INFORMACJA PRASOWA

Infoblox wprowadza najbardziej kompleksowe rozwiązanie do zabezpieczania DNS w sieciach korporacyjnych

SANTA CLARA, Kalifornia, … 2015 r. — Infoblox Inc. (NYSE:BLOX), firma specjalizująca się w sterowaniu sieciami, wprowadza na rynek Infoblox Internal DNS Security, najbardziej kompleksowe homogeniczne rozwiązanie do zabezpieczania DNS wewnątrz sieci korporacyjnych. Internal DNS Security chroni przed atakami, złośliwym oprogramowaniem i eksfiltracją danych.

Korporacyjne zapory sieciowe zwykle nie badają odpowiednio przychodzącego i wychodzącego ruchu DNS. Sprawia to, że DNS staje się słabym punktem, często wykorzystywanym przez cyberprzestępców. Złośliwe oprogramowanie po zagnieżdżeniu się w sieci wykorzystuje DNS do komunikacji z serwerami dowodzenia (Command&Control) BOTNET, kradzieży poufnych danych. Złośliwi użytkownicy wewnątrz sieci również mogą wykorzystać DNS do przeprowadzania ataków typu DDoS z przejętych przez siebie systemów.

Infoblox Internal DNS Security to zabezpieczone urządzenie, która przekształca słabości wewnętrznego serwera DNS w siłę, zapewniając ochronę przed wykorzystaniem DNS do ataków na infrastrukturę, instalowaniem złośliwego oprogramowania i zaawansowanymi uporczywymi zagrożeniami (advanced persistent threats, APT), a także eksfiltracją danych przez DNS.

Infoblox Internal DNS Security wykorzystuje bogate doświadczenie firmy Infoblox w dziedzinie zabezpieczeń DNS i zapewnia skuteczniejszą ochronę przed wieloma typami ataków, m.in.:

- **Wykrywanie i blokowanie ataków na infrastrukturę DNS.** Urządzenie wykrywa i blokuje wewnętrzne ataki DNS DDoS, exploity bazujące na DNS oraz tunelowanie DNS. Wspomagane sprzętowo zapobieganie atakom DDoS umożliwia zachowanie integralności i dostępności systemu nawet podczas bardzo intensywnych ataków.

- **Zakłócanie działania APT i złośliwego oprogramowania.** Stale aktualizowane źródło złośliwych adresów IP, serwerów DNS i domen sprawia, że znane APT i inne złośliwe aplikacje nie mogą komunikować się ze swoimi serwerami dowodzenia.

- **Zapobieganie eksfiltracji danych.** Infoblox Internal DNS Security potrafi wykrywać tunelowanie DNS, zgłaszać alarmy i blokować zapytania, co uniemożliwia eksfiltrację danych przez DNS i zapobiega kradzieży poufnych informacji.

Zabezpieczanie infrastruktury DNS ma dwa aspekty, a firma Infoblox zadbała o oba. Infoblox External DNS Security to specjalnie wzmocnione rozwiązanie, które chroni przed najszerszą gamą zewnętrznych zagrożeń, takich jak wolumetryczne ataki DDoS, przejmowanie zapytań DNS, exploity bazujące nad DNS oraz ataki zwiadowcze. Po wykryciu ataku DDoS rozwiązanie ogranicza jego skutki przez blokowanie wrogiego ruchu DNS i reagowanie tylko na rzeczywiste zapytania. Więcej informacji o Infoblox External DNS Security można znaleźć pod adresem www.infoblox.com/external-dns-security.

Zarówno Infoblox Internal DNS Security, jak i Infoblox External DNS Security używają standardowych interfejsów API, które współpracują z heterogenicznymi ekosystemami bezpieczeństwa, jakich zwykle używa się w sieciach. Interfejsy te umożliwiają urządzeniom Infoblox przyjmowanie informacji o zagrożeniach od innych rozwiązań w celu łagodzenia ataków oraz współdzielenie danych na temat detekcji, które pozwalają zidentyfikować urządzenia klienckie przejęte przez napastników.

Gartner, Inc., czołowa firma specjalizująca się w analizach rynku IT, w niedawnym raporcie „Market Guide for DNS, DHCP and IP Address Management (DDI)" podkreśliła rosnące zapotrzebowanie na zabezpieczony system DNS. Raport stwierdza: „Niedawne głośne ataki sprawiły, że organizacje są bardziej skłonne do inwestowania w rozwiązania zabezpieczające. Ponadto organizacjom coraz bardziej zależy na ochronie DNS, a wielu producentów DDI obecnie oferuje zabezpieczenia DNS. Widzimy rosnące zainteresowanie klientów zabezpieczeniami DNS powiązanymi z rozwiązaniami DDI. Komponenty zabezpieczające, takie jak zapory DNS, są obecnie obecne w około 20-30 proc. transakcji z klientami, które zbadał Gartner"*.

Bezpłatna kopia powyższego raportu jest dostępna pod adresem www.infoblox.com/gartner.

„Unikatowa pozycja systemu DNS w sieci sprawia, że jest to optymalny punkt do działań ochronnych i reagowania na zagrożenia" — powiedział Scott Fulton, starszy wiceprezes ds. produktów w Infoblox. — „Infoblox Internal DNS Security wykorzystuje tę szczególną pozycję, aby chronić krytyczną infrastrukturę DNS, blokować APT i złośliwe oprogramowanie oraz zapobiegać eksfiltracji danych, wszystko to bez wprowadzania żadnych zmian w oprogramowaniu punktów końcowych albo w architekturze sieci".

Ceny i dostępność

Infoblox Internal DNS Security oraz Infoblox External DNS Security są już dostępne na całym świecie. Informacje u cenach można uzyskać u przedstawicieli handlowych i dystrybutorów Infoblox.

** Gartner, Market Guide for DNS, DHCP and IP Address Management (DDI), Andrew Lerner, Christian Canales, 24.02.2015 r.*

Infoblox — informacje
Infoblox (NYSE:BLOX) dostarcza rozwiązania do zautomatyzowanego sterowania sieciami, fundamentalną technologię, która łączy użytkowników, urządzenia i sieci. Około 7500 przedsiębiorstw i dostawców usług wykorzystuje te rozwiązania do transformowania, zabezpieczania i skalowania złożonych sieci. Infoblox pomaga odciążyć ludzi od zadań związanych z zarządzaniem sieciami, ograniczyć koszty i zwiększyć bezpieczeństwo, dokładność oraz czas bezawaryjnej pracy systemów. Infoblox (www.infoblox.com) ma siedzibę główną w Santa Clara w Kalifornii i prowadzi działalność w 25 krajach.

Dodatkowych informacji udzielają:

Rafał Szewczyk
Regional Sales Manager Eastern Europe
Infoblox
tel. kom.: +48 881 91 66 66
rszewczyk@infoblox.com

Kinga Szkultecka
Specjalista ds. PR
SkyPR
tel. kom. +48 605 767022
kinga@skypr.com.pl