# Výpadek zařízení s OS Windows v důsledku aktualizace EDR nástroje CrowdStrike Falcon

portal.nukib.gov.cz/intra/informacni-servis/analyzy-a-prehledy/analyticke-vystupy/vypadek-zarizeni-s-os-windows-v-dusledku-aktualizace-edr-nastroje-crowdstrike-falcon

## Co se stalo?

**V pátek 19. července 2024 zasáhl širokou škálu zařízení s operačním systémem Windows po celém světě problém způsobující nefunkčnost těchto zařízení, konkrétně kolaps operačního systému do tzv. BSOD (blue screen of death) a následné neschopnosti se spustit.** Za vznikem stála chyba v aktualizaci Endpoint Detection and Respone (EDR) nástroje CrowdStrike Falcon®. Společnost CrowdStrike během několika hodin chybnou aktualizaci stáhla a vydala návod na opravu, který zahrnoval lokalizaci a postup pro odstranění problematického souboru. Ačkoliv byla oprava principiálně jednoduchá, zasažené zařízen bylo třeba manuálně spustit v bezpečném režimu. To znamenalo, že bylo třeba každé toto zařízení opravit individuálně, což výrazně prodloužilo dobu a dopady výpadku. Některé zasažené organizace se potýkaly s následky ještě následující pondělí.

## Proč se to stalo?

CrowdStrike Falcon® je EDR nástroj pro detekci hrozeb na koncových bodech a reakci na ně. Jeho úkolem je monitorovat procesy v zařízeních, na kterých je nainstalován, a hledat známky škodlivé činnosti (například malwaru). Když zjistí něco podezřelého, pomůže hrozbu zablokovat. Pro výkon svojí práce má nástroj významná privilegia k přístupu do citlivých procesů zařízení. CrowdStrike Falcon® běží na úrovni kernel, díky čemuž má neomezený přístup k systémové paměti a hardwaru. To bylo

důvodem, proč při nekompatibilitě aktualizace s OS Windows nedošlo pouze k selhání samotného nástroje, ale celého operačního systému.

Pro detailnější pochopení příčiny výpadku je třeba uvést kontext o fungování Falconu. Každý nasazený Falcon senzor živě sleduje aktivity na lokálním stroji a za použití dalších vstupů vyhodnocuje data a tvoří behaviorální IOAs (indicators of attack). Tyto informace jsou kontinuálně tvořeny a obohacovány za pomocí porovnávání vícero vstupů, kdy vedle lokálního obsahu ze senzoru (záznam o aktivitách atd.) figuruje tzv. Rapid Response obsah, který je čerpán z cloudu. Umožňuje rozšiřování nových detekcí a prevencí na senzoru, aniž by bylo nutné pokaždé měnit jeho kód. Rapid Response Obsah je vždy doručován skrze soubory známé jako „channel files“, kde ke každému náleží též právě jeden Template Type. Jde o formulář psaný v kódu, jež analytikům umožňuje rychle reagovat a za pomocí definovaných vstupních parametrů popsat danou hrozbu Falcon senzoru.

V reakci na nové typy útoků zneužívající named pipes a jiné funkce zajišťující interprocesní komunikace „IPC“ CrowdStrike vydal v únoru 2024 novou verzi senzoru 7.11, která představila nový IPC Template Type. Tento nový Template Type doručený skrze channel file 291 bohužel obsahoval logickou chybu, jelikož definoval 21 vstupních parametrů, přičemž kód sahající do channel files měl nadefinováno pouze 20 vstupních parametrů, se kterými měly korelovat. Samotná logická chyba měla dopad až 19. července, kdy byly skrze channel files 291 do produkce nahrány další IPC Template Types, které jako první vyžadovaly porovnání 21. parametru, který od senzoru nebyl poskytnut. Nastala situace známá jako **out-of-bounds memory read**, kdy se kód snažil nahrát neexistující data z paměti senzoru, což vedlo k pádu operačního systému. Na vině byl konkrétně channel file `C-00000291*.sys`.

