Ako sa vysporiadať s Ripple 20?

Cieľom tohoto dokumentu je poskytnúť priemyselným podnikom stručný návod, ako reagovať na riziká súvisiace s rodinou zraniteľností Ripple 20. Ripple 20 je súbor 19 zraniteľností v softvérovej knižnici na obsluhu sieťových protokolov TCP/IP. „Deravá" knižnica od spoločnosti Treck je použitá v produktoch približne stovky dodávateľov, a vyskytuje sa v stovke miliónov zariadení po celom svete. **Zariadenia s týmito zraniteľnosťami sa vo významnom množstve nachádzajú aj v slovenských podnikoch a firmách, čo znamená, že priemyselné systémy dnes nie sú voči nim dostatočne odolné. Zraniteľnosti umožňujú útočníkom získať plnú kontrolu nad zariadeniami, upraviť ich správanie, vyradiť z prevádzky, či použiť ako odrazový mostík k ďalším útokom vo vnútornej sieti.**

Viac informácií o zraniteľnostiach Ripple 20

Ako reagovať na riziká súvisiace s rodinou zraniteľností Ripple 20

Krok č. 1 - Identifikovať rozsah, či a kde sa zraniteľnosti Ripple 20 vo firme vyskytujú

Prvým krokom by mala byť identifikácia, akých komponentov, systémov či zariadení, ktoré firma vlastní či používa, sa Ripple 20 týka. To je možné niekoľkými spôsobmi:

- **Manuálne** - V ideálnom prípade existuje v spoločnosti presná a aktuálna evidencia všetkých aktív a technológií, ktorá obsahuje informácie o ich výrobcoch a konkrétnych používaných verziách. Dôležité je, aby tento zoznam obsahoval nielen kritické, ale všetky aktíva, pretože aj tie môžu po narušení fungovať ako „prestupná" stanica do zvyšku siete (napríklad to môže byť bežná tlačiareň). Pri manuálnej analýze je tento zoznam nutné porovnať s publikovanými zoznamami zraniteľných produktov, dostupných na https://www.jsof-tech.com/ripple20/ Vzhľadom na rozsah a absenciu štruktúrovaných dát ide o nevyhnutný, no náročný a zdĺhavý proces.

- **Skenovaním -** Ak inventarizácia absentuje alebo sú pochybnosti o aktuálnosti zoznamu používaných produktov a ich verzií, je alternatívou detekcia zraniteľnosti aktívnym skenovaním pripojených zariadení. Skenovanie identifikuje zraniteľné zariadenia na základe špecifických atribútov v ich sieťovej komunikácii, a preto je nutné ho realizovať v rámci infraštruktúry, do ktorej sú pripojené. Vyžaduje si to adekvátne technické znalosti a detekčné nástroje.

- **Prostredníctvom dodávateľov** – Ak sú informačné či prevádzkové technológie úplne alebo čiastočne pod správou externých dodávateľov, je nevyhnutné sa s otázkami obrátiť na nich a vyžiadať si stanovisko, ako sa zraniteľnosti Ripple 20 týkajú častí, za ktoré sú zodpovední. Každý takýto dodávateľ by mal hodnoverným spôsobom doložiť, ako sa ubezpečil o tom, že zraniteľnosti Ripple 20 v spravovanej infraštruktúre neexistujú.

Krok č.2 - Identifikovať dopad na zariadenia, technológie, systémy, a zvoliť nápravné opatrenia

Výstupom z prvého kroku by mal byť zoznam aktív (zariadení, systémov, technológií), v ktorých je potvrdená zraniteľnosť z rodiny Ripple 20. V ďalšom kroku je nutné vyhodnotiť pravdepodobné scenáre, akým spôsobom by mohla byť daná zraniteľnosť na danom zariadení zneužitá. Ako metodiku pre toto vyhodnotenie rizík je možné použiť buď skupinu štandardov ISO 27005 alebo aj ISA 62443.

- Významným vstupom pre analýzu rizík je určenie akceptovateľnej miery rizika – t.j. hranice, ktorú ešte toleruje vlastník rizika (štatutár spoločnosti, resp. osoba, na ktorú on túto zodpovednosť delegoval).
- Na základe úrovne akceptovateľného rizika je možné určiť vhodné a dostatočné opatrenia. Scenárov pre zníženie rizika je často viacero, a je potrebné zvoliť ten, ktorý spĺňa okrem zníženia miery rizika aj iné parametre (napr. výšku nákladov, schopnosti a vyťaženie zamestnancov, dostupnosť externých pracovníkov a pod...).
- Ideálne je pri určovaní dopadov aj plánovaní opatrení spolupracovať s dodávateľmi / výrobcami daných technológií. Určite sa odporúča zistiť, či výrobca zverejnil novšie verzie daného softvéru alebo firmvéru, o ktorých deklaruje, že v nich zraniteľnosti Ripple 20 boli odstránené.
- V prípade, že nie je možné aplikovať opatrenia na elimináciu zraniteľnosti (napr. nie je možný upgrade z dôvodu závislosti na konkrétnej verzii), je potrebné naplánovať a aplikovať

kompenzačné opatrenia, ktoré zmiernia (napr. iné zabezpečenie na úrovni siete) alebo presunú riziko (napr. poistenie dopadov pri zneužití či výpadku dotknutého systému).
- V rámci plánovania opatrení je dôležité aj určenie priorít – ktoré opatrenia (aktualizácie, nastavenia, sieťové zmeny a pod.) aplikovať v akom poradí. Po aplikácii každého z opatrení by bolo potrebné pretestovať bežnú funkčnosť systémov a zariadení.

