Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

CSIRT.SK

Všeobecné informácie o publikačnej činnosti

Varovania, mesačné správy, mesačné prehľady kritických a závažných softvérových zraniteľností, metodiky a návody

od **VJ CSIRT**

Publikačná činnosť

Vládna jednotka CSIRT („VJ CSIRT“) sa zameriava aj na publikačnú činnosť, ktorá predstavuje kľúčový pilier pre zdieľanie overených znalostí v oblasti kybernetickej bezpečnosti prostredníctvom verejných kanálov. Publikačná činnosť spočíva v systematickom vyhľadávaní, zbere, analýze a komplexnom spracovaní informácií o kybernetických hrozbách. Výsledkom sú včasné bezpečnostné varovania, ako aj prehľadové mesačné správy, prehľady kritických a závažných softvérových zraniteľností, metodiky a návody.

Týmto spôsobom VJ CSIRT aktívne formuje bezpečnejšie digitálne prostredie a zvyšuje celkové povedomie o aktuálnych rizikách. Výstupy jej publikačnej činnosti tak poskytujú ostatným organizačným zložkám, štátnym inštitúciám, orgánom verejnej moci, ale aj širokej verejnosti spoľahlivú vedomostnú základňu postavenú na profesionálnej úrovni.

Varovania

VJ CSIRT pravidelne vydáva bezpečnostné varovania, ktoré poukazujú na novonájdené kritické a vysoko závažné softvérové zraniteľnosti a s nimi spojené bezpečnostné aktualizácie a záplaty, kampane, útoky, či šíriaci sa škodlivý kód. Pre IT administrátorov a vývojárov v štátnom a verejnom, ale i súkromnom sektore predstavujú tieto informácie nástroj, ktorý im umožňuje okamžite zaplátať kritické diery v systémoch skôr, než môže dôjsť ku kompromitácii ich infraštruktúry.

Mesačné správy CSIRT.SK

Mesačné správy prinášajú prehľad kľúčových udalostí zo Slovenska aj zo zahraničia, ktoré formovali uplynulé obdobie. Popisujú útoky a kampane zasahujúce konštituenciu VJ CSIRT, a tiež prehľadovo mapujú sofistikované kampane rôznych APT skupín, ale i jednotlivcov, ktoré sú zamerané na krádež citlivých dát či infiltráciu do firemných sietí alebo kompromitáciu celej infraštruktúry. Prehľadné zhrnutie najdôležitejších udalostí mesiaca poskytne komplexný pohľad na aktuálne dianie na domácej, ale i zahraničnej pôde.

Mesačné prehľady kritických a závažných softvérových zraniteľností

Mesačné prehľady kritických a závažných softvérových zraniteľností poskytujú ucelený prehľad o kritických, prípadne závažných zraniteľnostiach, ktoré boli za daný mesiac objavené v najdôležitejšom softvéri využívanom našou konštituenciou. Informujú tiež o zraniteľnostiach, opravách, ale i odporúčaniach týkajúcich sa operačných systémov Microsoft, balíka MS Office, internetových prehliadačov, nástroja Adobe Acrobat a Reader, niektorých vývojárskych frameworkov a prehľadu iných závažných zraniteľností riešených v danom mesiaci.

Metodiky a návody

VJ CSIRT sa zameriava aj na publikáciu metodík a návodov, ktoré sú navrhnuté tak, aby pomohli jednotlivcom a organizáciám zvýšiť úroveň zabezpečenia. Materiály pokrývajú rôzne témy od základných princípov kybernetickej bezpečnosti cez postupy pre efektívne zabezpečenie IT infraštruktúry.

Publikované technické návody a odporúčania poskytujú praktický prehľad o používaní, konfigurácii a zabezpečení IKT infraštruktúry – od koncových staníc (desktopov, notebookov) až po servery. V danej časti sú podrobne spísané technické návody a materiály o PGP šifrovaní e-mailov a súborov, o AI a strojovom učení, o webových službách, o podozrivých e-mailoch a cloude, o operačných systémoch, o bežných softvérových produktoch a o zvyšovaní informačnej a kybernetickej bezpečnosti, či už o tom, prečo je ukladanie hesiel do prehliadača nebezpečné alebo o tom, prečo je dobré používať manažéra hesiel (napr. KeePass).

Publikované metodiky a hardening poskytnú koncovému používateľovi prehľad o systematickom zabezpečení organizácií verejnej správy v oblasti informačnej bezpečnosti, ktorý sumarizuje minimálne opatrenia potrebné na zabezpečenie informačných systémov a infraštruktúry organizácie so zvýšenými požiadavkami na bezpečnosť. V danej časti sú podrobne spísané príručky pre hardening OS Windows a OS Linux, príručka o ochrane pred útokmi DDoS, ale aj mnohé iné.