## Jaké byly dopady?

**Zasaženy byly organizace napříč kontinenty, nicméně dopady v ČR byly nízké.** NÚKIB situaci monitoroval a poskytoval podporu. Podle společnosti Microsoft bylo výpadkem poznamenáno přes osm a půl milionu zařízení, což je méně než jedno procento všech zařízení s OS Windows. I přesto se jedná o doposud největší IT výpadek v historii. V tuto chvíli však není ještě možné vyčíslit přesné škody, a ani za kolik z nich může být společnost CrowdStrike vedena k zodpovědnosti.

Ačkoliv výpadek zasáhl lékařská zařízení a další kritickou infrastrukturu, v současnosti nic nenasvědčuje tomu, že by byl někdo v jeho důsledku významně ohrožen na zdraví či životě. Vyčíslit konečné finanční dopady výpadku bude trvat ještě dlouho a nemusí být nikdy definitivní, jelikož výpadek způsobil řadu dalších sekundárních problémů, u kterých je sporné vyhodnotit podíl příčiny.

Pojišťovací společnost Parametrix odhaduje, že jen v tzv. Fortune 500 (žebříček 500 největších amerických společností dle hrubého obratu) dosáhnou škody 5,4 miliardy dolarů (v přepočtu zhruba 127 bilionů korun)

Akcie společnosti CrowdStrike, které se v roce 2023 více než zdvojnásobily, od výpadku klesly o více než 24 %, a v době psaní článku dále klesají v reakci na fakt, že první velká zasažená firma, americké aerolinky Delta Airlines, začala vyžadovat po společnosti Microsoftu a CrowdStrike odškodné. Poškozeny byly organizace využívající software CrowdStrike Falcon napříč sektory. S nejvýznamnějšími dopady se potýkaly aerolinky. Dál byly zasaženy např. televizní stanice, objednávkové systémy k lékařům, samoobslužné pokladny, bankovní služby nebo železnice.

**NÚKIB na celou situaci proaktivně reagoval skrze mapování dopadů výpadku v rámci České republiky a komunikoval se subjekty spadajícími pod zákon č. 181/2014 Sb, o kybernetické bezpečnosti.** Podle dostupných informací bylo zasaženo pouze minimum oslovených subjektů, což reflektuje odhady společnosti

Microsoft. NÚKIB dále informoval o možnostech nápravy prostřednictvím svých webových stránek, Portálu NÚKIB a průběžně také prostřednictvím účtu vládního CERT týmu na síti X.

## Implikace v kybernetické bezpečnosti

V současnosti není důvod se domnívat, že by se jednalo o cílený útok. Okolnosti problému jsou v tuto chvíli již známé a nic nenasvědčuje jiné příčině, než pochybení ze strany společnosti CrowdStrike. Přesto má tato událost implikace v rovině kybernetické bezpečnosti.

Krátce po události začali útočníci zneužívat situace v jiných škodlivých kybernetických aktivitách. Jedná se zejména o podvodné e-maily či telefonáty, ve kterých se podvodníci vydávají za zaměstnance společnosti CrowdStrike, případně za nezávislé výzkumníky nabízející technickou pomoc. Hlavním cílem podvodníků je přesvědčit oběť, aby nainstalovala malware, který poskytují pod záminkou, že se jedná o opravný nástroj nebo skript, který má pomoci vyřešit výpadek nebo jeho možné dopady. Před vlnou takových phishingových aktivit varovala přímo společnost CrowdStrike a její zjištění se shodují s veřejně dostupnými zdroji i informacemi od partnerů NÚKIB. **Podle nám dostupných informací je výpadek zneužíván jak kyberkriminálními, tak státem sponzorovanými aktéry, jako například íránským Yellow Dev 31** (též známým jako Void Manticore).

Otázkou, kterou nastalá situace zvedla, je rovněž úroveň přístupu kyberbezpečnostních produktů třetích stran k citlivým funkcím operačních systémů. Společnost Microsoft dala v reakci na tento incident najevo, že zvažuje omezení přístupu produktů třetích stran do jádra Windows, stejně, jako to například dělá společnost Apple ve svých operačních systémech. Obzvlášť tato situace ilustruje rizika zneužitelnosti dodavatelských řetězců, protože poukazuje na to, jak bezprecedentní přístup některé společnosti mají ke klíčovým

systémům a jak daleko by se mohl útočník dostat kompromitací jejich dodavatelské řetězce, například „pouhou“ škodlivou aktualizací.

