Podrobnosti o týchto plánoch sú popísané v rámcovom pláne na rok 2019.

4.3 Výskum

Členovia CSIRT OU vytvorili počas roku 2018 viacero vedeckých článkov, ktoré sú v súčasnosti v recenzentskom konaní. Tiež bola zahájená diskusia o možnostiach efektívnejšieho sledovania sieťovej prevádzky siete OU, na základe ktorej sa bude dať lepšie realizovať vedecká činnosť. Keďže ide o rozsiahlejší projekt, realizácia je dlhodobšia a posun sa očakáva v roku 2019.

4.4 Národná a medzinárodná spolupráca

- 22.6.2017 RNDr. Matej Zuzčák vystúpil na Pracovnej skupine CSIRT, ktorú organizoval CSIRT.CZ (CZ-NIC) ako koordinátor národnej komunity s odbornou prednáškou „Štatistické metódy analýzy dát zachytených honeypotmi“⁸. Ostravská univerzita sa vtedy zúčastnila ako pozorovateľ ešte bez oficiálneho zaradenia medzi CSIRT skupiny. CSIRT OU bol účastný stretnutia i v roku 2018.
- 20.12.2017 zavítala na našu univerzitu návšteva z CSIRT-MU na Masarykovej univerzite v Brne (reprezentovaná Bc. Tomášom Plesníkom - vedúcim pracoviska Skupiny reakcie na incidenty a RNDr. Martinom Husákom) a CSIRT.CZ (Mgr. Zuzana Duračinská - koordinátorka národných CSIRT tímov a členka riadiaceho výboru TF-CSIRT "Steering Committee"). Prebehlo pracovné stretnutie, na ktorom sa za účasti ľudí budujúcich CSIRT OU, členov KIP a pracovníkov CIT jednalo o potrebe zriadenia CSIRT skupiny na OU. Pozvané bolo i vedenie OU. Okrem toho si hostia pripravili i 3 prednášky pre študentov KIP.

⁵výstraha a analýza škodlivej správy v sieti OU – <https://www.osu.cz/23091/nebezpecny-e-mail/>

⁶Návod pre zabezpečenie e-mailovej komunikácie – <https://portal.osu.cz/wps/myportal/Doks?idDokument=31542>

⁷Sekcia „Praktické rady“ na webe csirt.osu.cz – <https://www.osu.cz/prakticke-rady/>

⁸„Štatistické metódy analýzy dát zachytených honeypotmi“ – Prednáška „Štatistické metódy analýzy dát zachytených honeypotmi“ na workshope CSIRT.CZ <https://www.nic.cz/page/3544/csirtcz-working-group/>



Obr. 2: Počas pracovnej diskusie o dôležitosti zriadenia CSIRT OU s hosťami.

- Z pohľadu medzinárodnej spolupráce bolo najdôležitejšie začlenenie skupiny CSIRT OU do medzinárodnej organizácie TF-CSIRT. Jednalo sa o neľahký proces, kedy každú skupinu CSIRT v pozícii kandidáta musia schváliť zvyšní členovia hlasovaním. Novo prijímaný tím musí mať 2 odborných garantov z pomedzi ostatných už akreditovaných, alebo certifikovaných tímov, ktorí zaručujú, že daný kandidát spĺňa všetky požiadavky organizácie. V prípade CSIRT OU boli garantmi CSIRT-MU a CSIRT.CZ - certifikované CSIRT tímy. Revízne a konzultačné stretnutie CSIRT OU s garantom CSIRT-MU, prebiehalo 18.6.2018, viac informácií je dostupných v správe⁹. Po tomto stretnutí CSIRT OU získal status „Listed“¹⁰ v TF-CSIRT 4.7.2018.

