CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

BEZODPLATNÉ SLUŽBY VLÁDNEJ JEDNOTKY CSIRT PRE SUBJEKTY VEREJNEJ SPRÁVY

DÁTUM VYPRACOVANIA: 29.7.2025

KONTAKTNÉ INFORMÁCIE

CSIRT.SK

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

Sekcia kybernetickej bezpečnosti

Pribinova 25, Bratislava 811 05

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

Pribinova 25

811 05 Bratislava

SLUŽBY

Vládna jednotka CSIRT (VJ CSIRT) poskytuje subjektom verejnej správy Slovenskej republiky široké portfólio odborných služieb v oblasti kybernetickej bezpečnosti, ktoré sú poskytované bezodplatne. Cieľom týchto služieb je zvýšiť odolnosť organizácií voči kybernetickým hrozbám, zabezpečiť rýchlu reakciu na incidenty a podporiť prevenciu prostredníctvom zdieľania informácií, tréningu a technického hodnotenia zraniteľností.

Služby sú rozdelené do troch hlavných oblastí: **proaktívne služby, vzdelávanie a zvyšovanie povedomia** a **reaktívne služby**, ktoré spoločne tvoria ucelený rámec pre efektívne riadenie kybernetickej bezpečnosti v štátnych a verejných inštitúciách.

1. REAKTÍVNE SLUŽBY

Reaktívne služby poskytujeme v prípade, že už došlo ku kybernetickému incidentu. Ich cieľom je rýchlo identifikovať, eliminovať a zdokumentovať incidenty s cieľom minimalizovať škody a zabrániť ich opakovaniu.

1. **Riešenie incidentov**. Medzi priority VJ CSIRT patrí efektívne a koordinované riešenie kybernetických bezpečnostných incidentov v prostredí štátnej a verejnej správy. Naším cieľom je minimalizovať dopad incidentov na prevádzku inštitúcií a zároveň posilňovať ich odolnosť voči budúcim hrozbám. Incidenty riešime podľa jasne definovaného a štruktúrovaného procesu, ktorý zahŕňa celý životný cyklus incidentu – od jeho počiatočnej detekcie až po následnú analýzu a preventívne opatrenia. Súčasťou procesu je aj dôsledná dokumentácia celého priebehu incidentu, ktorá slúži nielen ako spätná väzba pre zúčastnené organizácie, ale aj ako cenný zdroj poznatkov pre zlepšovanie reakčnej schopnosti v budúcnosti. Viac informácií sa dočítate na: https://csirt.sk/nahlasit-incident.html

2. **Analýza škodlivého kódu**. VJ CSIRT poskytuje špecializovanú službu analýzy malvéru, ktorá zohráva zásadnú úlohu pri ochrane informačných systémov. V prípade potreby sa vykonáva analýza škodlivého kódu, ktorý bol buď nahlásený, alebo zachytený ako súčasť kybernetického incidentu. Cieľom je podrobne identifikovať druh, správanie a cieľ malvéru. Zisťuje sa, aké systémy škodlivý kód napáda, aké dáta ohrozuje a akým spôsobom sa šíri. Výsledky analýzy slúžia nielen na rýchle prijatie protiopatrení, ale aj na

zlepšenie pripravenosti verejných inštitúcií voči podobným hrozbám v budúcnosti. Zároveň sa získané poznatky zdieľajú v rámci bezpečnostného systému, čím prispievajú k celkovej odolnosti štátu proti kybernetickým útokom.

3. Digitálna forenzná analýza. VJ CSIRT poskytuje profesionálne služby v oblasti digitálnej forenznej analýzy v rámci kybernetických bezpečnostných incidentov. Náš tím vykonáva dôkladnú analýzu napadnutých systémov a zariadení s cieľom získať kľúčové dôkazy o aktivite útočníkov. Zameriavame sa najmä na odhalenie spôsobu prieniku do systému, identifikáciu rozsahu kompromitácie a vykonaných škodlivých aktivít. Podrobne analyzujeme, akým spôsobom sa útočník v prostredí pohyboval, aké techniky a nástroje použil, aké systémy či služby kompromitoval a aký vplyv mala jeho činnosť na dostupnosť, integritu či dôvernosť údajov. Na základe týchto zistení vytvárame presnú chronológiu incidentu a poskytujeme jasný obraz o jeho priebehu. Súčasťou je aj identifikácia nedostatkov, ktoré incident umožnili, a navrhnutie účinných technických aj organizačných opatrení na predchádzanie podobným incidentom v budúcnosti.