## Prevence obdobných výpadků

Jednotlivé společnosti by měly mít v rámci prevence připravené plány kontinuity, vč. plánů obnovy, své infrastruktury, jednotlivých zařízení a služeb, které poskytují. V rámci těchto plánů by měla mít organizace zejména přehled o prioritách obnovy, závislostech jednotlivých částí infrastruktury a potřebných zdrojů pro obnovu (např. lidské zdroje, dodavatelé, výpočetní technika). Tyto plány by měly vycházet ze stanovených cílů kontinuity činnosti a určených hodnot RTO (Recovery Time Objective) a RPO (Recovery Point Objective), které mohou v praxi vycházet např. ze stanovených SLA (Service Level Agreement) se zákazníky.

Dalším doporučením v oblasti prevence proti výpadkům je zavedení funkčních procesů v oblastech řízení změn, projektového řízení, řízení zranitelností a nasazování bezpečnostních záplat a aktualizací, které je v rámci tzv. „best-practice“ vhodné nastavit. Jedná se např. o testování plánovaných změn, postupné nasazování změn (tzv. staging) vč. připravenosti pro případy tzv. „rollback“ scénáře, bezpečnostní testování (skenování zranitelností, penetrační testy a jiné), včasné aplikování záplat na známé zranitelnosti. Ovšem, jak jsme byli svědky tohoto ojedinělého a velice specifického kybernetického bezpečnostní incidentu, ani tato opatření nemusí být dostatečná.

Jakmile organizace disponuje výše uvedenými plány, procesy a postupy pro obnovu a řízení změn, je také potřeba mít zajištěnou technickou stránku prevence. Jedna z významných technických oblastí je zajištění dostupnosti, které docílíme pomocí pravidelného zálohování informací, dat a konfigurací (vč. nastavení) nástrojů a zařízení.

Přestože většina organizací je v domnění, že jejich systém zálohování je funkční a procesy v případě dopadu kybernetického bezpečnostního incidentu jsou nastaveny dobře, jedná se často pouze o iluzi. V praxi je mnohdy tato preventivní stránka opomíjena a k reálnému použití připravených organizačních i technických postupů dochází až při reálném incidentu. Je nutné nastavené procesy a plány pravidelně testovat, aktualizovat a upravovat na základě zpětné vazby z těchto testování.

## Doporučené zásady při zálohování

Pro zajištění kvalitní dostupnosti je nutné dodržovat několik pravidel zálohování, konkrétní implementace a zvolená řešení ale vždy záleží na organizaci a typech dat se kterými pracuje.

### Pravidlo 3-2-1

Vytvářet alespoň 3 kopie dat, které jsou následně uloženy na alespoň 2 typy zálohovacích médií a alespoň jedna kopie se nachází na bezpečném místě mimo organizaci a její síť.

### Neaktivní záloha

Alespoň jedna záloha musí být uložena v neaktivním (offline) stavu, tedy na externích discích nebo datových páskách. Neaktivní zálohování umožňují i někteří poskytovatelé cloudů.

### Obnovitelnost

Pro obnovování ze záloh musí existovat jasný technický proces a obnovování ze záloh je nezbytné pravidelně testovat, aby organizace věděla, zdali je zálohovací systém v praxi použitelný a relevantní osoby ví, jak s těmito systémy pracovat. Obnovování ze záloh by mělo být co nejvíce automatizované.

### Pravidelnost

Zálohy je nutné provádět pravidelně, opět je potřebné mít pro vytváření záloh proces a ideálně mít co nejvíc částí zálohování automatizován.

### Segmentace

Prostředí pro zálohování by mělo být vhodně odděleno od zbytku organizace a to včetně speciálních administrátorských účtů určených pouze pro zálohování.