Připojte se do sítě Honeypot senzorů NÚKIB!

portal.neweb.govcert.cz/informacni-servis/aktuality/pripojte-se-do-site-honeypot-senzoru-nukib

TLP:GREEN Autor: Národní úřad pro kybernetickou a informační bezpečnost,
23. 06. 2023

Odbor Vládní CERT jako součást Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) průběžně monitoruje, vyhodnocuje a analyzuje dění v kyberprostoru, aby měl maximální možný přehled o aktuálních trendech útočníků v tomto prostředí. Naším cílem je neustále sledovat využívané postupy útočníků, způsoby práce jejich nástrojů a analyzovat jejich cílení na slabiny systémů. Díky tomu pak lépe zaměřujeme naše kapacity!

Své zjištění a analýzy pak předáváme kolegům z NÚKIB k dalšímu využití. V případě potřeby pak máme možnost proaktivně varovat naše povinné subjekty před novými trendy útoků, či publikovat zajímavé analýzy pro povinné subjekty nebo i pro širokou veřejnost. Tím přispíváme k jejich lepšímu situačnímu povědomí, a přeneseně tak zvyšujeme kybernetickou bezpečnost a odolnost celé České republiky i jejích obyvatel. K dosažení tohoto cíle provozujeme na oddělení analýzy síťového provozu svoji vlastní síť Honeypot senzorů (HNPS) rozmístěných mezi zapojenými partnery. Takovýto senzor napodobuje například produkční server v DMZ, který ale není dobře chráněn. Oproti reálnému systému jde však pouze o emulaci, ke skutečné kompromitaci tedy nedojde. Útočník sice brzy zjistí, že jde o návnadu, i za krátkou chvíli však prozradí mnohé o svých postupech a nástrojích, například včetně volaných příkazů i parametrů. Jsme tak schopni vidět jeho činnost téměř jako za polopropustným zrcadlem. Získané logy nám tak umožní analyzovat a vyhodnocovat jeho činnost, včetně překlepů nebo časové osy jeho jednotlivých kroků.

Takto získaná data se v reálném čase odesílají šifrovaným kanálem do našeho analytického backend prostředí, kde probíhá jejich automatické předzpracování, obohacení a uložení do analytického systému. Tam s nimi efektivně pracují naši odborníci, vytvářejí korelace a (anonymizované) výstupy pro další části NÚKIB, povinné subjekty nebo pro veřejnost.

Samotný senzor (tedy náš systém pro běh honeypotů) je od základu vystavěn na bezpečných základech s filozofií zero-trust modelu. Nespoléháme na žádnou jedinou „všespásnou” technologii, která by měla senzor ochránit, ale vhodně vrstvíme mnoho na sobě nezávislých technologií a postupů, proaktivně monitorujeme systémové logy senzoru, to vše k dosažení opravdové kybernetické odolnosti! Překonání jedné, dvou, ba i všech našich ochran přesto neumožní útočníkovi ohrozit síť zapojeného partnera. I kdyby se mu povedlo překonat všechny naše překážky, tak je stále izolován mimo síť partnera a silně limitován v možnostech použít senzor k útoku dále do internetu (díky nezávislému firewallu zapojeného partnera a silně omezené možnosti odchozí

komunikace). Navíc bychom se díky okamžitému logování o všem dověděli (automatické alerty v našem analytickém systému při překročení daných mezí, nestandardnímu chování senzoru atd.).

Chtěli bychom poděkovat aktuálně zapojeným partnerům, že společně s námi pracují na zvýšení kybernetické bezpečnosti a odolnosti České republiky! Přestože tak činí zcela nezištně a jejich zapojení jim nepřináší žádný okamžitý užitek, dobrovolně a věcně spolupracují na vylepšování celého systému. Jako protiváhu pak od NÚKIB získávají pravidelné reporty o aktivitách útočníků, a v případě cílené kampaně jsou na ní proaktivně upozorněni.

Rádi bychom oslovili také další subjekty, kterým není lhostejná situace v kybernetickém prostoru, aby zvážili své možné přispění do projektu vlastním zapojením. Je to snadné, naprosto diskrétní (nikde nezveřejňujeme zapojené

partnery), neplynou z toho pro Vás žádné povinnosti a není potřeba nic nakupovat (využíváme, co už máte). Podmínky pro zapojení nejsou nijak náročné (jistě je snadno naplňuje i středně velká organizace).

Technické prerekvizity:

- volná veřejná IP adresa
- on-premise virtualizační platforma
- on-premise nezávislý hraniční firewall
- schopnost síťového oddělení od zbytku infrastruktury (např. separátní izolovaná VLAN)

(Ne)Náročnost běžícího senzoru:

- 1 vCPU
- 2 GB RAM
- 1 GB disk

Povinnosti Partnera:

- Nastavit svůj firewall pro důslednou izolaci senzoru od vlastní sítě
- Nastavit svůj firewall pro omezení odchozí komunikace daného senzoru (dle dodaného návodu)
- Mlčenlivost o detailech nasazení
- Možnost kdykoliv senzor vypnout a z účasti odstoupit
- Oznámit NÚKIBu případné cílené vypnutí senzoru
- Nulové personální náklady (žádný dohled, správa ani aktualizace ze strany partnera nejsou potřeba)

Pro více informací, a také pro konzultace možného zapojení, prosím pište email na: oasp@nukib.cz (v předmětu uveďte klíčové slovo "HNPS").

4