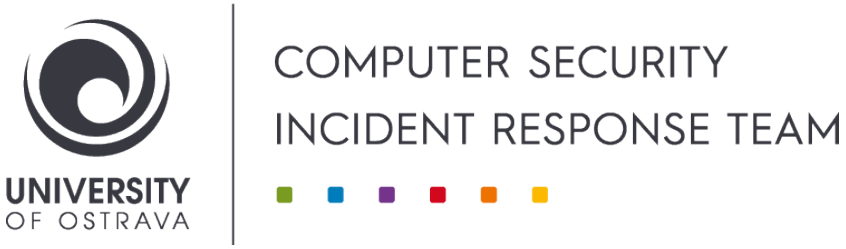

Computer Security Incident Response Team (Bezpečnostní tým pro řešení počítačových bezpečnostních incidentů) Ostravské univerzity

Výročná správa 2019

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

30.1.2020

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 sú:
  - RNDr. Matej Zuzčák (predseda),
  - RNDr. Tomáš Sochor, CSc.,
  - 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 v roku 2019 zahájil svoj druhý rok oficiálneho fungovania. Kybernetická bezpečnosť je i naďalej neustále veľmi 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.

Rok 2018 bol venovaný najmä zahájeniu činnosti a formálnemu zakotveniu tejto pracovnej skupiny. V uplynulom 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.

Hoci nie všetky činnosti išli tak rýchlo ako sme pôvodne očakávali, a to najmä kvôli nutnosti spolupracovať s ďalšími subjektmi OU, ale i s externými organizáciami, jednou z hlavných aktivít, ktorú sa podarilo počas uplynulého roka úspešne zrealizovať bolo veľké školenie o základoch IT bezpečnosti a o bezpečnom používaní systémov univerzity. Na školení sa podieľali všetky vyššie menované subjekty a jeho príprava i realizácia bola veľmi náročná, no potešila nás pozitívna odozva. V podobných aktivitách budeme pokračovať i naďalej. Okrem toho sme stále v rámci svojich možností riešili ohlasované bezpečnostné incidenty, spolupracovali na národnej i medzinárodnej úrovni a venovali sme sa i príprave náročnejších projektov, ktoré by sa mali realizovať v rokoch 2020/2021. Niektoré aktivity pôvodne plánované na rok 2019 sa bohužiaľ ako už bolo spomenuté - najmä kvôli časovej náročnosti ich plánovania a jednaní s inými účastníkmi museli posunúť, no nazdávame sa, že počas druhého roku fungovania sa tie najvýznamnejšie úlohy primárne v oblasti edukácie podarili.

Táto správa v súlade s opatrením rektora sumarizuje druhý rok fungovania CSIRT OU a predkladá víziu CSIRT OU i pre rok 2020. V CSIRT OU 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 2019 bol druhým rokom fungovania CSIRT OU. Povedomie medzi užívateľmi siete a systémov OU o tejto skupine už 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 sa týkali veľmi podobne ako v roku 2018 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. Užívateľom, korí sa obrátili na CSIRT OU nevznikli žiadne škody, za poskytnuté rady vyjadrili takmer vždy vďaku. Avšak okrem odporúčaní pre daného užívateľa nebolo možné podniknúť ďalšie technické kroky. V určitých prípadoch, kedy sa phishingová správa viac dotýkala OU, napr. sa snažila vylákať od užívateľa prihlasovacie meno a heslo, bolo v spolupráci s CIT vydané hromadné upozornenie. Okrem vzdelávania a prípadného upozornenia žiaľ z technického hľadiska nie je možné spraviť.

