



COMPUTER SECURITY
INCIDENT RESPONSE TEAM



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

Výročná správa 2021

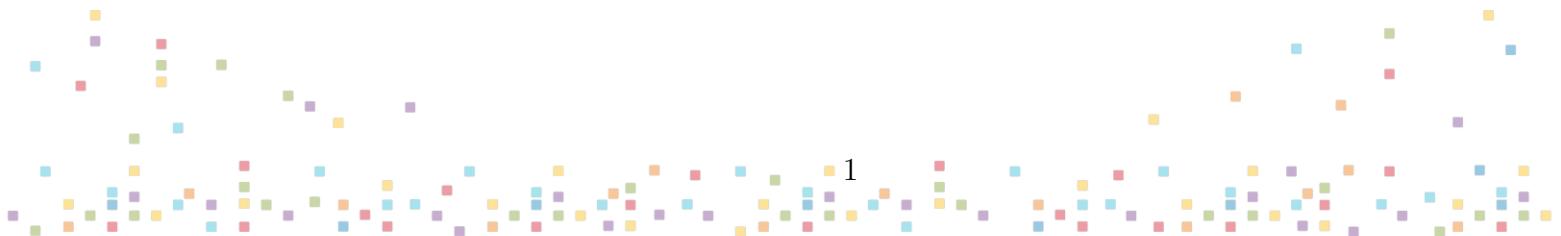
CSIRT OU
Ostravská univerzita
30. dubna 22, 701 03 Ostrava
cisrt@osu.cz | cisrt.osu.cz

16.04.2022



Obsah

1 Vymedzenie a členovia CSIRT OU	2
2 Úvod	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, národná a medzinárodná spolupráca	8
4.4 Pomoc s implementáciou národnej a európskej legislatívy	8
4.5 Ostatné	9
5 Rámcový plán na rok 2022	10



1 Vymedzenie a členovia CSIRT OU

- CSIRT OU má štatút pracovnej skupiny podľa opatrenia rektora 142/2021 (OU-43106/90-2021).
- Webová stránka CSIRT OU: csirt.osu.cz, anglická verzia: csirt.osu.eu.
- Kontaktný e-mail: csirt@osu.cz
- Hlásenie kybernetických bezpečnostných incidentov: security@helpdesk.osu.cz, alebo csirt@helpdesk.osu.cz
- Členmi skupiny CSIRT OU sú:
 - RNDr. Matej Zuzčák, Ph.D. (predseda),
 - Mgr. Bc. Jan Humpolík,
 - Tomáš Mazal,
 - Ing. Pavel Smolka, Ph.D (do 17.3.2022),
 - Ing. Pavel Pomezný,
 - Bc. Martin Stachura.
- CSIRT OU nemá vlastný rozpočet, drobné finančie pre možnosť základného fungovania poskytuje Katedra informatiky a počítačov (KIP), časť nevyhnutných nákladov kryje tiež Centrum informačných technológií (CIT) a spolupráca s úsekom manažéra kybernetickej bezpečnosti.
- CSIRT OU nemá priame výkonné právomoci a môže vydávať len odporúčania (najmä pri riešení bezpečnostných incidentov), pracovať v úlohe koordinátora a realizovať edukačné či výskumné aktivity, zaistovať národnú a medzinárodnú spoluprácu.
 - Detailný popis činností CSIRT OU obsahuje dokument RFC 2350¹.
 - CSIRT OU má od 30. augusta 2021 status „Accredited“² v medzinárodnej organizácii združujúcej CSIRT tímy najmä v EÚ.

