KERNUN

2,5 milionu zastavených útoků ve zdravotnictví

Případová studie nasazení zařízení KERNUN v Centru kardiovaskulární a transplantační chirurgie

36 580	22 541	10 676
zastavených unikátních útočníků	zablokovaných nebezpečných spojení z interní sítě	zastavených účtočníků denně

Centrum kardiovaskulární a transplantační chirurgie (CKTCH) Brno je státní příspěvkovou organizací v přímé působnosti Ministerstva zdravotnictví České republiky. Poskytuje vysoce specializovanou **zdravotnickou péči** zahrnující:

- diagnostiku a chirurgickou léčbu kardiovaskulárních onemocnění,
- diagnostiku a transplantace srdce, transplantace jater a ledvin a potransplantační sledování pacientů,
- odběry orgánů pro účely transplantací.

Takto specializovaná organizace pracující s lidským zdravím je velmi **citlivá na svoji kyberbezpečnost**. Stejně jako ostatní zdravotnická zařízení uchovává a zpracovává vysoké množství velmi citlivých dat pacientů, zaměstnanců a pojišťoven. Mnoho přístrojů je již dnes nějakým způsobem připojeno do IT infrastruktury a je potřeba myslet na jejich **neustálou a nejvyšší možnou ochranu**.

Jako společnost KERNUN jsme byli pověřeni naším řešením **KERNUN Security Appliance (KSA)** pomoci navýšit úroveň ochrany IT infrastruktury CKTCH. Úkol jsme brali velmi vážně, neboť u zdravotnických organizací tohoto typu nejde pouze o potenciální ztráty finanční, ale v případě úspěšného útoku se bavíme o potenciálních ztrátách na zdraví a životech pacientů.

Incidenty zachycené zařízeními KERNUN v síti CKTCH se odehrávaly na úrovni wifi sítí určených pro soukromé účely pacientů. Nejednalo se tedy o datové toky z vnitřní sítě CKTCH, ale celkového provozu, který KSA vzhledem k povaze nasazení zachytil.

„Nasazení KSA jako doplňku ke stávajícímu řešení ulevilo firewallu a pomohlo rovněž snížit počet incidentů zachycených v SIEM. Zároveň je uživatelsky přívětivý a v případě nutnosti lze rychle zablokovat podezřelé IP adresy již na perimetru."

Ing. Aleš Špidla
manažer kybernetické bezpečnosti
Centrum kardiovaskulární a transplantační chirurgie Brno

CKTCH | Centrum kardiovaskulární a transplantační chirurgie

www.kernun.cz info@kernun.cz +420 545 423 160

Řešení

Pro navýšení kyberbezpečnosti v CKTCH jsme se rozhodli použít dvojici **KERNUN Security Appliance s IP security package** v transparentním zapojení. Důvodů k tomuto rozhodnutí bylo hned několik:

- navýšení kompletní bezpečnosti celé sítě,
- žádná potřeba změny v topologii a adresaci sítě,
- neznatelné snížení propustnosti sítě.

Transparentní zapojení KERNUN Security Appliance s IP security package spočívá v nasazení ve formě L2 bridge. Dvě síťové karty se spojí dohromady a nechá se jimi protékat veškerý síťový provoz. Technologie KERNUN umožňuje i na L2 vrstvě kontrolovat zdrojové a cílové IP adresy, a díky tomu provádět kontrolu oproti reputační databázi aktivních hrozeb. Díky tomuto způsobu zapojení **není potřeba** vytvářet žádné mezisítě ani jakkoli jinak **zasahovat do adresace** interní sítě zákazníka, v tomto případě CKTCH. Díky jednoduché kontrole proti hotové databázi přímo v jádře operačního systému je **snížení propustnosti** sítě rovno téměř **nule**. Tato vlastnost je pro mnoho zákazníků včetně CKTCH kritická.

Navýšení kompletní bezpečnosti celé sítě

Žádná potřeba změny v topologii a adresaci sítě

Neznatelné snížení propustnosti sítě

Lokalizace zařízení KERNUN byla v CKTCH vymyšlena tak, aby zařízení byla článkem spojujícím interní síť s veřejným internetem. Toto umístění pomohlo **ulevit perimetrovým firewallům** díky tomu, že odfiltruje první vlnu útočníků přicházejících zvenčí. Velmi důležitým prvkem tohoto zapojení je ale **ochrana opačného směru**, tedy provozu směřujícího zevnitř do internetu. Pokud se totiž kdokoliv z interní sítě pokouší navázat spojení s někým, kdo se vyskytuje v KERNUN databázi aktivních hrozeb, jedná se o bezpečnostní incident.

Znamená to, že:

- Nějaký stroj v interní síti je napaden (např. se pokouší připojit do botnetu) nebo že je v interní síti uživatel, který se pokouší dostat někam, kde nemá být (ať už úmyslně, nebo omylem).
- Všechny ochranné prvky interní sítě (ochrana endpointů, antiviry, firewally atd.) toto propustily a spojení by se bez problému dostalo až na koncový server, pokud by ho KERNUN nezastavil.