- **Nájdenie bezpečnostnej zraniteľnosti na webovej stránke tep.osu.cz**
  28.8.2019 kontaktoval CSIRT OU tzv. „bugbounty hunter“, jedná sa o ľudí, ktorí hľadajú bezpečnostné zraniteľnosti a po ich identifikovaní sa obrátia na prevádzkovateľa príslušnej webovej stránky, alebo aplikácie, upozornia ho, poskytnú mu technické detaily a ponechajú mu určitý čas na odstránenie. Ak počas tejto doby k odstráneniu zraniteľnosti nedôjde technické detaily sú zverejnené. Ako odmenu zvyčajne týmto ľuďom postačuje uvedenie referencie na špecializovaných webových stránkach, v tomto prípade openbugbounty.org. Tento konkrétny nálezca objavil XSS zraniteľnosť na webovej stránke vytvorenej v PHP tep.osu.cz vo vlastnej réžii OU (nebol použitý redakčný systém, framework apod.). Po zaevidovaní zraniteľnosti CSIRT OU podnikol všetky náležité kroky, skontaktoval sa s objaviteľom, kontaktoval zodpovedného správcu danej webovej stránky s technickými detailami, aby mohol danú zraniteľnosť odstrániť. Po jej odstránení vedúci CSIRT OU napísal danému objaviteľovi pozitívnu referenciu.

- **Osobné údaje**
  V rámci monitoringu bezpečnostných incidentov bol CSIRT OU informovaný i incidente, kedy došlo k potenciálnemu zverejneniu osobných údajov Incident primárne riešilo CIT a poverenec GDPR na OU.

- **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 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 roka 2019 sme stihli zrealizovať niekoľko vzdelávacích aktivít a to najmä veľké školenie všetkých zamestnancov OU, ktorí mali záujem o základoch IT bezpečnosti a o bezpečnom používaní systémov a siete OU

- **Vzdelávanie študentov v rámci kurzu Úvod do štúdia**
  CSIRT OU sa už tradične 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 a pre študentov Katedry informatiky a Katedry informatiky a počítačů Přírodovědecké fakulty. 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.

- **Veľké školenie pre všetkých zamestnancov OU**
  CSIRT OU v spolupráci s poverencom GDPR, CIT, referátom BOZP a KIP počas apríla 2019 zorganizoval dobrovoľné školenie pre všetkých zamestnancov OU, v rámci ktorého si mohli rozšíriť svoje vedomosti a zlepšiť zručnosti v oblasti IT bezpečnosti a ochrany osobných údajov. Školenia sa zúčastnilo približne 200 zamestnancov naprieč všetkými fakultami a centrami univerzity, okrem akademikov tiež administratívni pracovníci. S prednáškou o GDPR vystúpil Mgr. Bc. Jan Humpolík (poverenec pre GDPR na OU), o základoch IT bezpečnosti poslucháčov informoval RNDr. Matej Zuzčák (vedúci CSIRT OU) a o problémoch, s ktorými sa stretávajú pracovníci CIT pohovorila RNDr. Pavla Lokajová (vedúca technického oddelenia CIT). Školenie prebiehalo na troch rôznych miestach, tak aby zúčastniť sa v mieste svojho pracoviska dostalo čo najviac zamestnancov OU. Po samotných školeniach prebiehali diskusie, do ktorých sa poslucháči mali možnosť aktívne zapojiť sa svojimi otázkami a pripomienkami. Po skončení školenia sa zhruba polovica zúčastnených zapojila do ankety o spokojnosti so školeniami. Väčšina zúčastnených školenia hodnotila pozitívne, objavila sa rad konštruktívnych pripomienok. Správa zo školenia je dostupná tiež na stránkach stránkach CSIRT OU[3].

[3]Školení zaměstnanců Ostravské univerzity o GDPR a IT bezpečnosti `https://www.osu.cz/23690/skoleni-zamestnancu-ostravske-univerzity-o-gdpr-a-it-bezpecnosti`

Obr. 1: Vedúci CSIRT OU - RNDr. Matej Zuzčák počas školenia zamestnancov OU.

Obr. 2: Poverenec GDPR - Bc. Mgr. Jan Humpolík počas školenia zamestnancov OU.

Obr. 3: Vedúca technického oddelenia CIT - RNDr. Pavla Lokajová počas školenia zamestnancov OU.