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

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

2 Úvod

Pre CSIRT OU bol rok 2021 pomerne zásadný. Vo štvrtom roku svojho fungovania bolo prijaté nové opatrenie rektora o fungovaní CSIRT OU, ktoré zakotvilo reálnu spoluprácu medzi zložkami, ktoré sa podieľajúcimi sa na zaistovaní kybernetickej bezpečnosti univerzity. CSIRT OU tak mohol naplno začať riešiť v spolupráci s ďalšími subjektmi univerzity, ktoré spravujú informačné systémy a siete OU, kybernetické bezpečnostné udalosti a incidenty. K tomuto stavu výrazne dopomohlo i praktické napĺňanie Zákona o kybernetickej bezpečnosti (ZKB) a úzka spolupráca so všetkými verejnými vysokými školami v ČR v rámci CRP projektu Kyber-21.

Okrem prijatia nového opatrenia rektora sa CSIRT OU podarilo obsadiť všetky potrebné členské miesta. Túto pracovnú skupinu teda v súčasnosti tvoria jednak pracovníci priamo sa podieľajúci na manažovaní systémov OU, akademickí a vedeckí pracovníci, ale aj člen právneho oddelenia a samotný manažér kybernetickej bezpečnosti. Skupina sa pravidelne stretáva, bol vybudovaný komplexný systém pre riešenie, evidenciu a klasifikáciu zaznamenaných kybernetických bezpečnostných udalostí a incidentov, ktorý sa dlhodobo plánoval a vznikal veľmi dlhé obdobie.

Významným úspechom bolo v auguste 2021 získanie statusu „Accredited“ v rámci organizácie TF-CSIRT. Proces akreditácie zahŕňal nevyhnutný proces vnútorného usporiadania organizácie práce, prijatia interných dokumentov a nastavenia procesov. Akreditácia priamo dopomohla k posunu v práci CSIRT OU. Výrazný dopad má tiež na zisk nových informácií a spoluprácu s inými CSIRT tímmi.

Aj v roku 2021 ešte doznievala pandémia ochorenia Covid19. Napriek tomu sa nám už podarilo zrealizovať i prezenčné aktivity. No pokračovali i práce na rozvíjaní online aktivít - hlavne vzdelávacích kurzov.

Táto správa sumarizuje štvrtý rok fungovania CSIRT OU a predkladá víziu CSIRT OU pre rok 2022. Veríme, že vďaka ústupu pandémie, nutnosti implementácie ZKB a počiatocnému nastaveniu procesov, bude rok 2022 znamenať ďalší progres.

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 udalosti i incidenty, ku ktorým v rámci OU došlo a odporúča preventívne opatrenia.

- **Edukačná činnosť**

CSIRT OU realizuje systematické vzdelávanie a jednorazové 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 cielená školenia.

- **Výskum**

V intenzívnej spolupráci s Katedrou informatiky a počítačov Přírodovědeckej fakulty OU (KIP PřF OU) CSIRT OU vykonáva vedecký výskum založený napr. na technickej a štatistickej analýze zachytených kybernetických incidentov. Podielá 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.

- **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. stretnutia 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).

V súčasnosti sa jedná práve najmä o prácu na implementácii ZKB.

4 Realizované aktivity CSIRT OU

4.1 Riešenie kybernetických bezpečnostných incidentov

Rok 2021 bol štvrtým rokom fungovania CSIRT OU. Užívatelia systémov a siete OU hlásili udalosti a incidenty, ku ktorým dochádzalo v rôznej intenzite. Samozrejme nie všetky incidenty boli zachytené priamo našou skupinou. Systém hlásení bol významne inovovaný a od roku 2022 poskytne výrazne kvalitnejší prehľad. Zaznamenané incidenty v roku 2021 možno rozdeliť do nasledujúcich skupín:

- **Phishing a spam**

Ako obyčajne mnoho incidentov, ktoré boli hlásené CSIRT OU i v roku 2021 sa týkali, veľmi podobne ako v predošlých rokoch, 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. Keďže ide o dlhodobý problém, v danej veci sa snažíme pôsobiť jednak preventívne - vzdelávaním a tiež CIT neustále zdokonaľuje technické možnosti ochrany - antis-pam, aktívne blokovanie problematikých zdrojov na firewalle aj v rámci klient-ských bezpečnostných riešení.