Co je KERNUN Security Appliance s IP security package?

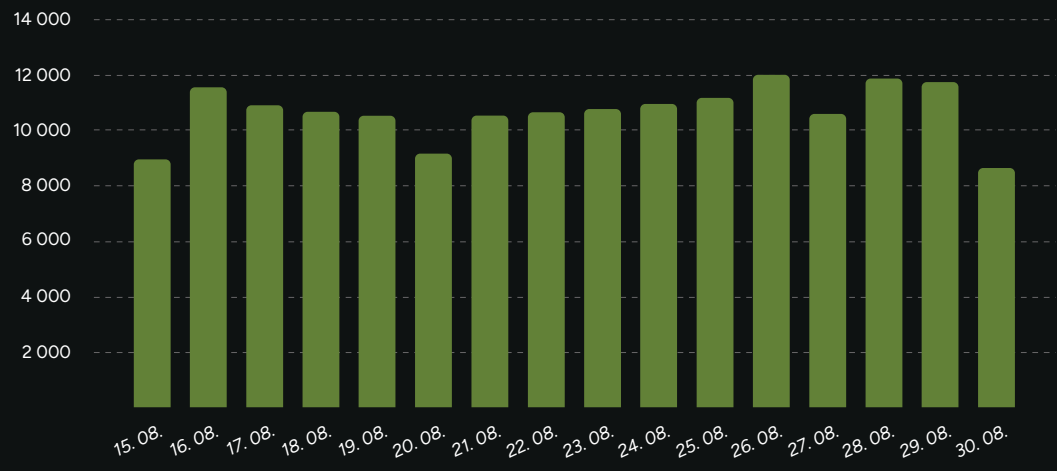
Jedná se o řešení navyšující bezpečnost interní sítě zákazníka pomocí **databáze aktivních hrozeb**. Již několik let pozorujeme český internet a navázali jsme spolupráci s mnoha dalšími subjekty, které se zabývají sběrem dat o bezpečnostních incidentech na území střední Evropy, zejména České republiky. Jsme součástí komunity CSIRT týmů, spolupracujeme se společnostmi jako jsou CESNET, CZ.NIC apod. a provozujeme vlastní síť honeypotů, na které lákáme nic netušící internetové útočníky. Pomocí všech takto získaných dat tvoříme každých 15 minut databázi aktivních hrozeb, která **přiděluje reputaci všem IP adresám**, které se v prostředí českého internetu chovají podezřele. Díky této databázi, která se na všech zařízeních KERNUN automaticky aktualizuje, jsou tak všechna zařízení KERNUN s IP security package **neustále chráněna**.

Pomohli jsme už více než 100 spokojeným zákazníkům. Přidejte se mezi ně.

Výsledky

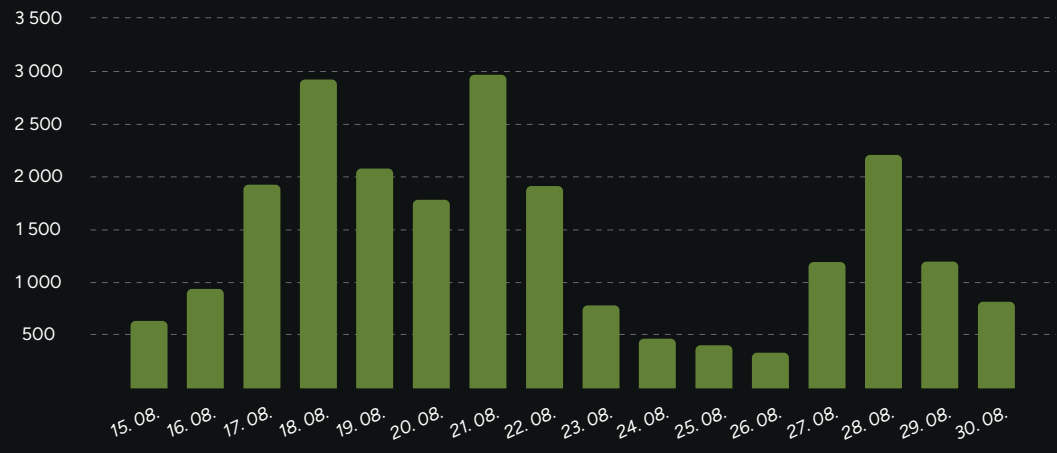
Pro tuto studii jsme provedli sledování spojení, která blokovala zařízení KERNUN v období od 15. srpna 2024 12:00 do 30. srpna 2024 12:00. Jedná se tedy o **data nasbíraná za dva týdny** provozu zařízení KERNUN v CKTCH.