4.3 Výskum, národná a medzinárodná spolupráca

Členovia CSIRT OU vytvorili počas roku 2019 viacero vedeckých článkov, ktoré boli publikované vo vedeckých časopisoch s impact factorom a tiež v recenzovaných zborníkoch prezentované na medzinárodných konferenciách. Započatá bola tiež príprava projektu do Fondu rozvoja CESNET, ktorého cieľom bude spustenie netflow monitoringu siete budovy A PřF. Tieto výsledky výrazne posilnia možnosti riešenia potenciálnych bezpečnostných incidentov a budú tiež zdrojom pre ďalší výskum.

V rámci spolupráce prebiehala v roku 2019 najmä spolupráca na národnej úrovni - napr. s CSIRT-MU (Masarykova univerzita v Brne) za účelom konzultácii k projektu monitorovania sieťovej prevádzky v sieti OU, vedúci CSIRT OU sa tiež zúčastnil stretnutia národných CSIRT tímov v Prahe.

5 Rámcový plán na rok 2020

V roku 2020 čaká CSIRT OU pravdepodobne realizácia jedného väčšieho projektu a viacero edukačných i vedeckých aktivít:

- **Edukačná činnosť:**
  - CSIRT OU plánuje v spolupráci s CIT, poverencom GDPR, referátom BOZP a PR oddelením pokračovať v školeniach. Tento raz pôjde primárne o workshopy zamerané na konkrétne témy dostupné pre všetkých zamestnancov i študentov OU - napr. zabezpečenie zariadenia s operačným systémom Android apod.
  - Pracovať budeme na vstupnom online kurze pre všetkých nových študentov OU, ktorý sa bude týkať nadobudnutia základných vedomostí a zručností z oblasti IT bezpečnosti a bezpečného používania systémov a siete OU i so základmi narábania s údajmi, ktoré spadajú pod špecifickú ochranu. Na záver účastníci absolvujú test, ktorý bude vyhodnotený v réžii zapojených fakúlt.
  - Pripravovať sa budú aj online kurzy tzv. webináre na rôzne témy, kedy by účastníci absolvovali celý kurz len online formou.
  - CSIRT OU bude so zainteresovanými stranami (CIT, poverenec GDPR, Referát BOZP, PR oddelenie) analyzovať i možnosť pokračovania veľkých školení o bezpečnosti IT pre zamestnancov OU, tak aby bola ich forma pre účastníkov čo najefektívnejšia.
- **Riešenie kybernetických 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 realizáciu ďalších vzdelávacích workshopov a využívanie komunikačných nástrojov (sociálne siete, nástenky apod.).
- **Výskum:**
  - Pripravujeme realizáciu projektu pokročilého bezpečnostného monitoringu pomocou technológie FlowMon, pre ktorý pripravíme projekt do Fondu rozvoja CESNET. Týmto pilotným projektom chceme vytvoriť technické predpoklady pre rozšírenie bezpečnostného monitoringu na celú sieť univerzity, to však bude vyžadovať zabezpečenie potrebných investičných finančných prostriedkov.
  - Pracovníci CSIRT OU plánujú publikovanie viacerých vedeckých článkov časopisoch s Impact Factorom a v recenzovaných zborníkoch na medzinárodných konferenciách.
- **Národná a medzinárodná spolupráca:**
  - CSIRT OU sa bude i naďalej snažiť zúčastňovať na všetkých relevantných podujatiach - konferencie, workshopy na národnej a pokiaľ možno i medzinárodnej úrovni. Obzvlášť pod záštitou CZ NIC, ktorý je koordinátorom národných CSIRT tímov.

I počas druhého roku svojej existencie CSIRT OU pokračoval v neľahkej ceste napomáhaniu Ostravskej univerzite dostať sa medzi inštitúcie, ktoré berú bezpečnosť ICT veľmi vážne, čo je základným predpokladom pre efektívnu prevenciu. Členovia CSIRT OU sa plnili a budú sa snažiť plniť i naďalej všetky stanovené úlohy najlepšie ako to bude v ich silách, avšak rovnako ako v uplynulom roku veľa zo stanovených úloh závisí aj od prístupu ďalších subjektov. Aj naďalej však 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 prispenia všetkých členov skupiny CSIRT OU.

COMPUTER SECURITY INCIDENT RESPONSE TEAM