V roku 2021 sme zaznamenali na univerzite i prípad tzv. vishingu (voice phishing), kedy zamestnanci univerzity čeliли pokusom o phishigový útok využitím priamych telefonických hovorov medzi útočníkom a nimi v anglickom jazyku. Útok bol však včas nahlásený a neboli zaznamenané žiadne škody.

- **Pracovné stanice infikované malwarom**

Ako každý rok aj v roku 2021 sme zaznamenali viacero infekcií koncových zariadení patriacich zamestnancom i študentom škodlivým kódom. V dvoch prípadoch sa jednalo o podozrenie na pripojenie zariadenia k botnetu. Často išlo i o súkromné zariadenia, ktoré sa pripájali na sieť napr. prostredníctvom siete Eduroam.

- **Porušovanie prevádzkových podmienok siete**

Počas roku 2021 boli hlásené - zväčša externými subjektmi i pokusy o šírenie nelegálneho obsahu (hlavne P2P siete), prípadne urážlivého obsahu, ktoré porušovali pravidlá používania siete. V tomto prípade sa jednalo o študentov, ktorí sa pripájali na sieť Eduroam zo svojich súkromných zariadení.

- **Zneužívanie zraniteľností softvérových produktov, ktoré využíva OU**

V roku 2021 sa objavilo niekoľko zraniteľností v softvérovom vybavení, ktoré je nasadené a používané na OU. Jednalo sa o zraniteľnosti v MS Exchange a zraniteľnosť Log4Shell. Keďže OÚ podľa ZKB spadá medzi subjekty regulované zo strany Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), oprávnené osoby museli postupovať podľa opatrení, ktoré táto organizácia vydala. Žiadne priame škody na našej infraštruktúre v spojitosti so zmienenými zraniteľnosťami neboli zaznamenané.

4.2 Edukačná činnosť

V mimoriadne dôležitej oblasti vzdelávania sme i počas roka 2021 zrealizovali niekoľko aktivít.

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

CSIRT OU sa už tradične - po štvrtý 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 sociálnych studií. Aj tento rok výhradne online formou, kedy sme daným fakultám poskytli online materiály. 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 nadálej publikované praktické články a návody pre zamestnancov a študentov OU i verejnosť (jedná sa hlavne o sekcie „Praktické rady“³ a „Aktuality“⁴).

- **Online Moodle kurzy pre zamestnancov a študentov OU**

CSIRT OU v spolupráci s CIT, pani kancelárkou OU a s poverencom GDPR pripravuje vzdelávacie online kurzy o základoch kybernetickej bezpečnosti na OU. Kurzy sú v súčasnosti vo finálnej fáze spracovávania a kurz pre všetkých zamestnancov OU by mal byť dostupný na začiatku nového akademického roku 2022/2023.

- **Prednáška o základoch bezpečného správania sa v kyber priestore pre študentov PřF**

CSIRT OU sa i tento rok zúčastnil na šírení osvety o základoch bezpečného správania sa v kyber priestore aj v rámci prednášky predmetu „Úvod do prírodných vied“ 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. Prednáška prebiehala prezenčne a súčasne bola i streamovaná naživo cez MS Teams. Záznam z minuloročnej podobnej prednášky (rok 2020) je k dispozícii v rámci OU Stream.⁵

- **Semináre NÚKIB**

Dňa 2.11.2021 navštívili našu univerzitu pracovníci NÚKIB, ktorí sa zúčastnili 2 seminárov. Jeden bol určený študentom KIP a druhý pracovníkom KIP a pozvaným hostom naprieč univerzitou.