4. Pokročilá analýza a diagnostika hardvérových zariadení. VJ CSIRT nedávno rozšírila svoje kapacity o nové Laboratórium hardvérovej a dátovej analýzy. Nové pracovisko výrazne posilňuje technické možnosti tímu v oblastiach hardvérovej bezpečnosti, forenznej analýzy a dátového spracovania. Je vybavené 11 špecializovanými zariadeniami vrátane osciloskopu, spektrálneho analyzátora, termovíznej kamery či programátorov pamätí. Po ukončení prípravnej fázy bude expertný tím vykonávať činnosti ako extrakcia a analýza čipov z dosiek plošných spojov, dynamická analýza zberníc, získavanie firmvéru, detekcia podozrivého bezdrôtového vysielania či útoky bočnými kanálmi na testovanie odolnosti zariadení. Laboratórium bude slúžiť aj na vývoj nástrojov pre efektívnejšiu forenznú analýzu. Nové kapacity umožnia dôkladnejšiu diagnostiku hardvéru pri kybernetických incidentoch a prispejú k obnovovaniu dát z poškodených zariadení. Zriadenie laboratória zároveň otvára priestor na odbornú spoluprácu s národnými a sektorovými tímami CERT a CSIRT, ako aj s ďalšími špecializovanými štátnymi inštitúciami a organizáciami verejnej správy. Viac sa dočítate na: https://kyberportal.slovensko.sk/aktuality/vladna-jednotka-csirt-otvorila-nove...

2. PROAKTÍVNE SLUŽBY

Proaktívne služby sú zamerané na prevenciu. Pomáhajú identifikovať zraniteľnosti skôr, než sú zneužité, hodnotiť technický stav bezpečnosti organizácie a sprístupňovať informácie o aktuálnych hrozbách. Sú určené na podporu včasného prijatia opatrení a zvýšenia technickej odolnosti organizácií.

1. Achilles, služba (nielen) vyhľadávania zraniteľností. Achilles bol vybudovaný na odhaľovanie zraniteľností z pohľadu aktéra hrozieb útočiaceho z prostredia verejného internetu a ich centralizovanú správu. V systéme Achilles VJ CSIRT získava a spracováva informácie o zraniteľnostiach, informuje inštitúcie o zraniteľnostiach, ktoré sú detegovateľné z verejného internetu. Súčasťou tejto služby je modul Domino, ktorý slúži pre monitoring dostupnosti verejných webových služieb, teda ako systém včasného odhaľovania útokov vedúcich k nedostupnosti služby (angl. Denial of Service, DoS), distribuovaných útokov spôsobujúcich nedostupnosť služby (Distributed Denial of Service, DDoS) alebo technických výpadkov. Služba Achilles zabezpečuje plošné hodnotenie zraniteľností a je vhodné ju doplniť hĺbkovým hodnotením zraniteľností formou penetračného testovania. Súčasťou tejto služby je aj návod pre overenie úniku prihlasovacích údajov z Vašej domény (https://csirt.sk/sluzba-overenia-uniku-udajov.html). Viac o službe Achilles sa dočítate na: https://csirt.sk/registracia-achilles

2. Ares, služba (nielen) penetračného testovania. Predstavuje službu hĺbkového hodnotenia zraniteľností formou penetračného testu a overenie súladu s tzv. CIS benchmark. Zameriava sa najmä na penetračné testovanie webových aplikácií (white-box, grey-box alebo black-box) ale aj externý penetračný test. Pri testovaní formou white-box sa jedná o testovanie zraniteľností s prístupom ku zdrojovému kódu. Zdrojový kód spolu s používateľskými účtami so všetkými rolami, ktorých oprávnenia sú súčasťou testov, je nutné poskytnúť pred vykonaním samotného penetračného testu. Podmienkou vykonania penetračného testovania je uzatvorenie písomnej dohody o penetračnom testovaní medzi MIRRI a Vašou organizáciou, v ktorej sa bližšie dohodne najmä predmet testovania a podmienky výkonu testovania, a následne podanie záväznej žiadosti o výkon penetračného testovania. Viac sa dočítate na: https://csirt.sk/registracia-ares.html

3. Afrodita, služba zdieľania informácií o hrozbách. Subjekty verejnej správy používajúce túto službu získajú na pravidelnej báze prístup k informáciám o indikátoroch kompromitácie z aktuálneho diania v kybernetickom priestore. Môžu

tak overovať prítomnosť indikátorov kompromitácie (angl. Indicators of Compromise, IoC) vo svojej infraštruktúre, alebo nasadiť preventívne opatrenia, aby predišli pokusom o vykonanie predmetného útoku. Navyše si subjekty môžu dané IoC korelovať s inými udalosťami v inštancii MISP „Afrodita“, čím je možné rozšíriť kontext samotných IoC, ale aj celej udalosti. V neposlednom rade je táto služba spojená s možnosťou ukladať si dané IoC v nástroji, ktorý slúži práve na prácu s IoC a ich zdieľanie. MISP „Afrodita“ je pravidelne doplňovaný o nové udalosti a IoC z aktuálneho diania v kybernetickom priestore od oddelenia Cyber Threat Intelligence (CTI) VJ CSIRT, čo zaručuje zlepšenie prehľadu a lepšiu prípravu na potenciálne hrozby u konštituentov. Viac sa dočítate na: https://csirt.sk/registracia-afrodita.html

3. ZVYŠOVANIE POVEDOMIA O KYBERNETICKEJ BEZPEČNOSTI A ODBORNÝ TRÉNING

Vzdelávanie a osvetové aktivity tvoria kľúčový pilier obrany proti kybernetickým hrozbám. Rozširovanie znalostí a budovanie povedomia u zamestnancov znižuje riziko chýb, zvyšuje schopnosť včas reagovať na incidenty a prispieva k celkovej kultúre bezpečnosti.

