DEEP SECURE

Nebezpečný obsah

A jak se s ním vypořádat

Digitální obsah jako nepostradatelná životodárná míza byznysu a obchodu je oblíbeným prostředkem využívaným současnými útočníky. Neobejdeme se bez něj, přesto občas můžeme litovat, že jsme s ním pracovali.

Hra na kočku a na myš

Kybernetická bezpečnost se hrozbou nebezpečného obsahu zabývá už dlouho. Již mnoho let probíhají „závody ve zbrojení“, v nichž ovšem tradičně mají navrch útočníci. Nejdříve přišly antivirové programy. Vzápětí se však objevily polymorfní viry, které je dokázaly překonat. Jako zázračná záchrana přišlo spouštění v izolovaném prostředí (sandbox) a zdálo se, že pokročilým perzistentním hrozbám konečně odzvonilo. Jenže útočníci se nevzdali a vyvíjeli metody, jak obranu obejít. Netrvalo dlouho a podařilo se jim to.

Vysoce citlivé veřejné systémy mezitím používaly technologii hloubkové kontroly obsahu (DCI, Deep Content Inspection), která blokovala všechno, co jen trochu připomínalo hrozbu. Ale ani zde se díky rostoucím schopnostem útočníků nepodařilo obráncům udržet si náskok.

Radikální proměna

Když si státy uvědomily, že útočníci začínají být schopni proniknout skrz DCI, pustily se do hledání alternativy, která by situaci opět obrátila v jejich prospěch. Měla to být metoda, která při blokování hrozeb nezávisí na jejich odhalování. Ukázalo se, že odpovědí je transformace. Vývoj probíhal za zavřenými dveřmi obranné a zpravodajské komunity. První viditelné známky této práce se objevily v roce 2004 v podobě patentu podaného týmem QinetiQ, který pracoval v rámci výzkumného programu kybernetické bezpečnosti britského ministerstva obrany.

Tento druh obrany nespoléhá na odhalování nebezpečných dat nebo chování. Místo toho transformuje data v něco jednoduchého a nepochybně bezpečného, čímž odstraňuje jakoukoli přítomnou hrozbu. K této transformaci dochází i v případě, že žádná hrozba neexistuje – data jsou transformována vždy. Z hlediska příjemce na tom nezáleží, neboť v každém případě dostane to, co potřebuje.

Nešlo však o příliš univerzální technologii, takže to zdaleka nebylo řešení vhodné pro komerční použití. Hodila se pro speciální zakázkové systémy za neuvěřitelné sumy. Rozšířit ji tak, aby ji bylo možno využít v produktech a službách, které lze snadno nasadit a škálovat a jsou přizpůsobivé a použitelné v celé řadě situací a prostředí, však byl zcela nový úkol. A donedávna ani neexistoval trh, který by něco takového využil. Celá technologie tedy ležela zapomenuta kdesi v zapadlém šuplíku.

Staronová metoda

Nová a nová selhání technologie pro obranu obsahu založené na detekci nicméně postupem času přiměla některé firmy změnit pohled na technologii hloubkové inspekce obsahu, která v minulosti chránila citlivé vládní systémy.
Výsledkem byla technologie Odzbrojení a rekonstrukce obsahu (CDR, Content Disarm and Reconstruction), což je komerční realizace myšlenky, podle níž je zablokováno vše, co je schopné posloužit jako nosič útoku.

Vychází z názoru, že aktivní obsah pravděpodobně není bezpečný a je tedy třeba ho zastavit. Jde o poněkud drakonický přístup, protože blokuje i některý bezpečný obsah. V minulosti čelily hrozbám dost vážným na to, aby něco takového bylo nutné, pouze veřejné systémy. Nyní jsou ale ve stejné pozici i systémy mnohých firem.

Problém je, že CDR je stejnou technologií jako DCI, takže trpí stejným problémem – obrana je jen tak dobrá, jak dobrá je schopnost obránců předpovídat další krok útočníků. A v takovém závodu mají útočníci vždycky navrch. Jde o to, že CDR/DCI hrozbu nezlikviduje, jen odstraní takové vektory, o nichž obránci vědí. Hrozba je sice omezena, zůstává však její část, o které nevíme.