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

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

⁵Prednáška o základoch kybernetickej bezpečnosti v rámci predmetu „Úvod do prírodných vied (11)“ - <https://web.microsoftstream.com/video/0e1a5fe3-6a77-4ba4-b9cc-a9b35551d7a3>

Témou diskusie so študentmi bola rola GovCERT tímu v ČR. Študenti sa aktívne zapojili i do diskusie o aktuálnych témach v oblasti kybernetickej bezpečnosti na národnej a medzinárodnej úrovni.

Seminár pre zamestnancov sa venoval téme aktuálnych hrozieb v českom kyberpriestore - hlavne hroznám z kategórie Ransomware-as-a-service (RaaS). Mnoho otázok však bolo i z oblasti aplikácie ZKB pre univerzity.



Obr. 1: Seminár na tému Rola GovCERT tímu v ČR.



Obr. 2: Seminár na tému Aktuálne hrozby v českom kyberpriestore.

4.3 Výskum, národná a medzinárodná spolupráca

Najvýznamnejšou aktivitou CSIRT OU v oblasti výskumu a medzinárodnej spolupráce bolo získanie statusu „Accredited“ v rámci organizácie TF-CSIRT. Procesu udeľenia akreditácie predchádzala niekoľkomesačná intenzívna príprava a potreba prijatia nového opatrenia rektora, zavedenie interných postupov a zlepšenie koordinácie pri spracovávaní kybernetických bezpečnostných udalostí a incidentov v spolupráci s CIT. Akreditácia bola udelená 30.8.2021. CSIRT OU je len druhým univerzitným akreditovaným CSIRT/CERT tímom v ČR. Viac informácií je možné nájsť v správe.⁶.



Obr. 3: Certifikát o akreditácii vystavený TF-CSIRT.

4.4 Pomoc s implementáciou národnej a európskej legislatívy

Zásadnou aktivitou v oblasti implementácie legislatívy bola v roku 2021 praktická implementácia Zákona o kybernetickej bezpečnosti 181/2014 Sb. (ZKB) a náležitých aplikačných vyhlášok: 316/2014 Sb., 317/2014 Sb. (so zapracovaním zmien z vyhlášky 360/2020 Sb.) a vyhláška 181/2014 Sb. Za týmto účelom vznikol v ČR CRP projekt Kyber-21 („Zvýšení úrovně kybernetické bezpečnosti v prostředí VVŠ“), kde sa zapojili takmer všetky verejné vysoké školy a OU bola jeho súčasťou. Projekt koordinovala Masarykova univerzita v Brne (MU) a jeho cieľom bolo pomôcť verejným vysokým

⁶Akreditácia CSIRT OU - <https://csirt.osu.cz/26441/csirt-ou-ziskal-prestizni-akreditaci/>

školám zvládnut' povinnosti vyplývajúce zo ZKB napr. zriadit' všetky potrebné roly pre koordináciu a riadenie kybernetickej bezpečnosti na univerzite, zmapovať aktíva a hlavne vybrať systémy, ktoré budú zaradené medzi tzv. významné informačné systémy (VIS), ktoré s ďalšími povinnosťami vysokých škôl spadajúce pod reguláciu NÚKIB, ktorý v tejto oblasti môže vykonávať i kontrolné audity.

Na univerzite teda intenzívne započal proces mapovania aktív, boli zvolené informačné systémy patriace medzi VIS, boli zriadené nevyhnutné roly pre riadenie kybernetickej bezpečnosti - hlavne manažér kybernetickej bezpečnosti a tiež sa pracuje na zriadení Výboru pre riadenie kybernetickej bezpečnosti a bol vykonaný i audit aktuálneho stavu. CSIRT OU priamo prispel do procesu jednak pripomienkováním a podieľaním sa na daných procesoch a tvorbe interných dokumentov (napr. nové smernice a opatrenia rektora), ale i vytvorením príručky o budovaní CSIRT tímu: „CSIRT tím v prostredí malej a strednej univerzity“.