1. **Tabletop cvičenia z oblasti informačnej bezpečnosti v rámci Výcvikového a školiaceho strediska (VaŠS), Kyberaréna**. Výcvikové a školiace stredisko pre bezpečnosť prevádzky a správy IT pre sektor verejnej správy je vybavené potrebnými informačnými a komunikačnými technológiami (IKT) a spĺňa moderné štandardy pre špecializovaný výcvik v oblasti informačnej a kybernetickej bezpečnosti. Umožňuje realizáciu špecializovaných výcvikov v oblasti kybernetickej bezpečnosti so zameraním pre zamestnancov štátnej a verejnej správy. Tabletop sú cvičenia, na ktorých sa členovia tímu stretávajú v neformálnom, riadenom prostredí, aby riešili úlohy podľa zadaných scenárov a mohli si otestovať koordináciu, procesy a komunikáciu. Súčasťou cvičenia je mix niekoľkých scenárov, ktoré si môžu používatelia vybrať. Pre registráciu na Tabletop cvičenie môžete použiť nasledujúci odkaz: https://kyberarena.csirt.sk/registracia/

2. **Technické cvičenia v rámci VaŠS, Kyberaréna**. Kybernetické hrozby sa neustále vyvíjajú a preto je potrebné pravidelne trénovať technický tím, aby bol v prípade potreby pripravený zasiahnuť. Školenie v rámci Kyberarény ponúka dynamické prostredie, kde sa účastníci môžu zapojiť do viac ako 70 scenárov, v ktorých musia riešiť kybernetické útoky a incidenty ako napríklad DoS, ransomvér, podvrhnuté phishingové emaily a škodlivé prílohy. V rámci tímu spolupracujú s kolegami na odhalení, zdokumentovaní a mitigácii incidentu pri ochrane infraštruktúry simulovanej organizácie. Hlavným cieľom je rozvoj technických, tzv. hard-skills, tímová spolupráca, reakcia na incidenty, práca v časovej tiesni a možnosť vyskúšať si rôzne bezpečnostné nástroje. Pre registráciu do Kyberarény môžete použiť nasledujúci odkaz: https://kyberarena.csirt.sk/registracia/

3. **Vzdelávacie prezentácie tém kybernetickej bezpečnosti** sú určené pre zamestnancov verejnej správy, ale aj študentov a pedagógov. Budovanie všeobecného povedomia v oblasti informačnej bezpečnosti prebieha najmä formou diskusných prednášok. Jednotlivé témy prezentácie sú voliteľné podľa potrieb a požiadaviek daného subjektu. Štandardom je však predstavenie základov z každej témy pre celkovú informovanosť publika a následný hlbší výklad pre

zvolené témy. Počas prezentácií je publikum nabádané k aktívnej participácii na výklade formou dialógu a príkladov s ktorými sa stretáva na dennej báze. VJ CSIRT ponúka možnosť klásť otázky aj anonymnou formou pre obzvlášť citlivé témy. Pre registráciu na vzdelávaciu prezentáciu môžete použiť nasledujúci odkaz: https://kyberarena.csirt.sk/registracia/

4. **Publikačná činnosť** slúži ako komunikačný kanál pre konštituenciu VJ CSIRT, no taktiež pre širokú verejnosť. Výsledkom úzkej spolupráce analytického a vzdelávacieho oddelenia sú publikácie varovaní a tlačových správ o súčasných hrozbách v kybernetickom priestore, ktorými VJ CSIRT informuje verejnosť o aktuálnom dianí. Tieto publikácie sú dostupné na webovom sídle VJ CSIRT (https://csirt.sk/index.html) a v sekcii **Naše publikácie** (https://csirt.sk/dokumenty.html), **Metodiky a návody** (https://csirt.sk/rady-a-navody.html) a sú určené najmä pre správcov a prevádzkovateľov IT služieb v konštituencii VJ CSIRT ale aj odbornej verejnosti.

Ak ste organizácia verejnej správy a máte záujem o niektorú z vyššie uvedených služieb, kontaktujte nás prostredníctvom oficiálneho formulára na stránke https://www.csirt.sk. Naším cieľom je budovať odolné, informované a bezpečné inštitúcie, ktoré sú pripravené čeliť kybernetickým výzvam dneška aj zajtrajška.

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Informačný dokument vypracovaný

CSIRT.SK

Všeobecný kontakt

info@csirt.sk

Služby CSIRT.SK

MISP AFRODITA

ACHILLES

CTI

ARES by CSIRT.SK ATTACK TO PROTECT

KYBER ARENA