Krok č. 3 - Zrealizovať nápravné opatrenia

Nakoľko zraniteľnosťami Ripple 20 je dotknuté značné množstvo zariadení mnohých výrobcov, je možné očakávať, že aj opravných opatrení, ktoré bude nutné zrealizovať bude mnoho, a budú vyžadovať dlhší čas na implementáciu. Odporúčame preto:

- Sledovať dotknuté systémy a podozrivé správanie v nich, ktoré by mohlo znamenať ich zneužitie / narušenie ešte pred aplikovaním opráv (napr. reštarty, zmeny konfigurácie, neobvyklé sieťové spojenia, špecifické znaky v sieťovej komunikácii, atď.).
- Vypracovať presný plán a postup riadenia zmien, ako zrealizovať jednotlivé opatrenia, ktoré boli určené v predošlom kroku.
- Pri plánovaní dbať na dobre definované kompetencie, zodpovednosti a vlastníkov, ktorí budú strážiť riziká pri implementácii opatrení a súvisiacich udalostiach (napr. odstávkach systémov a pod.). Prirodzene, v malej alebo strednej firme bude vlastníkov/správcov systémov len zopár, a títo ľudia budú projektom odstránenia zraniteľností Ripple 20 určitú dobu zaťažení.
- Ak je to možné, otestovať a odladiť zmenu – plánované opatrenie najprv mimo produkčných systémov (napr. na záložných zariadeniach/systémoch).
- Mať pripravený „rollback“ plán - postup krokov, ktoré sa budú realizovať, ak by zmena neprebehla úspešne (napr. ako sa vrátiť k predošlej verzii či konfigurácii).
- Je veľmi dôležité skoordinovať aj komunikačné plány pre výpadky/odstávky systémov, ktoré sú danou zmenou dotknuté.
- Spolupracovať s dodávateľmi resp. tretími stranami, ak ide o systémy, ktoré sú dodávané ako celok “na kľúč” alebo sú pod ich výlučnou správou.
- Priebežne dokumentovať vykonávané činnosti, aby v prípade, že sa až s odstupom času objavia poruchy funkčnosti systémov, bolo možné rekonštruovať, či tieto poruchy môžu súvisieť s vykonanými opatreniami.
- Vedľajším efektom celej akcie by mal byť dôležitý benefit – lepšia dokumentácia verzií používaných softvérov a firmvérov.

Krok č.4 - Revidovať proces pre identifikáciu zraniteľností a aplikovanie opatrení na základe týchto skúseností

Ripple 20 je svojím rozsahom a výskytom výnimočnou udalosťou, no zraniteľnosti a kybernetické hrozby nie sú ničím novým, neustále pribúdajú nové, a budú aj naďalej. Na základe skúseností s popísanými krokmi odporúčame revidovať proces, ktorý pomôže spoločnosti vysporiadať sa s podobnými hrozbami v budúcnosti. Mal by obsahovať:

1. **Zachytávanie hrozieb a zraniteľností** - Aktívny monitoring informácií o hrozbách a zraniteľnostiach a práca so zisteniami.
2. **Identifikácia rozsahu** - Schopnosť efektívne identifikovať zasiahnuté komponenty v infraštruktúre.
3. **Určenie dopadu a voľba opatrení** - Schopnosť vyhodnotiť dopad a riziko pre jednotlivé zasiahnuté komponenty, a voľba primeraných opatrení.
4. **Vykonanie nápravných opatrení** - Implementácia bezpečnostných opatrení riadeným spôsobom v spolupráci s dodávateľom technológie.

Záverom

Uvedomujeme si, že realizácia popísaných krokov môže v mnohých prípadoch byť nad rámec kapacít vlastných IT špecialistov, a preto ponúkame sprostredkovanie odbornej pomoci s ktorýmkoľvek spomínaným krokom (prostredníctvom členov AKB, resp. na komerčnej báze). Kontakt na špecialistov dočasného tímu AKB je možný cez kontaktný formulár na adrese: https://www.akb.sk/ripple-20-contact/

Členmi dočasného tímu AKB sú:
Dávid Dvořák (david.dvorak@soitron.com)
Marián Trizuliak (marian.trizuliak@outlook.com)
Tomáš Zaťko (tomas.zatko@citadelo.com)
Martin Lohnert (martin.lohnert@voidsoc.com)