Tváří v tvář neznámu

Pokud obrana odstraní všechny hrozby, které zná a rozumí jim, některé hrozby přetrvají. I pokud je odstraněných hrozeb hodně, neznamená to, že zbývající hrozby jsou nepodstatné. Zbývající riziko je totiž neznámé a nevyčíslitelné. Netušíte, zda útočník stále nemůže jednoduše proniknout do vašeho systému pomocí bezpečnostní mezery, na kterou jste nepomysleli. Manažeři, kteří povolují velké výdaje za kybernetickou obranu, se dřív ptali: „Kolik hrozeb bylo zastaveno?“ a předpokládali, že pokud zastavíme velký počet hrozeb, nemůže jich zůstat dost na to, aby bylo třeba se jimi zabývat. V dnešní době nicméně vychází najevo, jak moc klamné to může být. Dnes si spíše pokládáme otázku „Jaké útoky to propustí?“ A na tu nám nedokáží odpovědět ani antivirové programy, spouštění v sandboxu ani CDR/DCI.

A to není zdaleka vše. Zdá se, že útočníkům už nestačí překonat naši současnou obranu. Posouvají úhybné manévry na novou úroveň. Především pomocí steganografie maskují útoky, skrývají kanály umožňující ovládání a nenápadně vynášejí citlivé informace. A ačkoli už tak mají navrch, snaží se posunout ještě dál – využívají techniky skrývání informací, které zcela znemožňují odhalení. To už není hra na kočku a na myš. Zákeřní hlodavci už kočku dávno sežrali.

Odpověď na digitální hrozbu

Neexistuje způsob, jakým by obránci mohli ztrátu dohnat. Alespoň ne pokud budou dál hrát podle pravidel a jen se pokusí běžet rychleji. Je potřeba něco radikálně odlišného, co útočníky okamžitě přeskočí a navždy jim zablokuje cestu. Je čas vrátit se k myšlence transformace a změnit ji v komerční realitu. Je čas podívat se, co dělá společnost Deep Secure.

Transformace je způsob, jak získat náskok před útočníky a udržet si ho, protože odstraňuje hrozbu a nedává šanci vymyslet metodu, jak se obraně vyhnout. Tomuto přístupu říkáme Odstranění hrozby z obsahu (CTR, Content Threat Removal), protože přesně to dělá.

Původní myšlenkou bylo transformovat data přicházející od potenciálních útočníků v prostá data, která jsou evidentně bezpečná. To je sice dobré, ale použití je omezené, protože to funguje pouze s jednoduchými formáty dat. Což není příliš univerzální a v komerčním prostředí to tudíž není ani moc užitečné. Společnost Deep Secure tento princip rozvinula a posunula na vyšší úroveň – namísto transformace dat transformujeme to, jak jsou data reprezentována.

CTR je založeno na předpokladu, že žádná data nejsou bezpečná. Nesnaží se odlišit dobrá od škodlivých. Zablokuje všechna data, která útočníci pošlou. To je víc než u CDR/DCI, kde jsou zablokována pouze data považovaná za nebezpečná. Není třeba se rozhodovat, co je bezpečné a co ne, takže nelze udělat chybu. Jak to ale funguje? Jak získá firma informace, které potřebuje?

CTR obchodní informace extrahuje z přijatého digitálního obsahu. Data nesoucí tyto informace jsou poté zahozena a jsou vytvořena nová bezpečná data, kterými jsou obchodní informace předány ke svému cíli. Útočník tak nepronikne obranou a firma přesto dostane, co potřebuje. Žádná jiná metoda odstraňování hrozby z obsahu nemůže být účinnější. Bezpečnostní tým je spokojen, protože hrozba byla odstraněna. A zbytek firmy je spokojen také, protože dostal potřebné informace.

Zní to podezřele snadno. Aby však software pro CTR fungoval, je třeba velmi dobře znát způsob, jakým je tvořen a používán obsah. Software musí vědět, jak jsou informace v datech zachyceny, dokázat je extrahovat a vytvořit nová data. Žádné obchodní informace při tom nesmějí být ztraceny a zároveň nesmí útočník dostat šanci ovlivnit jejich doručení. I pro jeden jednoduchý formát dat je to náročné. Ale pokud to musíme opakovat pro všechny složité formáty, nevznikne škálovatelné a udržitelné řešení. Vyřešení tohoto problému je jedním z průlomů, který se společnosti Deep Secure při práci na CTR podařil.

Flexibilita: klíč k úspěchu

Má-li se transformace dostat z pozice okrajové metody a na trhu uspět, je potřeba taková technologie CTR, kterou lze nasadit mnoha různými způsoby splňujícími požadavky různých firem. Většina firem se může opřít o izolační a separační funkce zabudované do nějaké cloudové služby, které zabraňují v přístupu k jejich informacím ostatním uživatelům této služby.