4.5 Ostatné

V priebehu roku 2021 bol CSIRT tím de facto „nanovo“ vytvorený - prijatím nového opatrenia rektora 142/2021 (OU-43106/90-2021), ktoré prešlo náročným procesom a pripomienkováním počas jeho tvorby. Členská základňa CSIRT OU bola tiež zásadným spôsobom rozšírená. V súčasnosti má CSIRT OU vždy minimálne 6 členov, 2 členovia sú z akademického/výskumného prostredia z KIP. 2 členovia sú z CIT s priamymi výkonnými právomocami pri správe systémov a siete OU, členom je aj poverenec GDPR a zároveň právnik pre IT oblasť na OU a v neposlednom rade je členom i samotný manažér kybernetickej bezpečnosti na OU. Toto zloženie umožňuje veľmi adresne a operatívne konať a tiež určovať strategický smer smerovania kybernetickej bezpečnosti na OU.

Prijatých bolo tiež niekoľko interných smerníc pre fungovanie CSIRT OU - riešenie kybernetických bezpečnostných udalostí a incidentov a pre ich klasifikáciu. Tieto dokumenty predstavujú zásadný predpoklad pre efektívne fungovanie CSIRT OU a boli tiež nevyhnutné pre akreditáciu v rámci TF-CSIRT.

O celkovom fungovaní CSIRT OU, akreditácií i význame kybernetickej bezpečnosti na OU bol i rozhovor s predsedom CSIRT OU RNDr. Matejom Zuzčákom, Ph.D., dostupný na tomto odkaze.⁷..

⁷Rozhovor pre OU Live Kyberbezpečnost se týká každého z nás, říká předseda CSIRT OU Matej Zuzčák - <https://alive.osu.cz/hlavne-si-csirt-nepredstavujte-jako-pet-kouzelniku-rika-matej-zuzcak/>



Obr. 4: Členovia tímu CSIRT OU k 13.10.2021, zľava: Bc. Martin Stachura, RNDr. Matej Zuzčák, Ph.D. (vedúci tímu), Ing. Pavel Pomezný (manažér kybernetickej bezpečnosti), Mgr. Bc. Jan Humpolík (poverenec GDPR), Ing. Pavel Smolka, Ph.D.

5 Rámcový plán na rok 2022

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

- CSIRT OU bude aktívne pokračovať v dokončení aplikácie nevyhnutých procesov a zmie vyplývajúcich zo ZKB. Z atýmto účelom v roku 2022 bude pokračovať CRP projekt Kyber-22 pre všetky verejné vysoké školy, ktorý priamo nadviaže na CRP projekt z roku 2021 - Kyber-21.
- Vzdelávanie - edukačná činnosť zostane ako obyčajne medzi prioritami CSIRT OU aj v roku 2022. Predpokladané uvoľnenie reštrikcií ohľadom Covid19 nám pravdepodobne umožní aj realizáciu viacerých prezenčných vzdelávacích aktivít.
- Vnútorné aktivity - CSIRT OU bude stále pracovať na zlepšovaní vnútornej organizácie i na vzdelávaní členov tímu, prípadne zainteresovaných osôb napr. technikov na CIT.
- Pokračuje snaha o vybudovanie zaistenie situačného povedomia v sieti Ostravskej univerzity, v súčasnosti OU zvažuje nasadenie viacerých riešení pre monitorovanie siete. Ukončenie procesy obstarávania riešenia možno očakávať koncom roka 2022, alebo v roku 2023. Toto riešenie výrazne zlepší i možnosti výskumnej činnosti, na koľko bude predstavovať významný zdroj vstupných dát pre najrôznejšie analýzy.
- Zavedením systému pokročilej kategorizácie a evidencie kybernetických bezpečnostných incidentov a hrozieb by od roku 2022 mala byť súčasťou výročnej správy vždy podrobnejšia bilancia takto zaznamenaných udalostí a incidentov, ktorá bude vždy predkladaná i vedeniu OU.

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



COMPUTER SECURITY INCIDENT RESPONSE TEAM

