NSA: „Co je vaše, to je naše. A co je naše, po tom vám nic není.“

Autor: Clint Boulton

Ředitel IT oddělení Národní bezpečností agentury (NSA) říká, že analytický mechanismus ochraňuje soukromý cloud systém americké zpravodajské komunity před vnitřními i vnějšími hrozbami.

NSA během posledních více než dvou let od vynesení tajných informací jejím bývalým spolupracovníkem Edwardem Snowdenem výrazně navýšila své schopnosti detekovat kybernetické hrozby. Mnohovrstvá opatření zahrnující mj. analýzu chování uživatelů nyní ochraňují soukromý cloud, který jako úložiště a nástroj výpočetní a operační analýzy využívá zpravodajská komunita, řekl CIO.com ředitel IT oddělení (CIO) Greg Smithberger.

„Probíhá tam množství operací, které skutečně využívají spoustu naší na data náročné analýzy, je tam hodně technologie vyvinuté pro naše zahraniční zpravodajské operace i technologie, které jsme vytvořili uvnitř našeho Information Assurance Directorate,“ říká Smithberger, který nastoupil do nové pozice před šesti měsíci poté, co uplynulých 27 let strávil na rozličných operačních postech zahraniční rozvědky. NSA podle něj využívá automatizované možnosti „k posunutí naší práce na vyšší úroveň“ při detekci a reakci na anomálie, mezi něž patří cokoliv od vnějších útoků po podezřelou vnitřní aktivitu.

NSA schytala od mainstremamových médií i aktivistů zaměřujících se na ochranu soukromí tvrdé direkty, když Edward Snowden během práce pro NSA (jako zaměstnanec kontraktora Booz Allen Hamilton) v roce 2013 okopíroval a začal zveřejňovat dokumenty zachycující podrobnosti tajných programů, v jejichž rámci NSA sleduje komunikaci v USA i zahraničí. Tyto dokumenty staví do nového světla vládní monitoring telefonních a emailových záznamů při sledování podezřelých z terorismu. Každé další odhalení přiživuje plameny kontroverze – mezi nimi například expozé New York Times o tom, že NSA rozšiřuje metody, kterými se při hledání zloduchů probírá záplavou digitálních dat.

Analytické kapacity NSA brání vnitřním i vnějším hrozbám

NSA také zvýšila úroveň odhalování hrozeb ve svých vlastních sítích, které využívají analytici, operativci i programátoři při získávání zpravodajských informací.

Podle Smithbergera je jedním z jednodušších příkladů schopnost rozpoznat anomálii v případě, že se oprávněný uživatel přihlásí do sítě v neobvyklý čas nebo z neobvyklého místa. Představte si například, že se uživatel identifikovaný jako analytik NSA ve Virginii, který zpravidla zpracovává citlivé informace mezi sedmou ranní a sedmou večerní, pokouší ke stejným informacím dostat ve 3 ráno amerického času (EST) z Tel Avivu. Taková behaviorální analýza, zahrnující profilování a detekci anomálií, založenou na „strojovém učení“ je sice novinkou, která nabývá na popularitě v korporátním světě, kde se podle zjištění výzkumu provedeného analytičkou společnosti Gartner Avivah Litanovou využívá k včasnému odhalení prolomení prioritizace nejvěrohodnějších výstrah.

NSA v reálném čase provádí forenzní analýzu kyberbezpečnostního softwaru a zařízení, včetně firewallů, VPN a záznamových logů každého zařízení v síti „abychom dokázali zpozorovat věci, které si lidé sami nedokáží spojit,“ poznamenává Smithberger a dodává, že existují i další, mnohem „jemnější“ metody odhalování hrozeb, které však odmítá podrobněji popsat. „Rozhodně se nebudu pouštět do podrobností, ale jde o to uvědomit si, co je na vaší síti normální a jednoznačně povolené… a v reálném čase porovnat zaznamenané údaje s povoleným a běžným.“

Tato opatření mají za úkol ochránit pečlivě vyprojektovaný soukromý cloud, který dle Smithbergera využívá podobné technologie, jako by člověk očekával od veřejných cloudových služeb typu Amazon Web Services, včetně virtuálních serverů a aplikací. Přesto se však najdou zásadní rozdíly, jelikož technologie je nastavena k zajištění přístupu pro velké množství analytiků a operativců s různým stupněm oprávnění přístupu k informacím, od velice nízkého po přísně tajný. Přístup je velice pečlivě kontrolován až po nejnižší úroveň dat. Dva analytici provádějící totožné vyhledávání uvnitř systému mohou na základě stupně své bezpečnostní prověrky vidět odlišné výsledky, říká Smithberger.

> „Uvnitř i vně sítě máme mnoho úrovní, které nás oddělují od vnějšího světa… vrstevnatý bezpečnostní model, kombinující vládní, na zakázku zhotovené a soukromé produkty. Tato paranoidní, mnohovrstvá obrana je skutečné nejlepší

> odpovědí a upřímně řečeno, když to nastavíte dobře, jakékoliv vnitřní problémy se stanou okamžitě viditelnými," popisuje Smithberger

Soukromý cloud vytvořený ve stylu veřejného

I samotný soukromý cloud lze označit za triumf. Vybudovaný v rámci programu Intelligence Community Information Technology Enterprise (ICITE), byl v roce 2011 navržen tak, aby jeho prostředí umožňovalo bezpečnostní komunitě bezpečně přistupovat k informacím a bezpečně je sdílet. Bývalý zastupující ředitel Defense Intelligence Agency David Shedd v březnu řekl, že „kulturní odpor," nikoliv technologie, představuje největší překážku vybudování soukromého cloudu.

Podle Smithbergera je dnes soukromý cloud NSA plně funkční díky pomoci několika spolupracovníků vlády z privátní sféry a jeho vlastním lidem z IT oddělení, kteří nahradili množství stárnoucích a na zakázku vyrobených serverů, databázového softwaru a aplikací, z nichž mnohé ukádaly data odděleně. Vylepšení těchto technologií vytvořením integrovaného, společně sdíleného zdroje prostředků a informací se NSA dle svých vlastních slov dostane do lepší pozice při analýze svých informačních zdrojů, a tak bude moci lépe sloužit analytikům, operativcům a dalším složkám.

Smithberger dodává, že tento soukromý cloud disponuje mnohem jemněji nastaveným zabezpečením než jakýkoliv jiný produkt na trhu. Přesto ale neoznačuje soukromý cloud NSA za neproniknutelný.

„Označit průnik do naší sítě na nemožný by zaváněl arogancí. S velkou pečlivostí jsme však vytvořili řadu mechanismů na ochranu našeho utajeného světa před světem vnějším a neustále pokračujeme ve vývoji nových myšlenek k dalšímu posílení zabezpečení novými a novými vrstvami – řekněme, že nejsme snadné sousto," uzavřel.

Článek Clinta Boultona How the NSA uses behavior analytics to detect threats vyšel na stránkách CIO.com 7. prosince 2015.