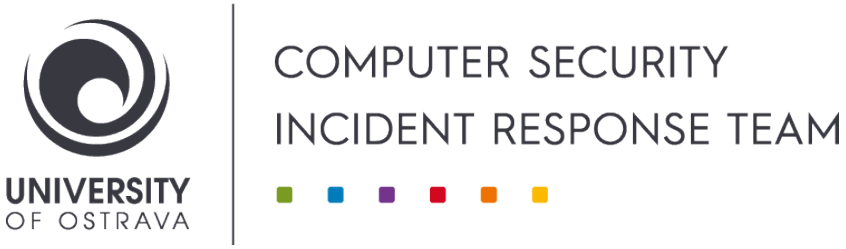

Computer Security Incident Response Team (Bezpečnostní tým pro řešení počítačových bezpečnostních incidentů) Ostravské univerzity

Výročná správa 2020

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

25.1.2021

Obsah

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
- Členmi skupiny CSIRT OU od 1.1.2021 sú:
  - RNDr. Matej Zuzčák, Ph.D. (predseda),
  - Ing. Pavel Smolka, Ph.D.
- CSIRT OU nemá vlastný rozpočet, drobné financie pre možnosť základného fungovania poskytuje Katedra informatiky a počítačů (KIP).
- CSIRT OU nemá výkonné právomoci a môže vydávať len odporúčania (najmä pri riešení bezpečnostných incidentov), pracovať v úlohe koordinátora a realizovať edukačné či výskumné aktivity, zaisťovať národnú a medzinárodnú spoluprácu.
- Detailný popis činností CSIRT OU obsahuje dokument RFC 2350[1].
- CSIRT OU má status „Listed“[2] v medzinárodnej organizácií združujúcej CSIRT tímy najmä v EÚ.

[1] dokument RFC 2350– `https://dokumenty.osu.cz/csirt/CSIRT-OUrfc2350.txt`

[2] status „Listed“ v organizácií TF-CSIRT pre CSIRT OU `https://www.trusted-introducer.org/directory/teams/csirt-ou.html`

2 Úvod

CSIRT OU sa v roku 2020 posunul do tretieho roku svojho oficiálneho fungovania. Kybernetickej bezpečnosti sa i v tomto roku venovala náležitá pozornosť. Okrem pozornosti vyvolanej rôznymi kybernetickými hrozbami sa objavila aj pozornosť z pohľadu štátnych a európskych regulátorov, nakoľko dopad kybernetických hrozieb sa začína čím ďalej viac prejavovať aj na fungovaní verejnej správy, kde je potrebné zaujať proaktívny prístup.

Rok 2018 bol venovaný najmä zahájeniu činnosti a formálnemu zakotveniu tejto pracovnej skupiny. V roku 2019 sme ako jednu z najdôležitejších činností zahájili vo väčšom rozsahu spoluprácu s ostatnými zložkami univerzity. Prirodzene sa jednalo v prvom rade o spoluprácu s Katedrou informatiky a počítačů na Přírodovědeckej fakulty (KIP PřF), s Centrom informačních technologií (CIT), poverencom GDPR a s Referátom bezpečnosti práce a požiarnej ochrany, ale i s PR oddelením Ostravskej univerzity. To viedlo i k spusteniu najrôznejších edukačných aktivít pre zamestnancov i študentov OU. V roku 2020 sme na tieto aktivity popri bežnej činnosti spočívajúcej v riešení kybernetických incidentov nadviazali. Avšak mnohé plány nečakane pozmenila pandémia corona vírusu. Táto pandémia iste veľmi podobne obmedzila a zasiahla do fungovania i mnohých iných činností na OU.

Na pandémiu sme reagovali tým, že väčšinu aktivít sme podobne ako pri výuke presunuli do online priestoru. Vzniklo preto niekoľko pomerne zaujímavých seminárov pre zamestnancov i študentov, kde sme tieto dve podstatné skupiny oboznámili s najčastejšie sa vyskytujúcimi nástrahami kyber priestoru. Nie všetky činnosti bohužiaľ vyšli tak, ako sme ich plánovali a isté problémy sa prejavili i v personálnom obsadení CSIRT OU. Jednalo sa o odchody členov, ktorým skončili ich pracovné a študijné úväzky na OU, keďže samotné členstvo v CSIRT OU nie je pracovným pomerom. Túto situáciu budeme intenzívne riešiť v roku 2021 ako uvádzame i ďalej v tejto správe.

Táto správa v súlade s opatrením rektora sumarizuje tretí rok fungovania CSIRT OU a predkladá víziu CSIRT OU pre rok 2021. V CSIRT OU opäť veríme, že práca i realizácia ďalších aktivít bude úspešne napredovať.