⁹Správa z návštevy CSIRT-MU – <https://www.osu.cz/22527/csirt-ou-na-navsteve-csirt-mu/>

¹⁰Status „Listed“ tímu CSIRT OU – <https://www.trusted-introducer.org/directory/teams/csirt-ou.html>



Obr. 3: Spoločná fotka po stretnutí v Brne. Na fotografii zľava: Mgr. Martin Laštovička (CSIRT-MU), Ing. Pavel Smolka, Ph.D (CSIRT OU), RNDr. Tomáš Sochor, CSc. (CSIRT OU), Tomáš Plesník (CSIRT-MU, vedúci Skupiny reakcie na incidenty), RNDr. Matej Zuzčák (vedúci CSIRT OU), Mgr. Milan Zenka (CSIRT OU), RNDr. Martin Husák (CSIRT-MU).

4.5 Pomoc s implementáciou legislatívy

- CSIRT OU veľmi víta zosúladienie interných predpisov OU s Nariadením Európskeho parlamentu a Rady 2016/679 (GDPR) a teší nás práca, ktorú odvodili v tomto smere najmä pani kancelárka - Mgr. Monika Šumberová a poverenec GDPR Mgr. Bc. Jan Humpolík.
- Primárnym cieľom CSIRT OU je dosiahnuť zo strany OU splnenie požiadavok vyplývajúcich zo zákona 181/2014 Sb. „Zákon o kybernetické bezpečnosti“ (ZKB) - ktorý definuje univerzity ako VIS (významný informačný systém) podľa vyhlášky 317/2014 Sb. a to najmä vytvorením nových smerníc rektora, či aktualizáciou existujúcich a vzdelávacou činnosťou, tak aby sa predpisy čo najviac aplikovali v praxi.
- 13.12.2018 sa uskutočnilo pracovné stretnutie organizované CSIRT OU, ktorého sa zúčastnili za CSIRT OU: RNDr. Matej Zuzčák, RNDr. Tomáš Sochor, CSc.; za CIT: RNDr. Pavla Lokajová, Jiří Kubina, Martin Kozelský; poverenec GDPR: Mgr. Bc. Jan Humpolík; referát BOZP: Ing. Martin Zimný. Na tomto stretnutí okrem iného zaznelo silné odhodlanie všetkých zúčastnených implementovať požiadavky ZKB v čo najkratšom možnom čase. Existujúce smernice a opatrenia k bezpečnosti ICT OU - v súčasnosti smernice 150 a 151 budú aktualizované. Do aktualizovaných resp. nových smerníc budú zakomponované požiadavky CIT a najmä legislatívne požiadavky vyplývajúce zo zákona 181/2014 Sb. (ZKB), ktorý definuje univerzity ako VIS vyhlášky 317/2014 Sb. a zohľadní sa najmä vyhláška 82/2018 Sb. ukládajúca konkrétne povinnosti pre VIS. Vytvorenie smerníc resp.

opatrení bude primárne viesť p. Humpolík. CSIRT OU a CIT sa aktívne zúčastnia pri pripomienkovaní a predkladaní návrhov, podnetov a pri koordinovaní.

5 Rámcový plán na rok 2019

V roku 2019 čaká CSIRT OU v spolupráci s rôznymi subjektmi univerzity mnoho úloh, pôjde najmä o:

- **Vzdelávacia činnosť:**

- CSIRT OU plánuje v spolupráci s CIT, poverencom GDPR a referátom BOZP školenie pre všetkých zamestnancov OU - akademických i neakademických o základoch kybernetickej bezpečnosti. Školenie by malo pozostávať z častí: Základy bezpečnosti ICT, osobné údaje a narábanie s nimi a základné pravidlá bezpečného používania systémov a sietí OU. Školenie by sa malo konať pravdepodobne v apríli 2019 2 kurzy na 2 rôznych miestach. (pravdepodobne Českobratrská a Fr. Šrámka).
- CSIRT OU v úvode akademického roku 2019/2020 aktívne ponúkne krátke školenie o základoch kybernetickej bezpečnosti v rámci kurzov Úvod do štúdia. Pounka bude smerovať všetkým fakultám a CSIRT OU osloví pre lepšiu propagáciu aj vedenie OU a PR oddelenie OU.
- CSIRT OU zrealizuje po predbežnej dohode s CIT školenie pre technikov CIT pravdepodobne počas apríla 2019.
- CSIRT OU pripraví osobitné workshopy na rôzne témy. Napríklad v letnom semestri 2018/2019 bude realizovať workshop o základoch zabezpečenia zariadení s operačným systémom Android prístupné všetkým študentom a zamestnancom OU, neskôr možno i verejnosti.
- CSIRT OU zváži možnosť prípravy špecifických webinárov (kurzov dostupných cez online webové prostredie) na rôzne témy.