Počet nebezpečných IP adres, které se pokoušely připojit do CKTCH



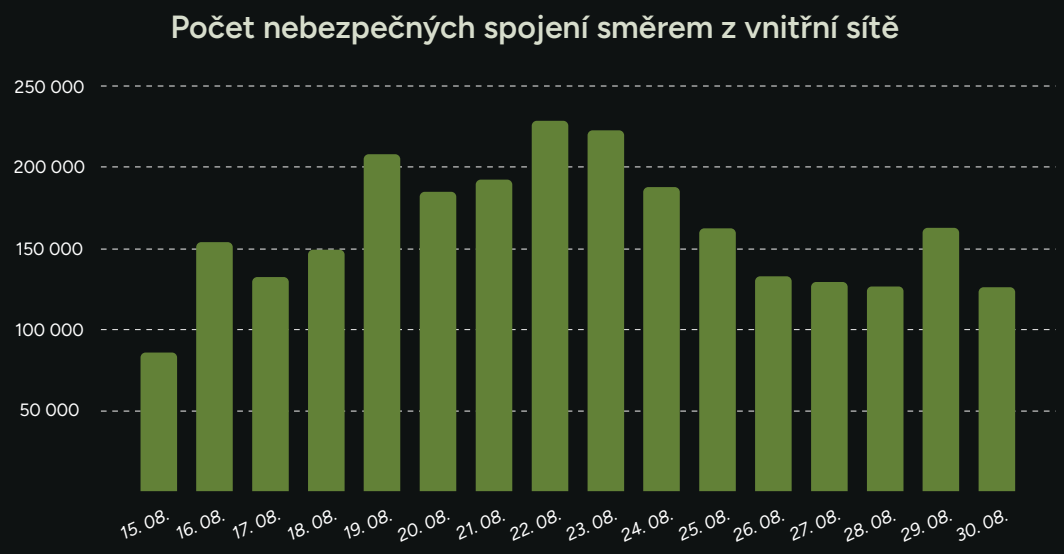
Jak je vidět z grafů, směrem z internetu na perimetr sítě CKTCH směřovalo denně v průměru **10 676 IP adres**, o kterých zařízení KERNUN vědí, že jsou podezřelé a účastnily se v posledních 48 hodinách bezpečnostního incidentu na území České republiky. Tyto IP adresy produkovaly směrem k CKTCH **průměrně 161 877 spojení denně**. Z toho vyplývá, že zařízení KERNUN nejen že tyto pokusy o spojení úspěšně zastavila, ale navíc ulehčila práci perimetrovým firewallům, které tak musely kontrolovat průměrně o 6 744 spojení méně každou hodinu (počítáno bez zohlednění pracovní doby).

Počet nebezpečných spojení směrem z interní sítě



Velmi alarmující data jsme nasbírali při monitoringu blokovaných spojení **směrem z vnitřní sítě do internetu**. Za dva týdny pozorování došlo každý den k několika pokusům se z vnitřní sítě CKTCH připojit do internetu na adresu, kterou zařízení KERNUN považovala za nebezpečnou. Velmi důležité je, že se interní zařízení pokoušela spojit sice pouze na relativně malý počet nebezpečných IP adres, v průměru na 3,6 adresy denně, ale pokusů o spojení na tyto nebezpečné adresy byly **denně stovky až tisíce**.

Blokace těchto pokusů o spojení je největší přidanou hodnotou zařízení KERNUN pro CKTCH, protože to, že se tato spojení na KERNUN vůbec dostala, značí, že veškeré **ostatní způsoby** zabezpečení **nezafungovaly**.



Z grafů zastavených spojení směrem z internetu je dále vidět, že počet nebezpečných adres pokoušejících se navázat spojení do interní sítě CKTCH **není nijak závislý na dni v týdnu**, je tedy potřeba síť chránit nepřetržitě, což automaticky aktualizovaná databáze aktivních hrozeb na zařízeních KERNUN splňuje.

Jak to, že KERNUN neblokuje validní provoz?

Výpočet reputace IP adres pro databázi aktivních hrozeb je velmi komplexní. Zohledňuje se mnoho faktorů, jako například počet zdrojů, které IP adresu zaznamenaly při bezpečnostním incidentu, časová vzdálenost jednotlivých incidentů, typ útoku, jehož byla adresa součástí, historický vývoj reputace IP adresy a podobně. Systém počítá s tím, že IP adresy nejsou statické a že každý den může IP adresu provozovat někdo jiný. Díky kombinaci všech zohledňovaných faktorů je databáze velmi **odolná vůči false positives**.

Závěr

Dvojice zařízení KERNUN **prokazatelně a měřitelně zvýšila zabezpečení interní sítě** organizace CKTCH. Zařízení KERNUN aktivně a automaticky blokuje veškeré podezřelé aktivity na síťovém provozu, a to **bez znatelných následků pro běžný provoz**. Za celou dobu měření nebyla zaznamenána ze strany CKTCH žádná stížnost týkající se rychlosti provozu nebo blokace legitimního provozu (false positives).

20+
let s vámi na trhu

100+
zákazníků nám důvěřuje

5 000+
zařízení pomáháme chránit

Odrazte útoky dříve, než vás stihnou ohrozit.
Přidejte se mezi naše spokojené zákazníky.

www.kernun.cz info@kernun.cz +420 545 423 160