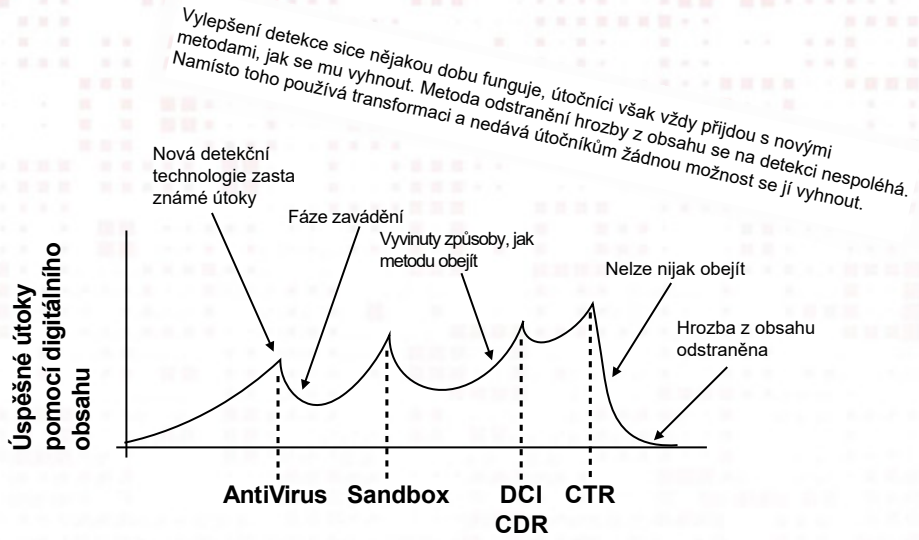
Tyto firmy potřebují CTR nasazené způsobem vhodným pro cloud. Jiné společnosti potřebují soukromé cloudy. CTR pak musí být součástí izolačního mechanismu chránícího daný cloud. V extrémních případech, například u státních obranných a zpravodajských systémů, musí být izolační mechanismy vysoce spolehlivé a zajišťovat úplnou izolaci komerčního systému.

Dosáhnout toho všeho byl další průlom společnosti Deep Secure. Díky tomu, že umožnila fungování stejné implementace při nasazení ve veřejném cloudu, v soukromém cloudu i v situacích vyžadujících vysokou spolehlivost, poskytla společnost Deep Secure svým zákazníkům bezprecedentní výběr. Stejnou technologii lze nasadit v různých částech firmy a dosáhnout různých cílů, čímž se vyhnete zbytečně komplikovanému systému a zároveň ušetříte.

Skutečným důkazem výkonnosti CTR je jeho účinek v případě použití steganografie. Obrany založené na detekci nemají šanci, protože tuto metodu detekovat nelze. CTR se však hrozby odhalovat nesnaží. Steganografie funguje tak, že skrývá informace v redundantních částech dat. CTR z dat extrahuje užitečné informace, přičemž samozřejmě vynechá veškeré informace zakódované v redundantních datech. CTR překonává steganografii jejím ignorováním – žádné jiné metody ji překonat nedokáží, protože ji nevidí.

Budoucnost

Spolu s rostoucí pokročilostí útoků se zlepšují i obranné metody, které tyto útoky mají odhalit. Každé vylepšení obrany nicméně přiměje útočníky vyvinout nové techniky, kterými se obraně vyhnou. Zdá se však, že pro detekční systémy nastává konec, protože útočníci se schovávají za steganografii, kterou detekovat nelze. V budoucnu je třeba přijít s něčím radikálně odlišným – s odstraněním hrozby z obsahu. Je to obrana, která jednou provždy likviduje hrozbu, kterou mohou útočníci skrýt v digitálním obsahu.
CTR neznamená konec jiných bezpečnostních opatření. Stále je potřeba zabezpečit koncové body, protože existují vstupní body do systému, které CTR nekontroluje, a nadále je třeba chránit hranice systému. Stále bude nezbytné i vnitřní sledování a ochrana před únikem dat, protože i vlastní zaměstnanci budou nadále hrozbou. Při nasazení CTR nicméně zmizí mnoho „šumu“, kvůli kterému je tyto jiné mechanismy těžké spravovat.



CTR je navíc prospěšné i pro obchodní analýzu. Protože z obsahu získává obchodní informace, dokáže dodávat velmi kvalitní údaje o činnosti firmy. Kvůli tomu, abyste zjistili, co se ve firmě děje, už nebude potřeba se soustředit na aktivitu v síti. Budoucí analytické funkce budou moci pracovat přímo s relevantním materiálem, takže přinesou podrobnější statistiky a snáze odhalí podvod.

CTR je jedinou cestou vpřed. A Deep Secure již tuto metodu používá ve své platformě Content Threat Removal.

Další informace

Další informace naleznete na webu **www.deep-secure.com.**