- **Riešenie kybernetických bezpečnostných incidentov:**

- CSIRT OU sa posnaží zlepšiť a prehĺbiť spoluprácu s CIT - najmä vyjednať dohodu o nakladaní s vyhradenými údajmi, ktoré sa vyskytujú pri riešení bezpečnostných incidentov.
- CSIRT OU sa v spolupráci s PR oddelením OU a s vedením OU posnaží zlepšiť povedomie o CSIRT OU, aby sa zvýšil počet hlásených incidentov a tiež prevencia. Pôjde hlavne o využitie komunikačných kanálov OU: Facebook, web OU, nástenky jednotlivých budov OU.

- **Výskum:**

- CSIRT OU sa pokúsi do siete OU integrovať prostriedky pre jej lepšiu monitoring, čo by výrazne prispelo k zlepšeniu výskumných možností našej skupiny. Pravdepodobne sa bude jednať o technológiu NetFlow. Realizácia závisí na rokovaní s CIT. Ide o dlhodobejší zámer.
- CSIRT OU sa pokúsi dohodnúť s CIT na efektívnejšom vyhodnocovaní zaznamenaných incidentov, nielen priamo bezpečnostných, ale i príbuzných, čo by tiež výrazne zlepšilo výskumné možnosti CSIRT OU - napr. využitie štatistických analýz z takýchto dát.

- **Národná a medzinárodná spolupráca:**

- CSIRT OU bude i naďalej udržiavať čo najužšie kontakty s ostatnými univerzitami ako je napr. Masarykova univerzita v Brne, ale i organizáciami ako napr. CZ-NIC a TF-CSIRT.
- CSIRT OU sa bude snažiť zúčastňovať na všetkých relevantných podujatiach - konferencie, workshopy na národnej a pokiaľ možno i medzinárodnej úrovni. Zvlášť je potrebné zamerať sa i na podujatia združenia CESNET.

- **Pomoc s implementáciou národnej a európskej legislatívy:**

- CSIRT OU považuje za prioritu, ako už bolo povedané implementáciu ZKB a s tým spojených vyhlášok týkajúcich sa VIS do vnútorných predpisov OU. V tejto veci bola zahájená spolupráca s poverencom GDPR a CIT ktorá by mala pokračovať i v roku 2019.
- CSIRT OU za dôležité tiež považuje vypracovať bezpečnostnú politiku OU o čo sa bude snažiť najmä v spolupráci s CIT a vytvoriť „Výbor pro řízení kybernetické bezpečnosti“ v súlade s vyhláškou 82/2018 o čo sa bude snažiť najmä v spolupráci s poverencom GDPR.

Za posledný rok CSIRT OU urazil neľahkú cestu a pomohol sa Ostravskej univerzite dostať sa medzi inštitúcie, ktoré berú bezpečnosť ICT veľmi vážne, čo je základným predpokladom pre efektívnu prevenciu. Členovia CSIRT OU sa budú snažiť plniť všetky stanovené úlohy najlepšie ako to bude v ich silách, avšak veľa zo stanovených úloh závisí aj od prístupu ďalších subjektov. Veríme, že nájdeme spoločnú reč a konštruktívne sa posunieme ďalej pri budovaní silnej ale i kyberneticky bezpečnej univerzity.

Dokument vypracoval RNDr. Matej Zuzčák (predseda skupiny CSIRT OU) s odsúhlasením a za príspevia všetkých členov skupiny CSIRT OU.



COMPUTER SECURITY
INCIDENT RESPONSE TEAM