3 Oblasti pôsobnosti CSIRT OU

CSIRT OU pôsobí primárne v piatich oblastiach:

- **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.

- **Edukačná 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 kybernetické hrozby vydáva odporúčania (best practices), prípadne vykonáva cielená školenia.

- **Výskum**
  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 publikovanie 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.

- **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 2020 bol tretím rokom fungovania CSIRT OU. Povedomie medzi užívateľmi siete a systémov OU o tejto skupine opäť o niečo vzrástlo. Samozrejme členovia CSIRT OU i naďalej intenzívne pracujú na tom, aby užívatelia bezpečnostné incidenty vnímali a CSIRT OU ich aktívne hlásili. Zaznamenané incidenty možno rozdeliť do niekoľkých skupín napr.:

- **Phishing a spam**
  Mnoho incidentov, ktoré boli hlásené CSIRT OU v roku 2020 sa týkali veľmi podobne ako i v rokoch 2018 a 2019 obťažujúcich, nevyžiadaných 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. Jedná sa o zásadný problém pre univerzitu, nakoľko najčastejším problémom po infekcii účtu/zariadenia našich zamestnancov je masívne rozosielanie spamu, čo automaticky znamená blokovanie IP adries univerzity pre iné subjekty, pričom náprava tohto stavu je zložitá a vyžaduje i finančné prostriedky. Napriek tomu, že sme zrealizovali už dve rozsiahle školenia - jedno prezenčne a druhé dištančnou online formou, problém pretrváva. Technické riešenia tohto problému sú do značnej miery obmedzené, nakoľko vysokou mierou filtrácie vzniká (a reálne k nemu aj došlo) riziko straty i takých e-mailových správ, ktoré sú legitímne. Avšak určité špecifické technické riešenia budú postupne implementované v gescii správcu e-mailového serveru, k čomu sme pripravení poskytnúť podporu. Okrem toho v spolupráci s rektorátom zintenzívnime i ďalšie vzdelávanie zamestnancov a študentov a to napr. i kratšou formou rôznych inštruktážnych videí a rôznymi grafickými pomôckami, ako sme už i začali. Bude tiež potrebné zvážiť povinnosť základných kurzov k kybernetickej bezpečnosti pre všetkých zamestnancov a študentov OU a motiváciu prípadne represiu pri (ne)dodržaní zásad bezpečného používania siete.

- **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.

4.2 Edukačná činnosť

CSIRT OU i naďalej považuje vzdelávanie všetkých troch skupín v rámci OU - zamestnanci (akademickí i neakademickí), študenti, technici CIT za jednu z hlavných priorít, nakoľko prevencia je najefektívnejšia v zabránení vzniku potenciálnych hrozieb. Počas roka 2020 sme zrealizovali viaceré vzdelávacie aktivity v online forme.

- **Vzdelávanie študentov v rámci kurzu Úvod do štúdia**
  CSIRT OU sa už tradične - po tretí raz zapojil do vzdelávania študentov o základoch bezpečného používania ICT a kybernetickej bezpečnosti v rámci kurzu „Úvod do štúdia“ ako súčasť predmetu INPOG pre všetky obory Pedagogické

fakulty a Fakulty sociálních studii. Tento rok kurz prebehol výhradne online formou. 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.

- **Príspevky a návody na webe csirt.osu.cz**
  Na webovej stránke csirt.osu.cz sú i naďalej publikované praktické články a návody pre zamestnancov a študentov OU i verejnosť (jedná sa hlavne o sekcie „Praktické rady“[3] a „Aktuality“[4]. Ako príklad možno uviesť prehľadnú infografiku[5] týkajúcu sa phishingových e-mailov. Snažíme sa v nej stručne a jasne poukázať na čo si musia dávať zamestnanci a študenti OU pozor pri práci hlavne s e-mailovou poštou.

- **Online školenie pre všetkých zamestnancov OU**
  CSIRT OU v spolupráci s pani kancelárkou OU Mgr. Monikou Šumberovou, s poverencom GDPR, CIT zorganizoval ďalšie dobrovoľné školenie formou online webináru pre všetkých zamestnancov OU, v rámci ktorého si mohli rozšíriť svoje vedomosti a zlepšiť zručnosti v oblasti IT bezpečnosti. S prednáškou o právnych aspektoch správania sa zamestnancov OU v kyber priestore vystúpil Mgr. Bc. Jan Humpolík (poverenec pre GDPR na OU), o základoch IT bezpečnosti poslucháčov informoval RNDr. Matej Zuzčák, Ph.D. (vedúci CSIRT OU) a o problémoch, s ktorými sa stretávajú pracovníci CIT pohovorila RNDr. Pavla Lokajová (vedúca technického oddelenia CIT). Po samotných prednáškach prebehla intenzívna diskusia, do ktorých sa poslucháči mali možnosť aktívne zapojiť sa svojimi otázkami a pripomienkami. Online bolo prítomných vyše 70 zamestnancov OU, ďalší si pozreli tento webinár v online archíve. Správa zo školenia je dostupná tiež na stránkach CSIRT OU[6].

- **Online prednáška o základoch bezpečného správania sa v kyber priestore pre študentov PřF**
  CSIRT OU sa zúčastnil na šírení osvety o základoch bezpečného správania sa v kyber priestore aj v rámci prednášky predmetu „Úvod do přírodních věd“ v spolupráci s dekanom PřF doc. RNDr. Janom Hradeckým, Ph.D. Kurz je určený pre všetkých študentov PřF, čo znamená, že dané vedomosti by mohli poslúžiť čo najvyššiemu počtu študentiek a študentov PřF. Záznam je k dispozícií v rámci OU Stream[7]

[3]Sekcia „Praktické rady“ (pre zamestnancov a študentov OU v oblasti kybernetickej bezpečnosti) `https://www.osu.cz/prakticke-rady/`

[4]Sekcia „Aktuality“ (pre zamestnancov a študentov OU v oblasti kybernetickej bezpečnosti) `https://www.osu.cz/aktuality-csirt/`

[5]Praktická infografika o phishingových e-mailech `https://www.osu.cz/24765/prakticka-infografika-o-phishingovych-e-mailech/`

[6]Online webinář Kybernetická bezpečnost – jak se bránit podvodným e-mailům a zneužití vašeho e-mailového účtu - `https://www.osu.cz/25485/kyberneticka-bezpecnost/`

[7]Prednáška o základoch kybernetickej bezpečnosti v rámci predmetu „Úvod do přírodních věd (11)“ - `https://web.microsoftstream.com/video/0e1a5fe3-6a77-4ba4-b9cc-a9b35551d7a3`

Obr. 1: Prednášajúci a moderátorka online workshopu o kybernetickej bezpečnosti pre zamestnancov OU.

Obr. 2: Prednáška v rámci predmetu „Úvod do přírodních věd (11)“.

4.3 Výskum, národná a medzinárodná spolupráca

Členovia CSIRT OU vytvorili i počas roku 2020 viacero vedeckých článkov, ktoré boli publikované vo vedeckých časopisoch s impact factorom a tiež v recenzovaných zborníkoch prezentované na medzinárodných konferenciách (možné nájsť v databáze PUBL). Pôvodne plánovaný projekt v rámci Fondu rozvoja CESNET týkajúci sa netflow monitoringu siete budovy A PřF sa bohužiaľ zrealizovať nepodarilo. Dôvodmi boli: nedostatok finančných prostriedkov a nedostatok ľudských zdrojov. Ďalším čiastkovým problémom bola tiež komplexná rekonštrukcia budovy A. Avšak ako náhrada bude v nasledujúcich 2 rokoch realizovaný projekt vo vlastnej réžii s menšími finančnými nákladmi a to z veľkej často aj v rámci riešenia diplomovej práce konkrétneho študenta. Toto riešenie bude realizované pomocou open-source nástrojov a mohlo by byť rozšírené aj na monitoring celej siete OU.

4.4 Ostatné

V priebehu uplynulého roka tiež došlo bohužiaľ k úbytku členov skupiny CSIRT OU. Tento úbytok nebol spôsobený v súvislosti s plnením si povinností v rámci CSIRT OU, ale v záležitostiach týkajúcich sa primárnych pracovných/štúdijných úväzkov dvoch členov tímu. Členovia CSIRT OU nemajú priamy pracovný pomer s CSIRT OU, ale pôsobili na PřF KIP. V jednom prípade došlo k ukončeniu pracovného pomeru odborného asistenta/docenta na KIP PřF a v druhom došlo už k dávnejšiemu ukončeniu doktorského štúdia na KIP PřF. Prijatie nových členov a celková reorganizácia CSIRT OU bude riešená tento rok tak ako je popísané v rámcovom pláne na rok 2021.

5 Rámcový plán na rok 2021

V roku 2021 čaká CSIRT OU najmä práca na väčšom CRP projekte a viacero organizačných, edukačných i vedeckých aktivít:

- CSIRT OU sa aktívne zapojí do participácie na CRP projekte „Zvýšení úrovně kybernetické bezpečnosti v prostředí VVŠ“, ktorého hlavným koordinátorom je Masarykova univerzita v Brne. Do projektu sa okrem OU zapájajú aj všetky zvyšné verejné vysoké školy/univerzity v ČR. Primárnym cieľom je pripraviť české univerzity na Zákon 181/2014 Sb. o kybernetickej bezpečnosti (ZKB), aplikovať vyhlášky 316/2014 Sb., 317/2014 Sb. (so zapracovaním zmien z vyhlášky 360/2020 Sb.) a vyhlášku 181/2014 Sb., vybudovať potrebné zázemie, klasifikovať tzv. „významné informačné systémy“ (VIS) nahlásiť ich so všetkými náležitosťami na „Národní úřad pro kybernetickou a informační bezpečnost“ (NÚKIB). Ďalej tiež zmapovať aktíva, prijať vnútorné smernice a opatrenia na posilnenie kybernetickej bezpečnosti v rámci OU a nastaviť procesy na ochranu dát a bezpečnostnú politiku celej organizácie. Súčasťou je tiež zlepšovanie vzdelávania zamestnancov a študentov OU. Predseda skupiny CSIRT OU - RNDr. Matej Zuzčák, Ph.D. je spolu s Ing. Pavlom Pomezným (riaditeľ CIT a hlavný riešiteľ), Mgr. Bc. Janom Hupolíkom (poverenec GDPR a kontaktná osoba) a Mgr. Monikou Šumberovou (kancelárka OU) medzi hlavnými riešiteľmi projektu. Projekt bude ukončený k 31.12.2021 a bude predstavovať hlavnú náplň práce pre CSIRT OU na tento rok. Po skončení sa na rok 2022 predpokladá pokračovanie nadväzujúceho CRP projektu.

- Vzdelávanie - edukačná činnosť zostane medzi prioritami CSIRT OU aj v roku 2021. Počas pandémie sa samozrejme budeme musieť sústrediť najmä na dištančné formy vzdelávania zamestnancov a študentov. Pri tomto cieli by sme radi nadviazali už na zrealizované webináre a vytvorili osobitý Moodle kurz i pomocné grafické materiály, návody, postupy apod. S vedením OU i ďalšími zložkami budeme diskutovať i o povinných školeniach, motivácií, testovaní a potenciálnych benefitoch/reštrikciách za opakované plnenie/porušovanie bazálnych bezpečnostných pravidiel zo strany zamestnancov a študentov. Presadzovať budeme stále viac používanie elektronicky podpísaných e-mailov.

- Vnútorná reorganizácia - aj vzhľadom na odchody členov skupiny (popísané vyššie, netýkali priamo činnosti CSIRT OU) bude potrebné reorganizovať štruktúru (prijať nových členov) a zefektívniť fungovanie. Našim plánom je pripraviť viacero možných scénarov a tie prejednať s vedením OU a právnym oddelením. Tiež by

sme radi viac koordinovali riešenie kybernetických incidentov s CIT a zjednotili ich interné hlásenie (osobami z prostredia OU) do jednej helpdeskovej fronty, tak aby sa tieto aktivity neduplikovali. Za dôležité považujeme aj vzájomnú výmenu informácií, túto činnosť je nutné zintenzívniť oproti súčasnému stavu. Ďalšou výzvou je previazať CSIRT OU na organizačnú štruktúru, ktorá vznikne podľa ZKB.

- Vzhľadom na to, že pôvodne zamýšľaný projekt pre monitoring sieťovej prevádzky budovy A PřF OU zlyhal (popísané vyššie) plánujeme realizovať náhradu. Plán je vybudovať zaistenie situačného povedomia v sieti Ostravskej univerzity pomocou open-source nástrojov a rozšíriť ho na monitorovanie čo najväčšej časti siete. S týmto zámerom je previazaná aj konkrétna diplomová práca. Obdobie realizácie je odhadované na približne 2 roky, horizont nasadenie sa teda dá očakávať pravdepodobne v roku 2022/2023.

- Akreditácia CSIRT OU - v rámci spomínaného CRP projektu by sme tento rok radi akreditovali náš CSIRT tím v rámci štruktúr TF-CSIRT. Získanie statusu „Accredited“ by pre univerzitu okrem prestíže znamenalo aj prístup k cenným dátam, poznatkom, know-how a nových odborných kontaktov v rámci komunity.

Dokument vypracoval RNDr. Matej Zuzčák, Ph.D. (predseda skupiny CSIRT OU) s odsúhlasením a za prispenia všetkých členov skupiny CSIRT OU.

COMPUTER SECURITY INCIDENT RESPONSE TEAM