Attack Deception System

Zapewnienie bezpieczeństwa IT, jakie znamy, już nie działa

Z racji ich znaczenia strategicznego, firmy stoją w obliczu wyzwań ochrony przed coraz bardziej zaawansowanymi technikami ataków ukierunkowanych (APT – Advanced Persistent Threats) cechujących się: wysokim poziomem wiedzy technicznej atakującego, wysokimi nakładami finansowymi przeznaczonymi na realizację ataku, długoterminowym i systematycznym działaniem oraz głęboką wiedzą o wewnętrznych mechanizmach działania organizacji. Ataki APT nie ograniczają się jedynie do obszaru systemów IT, a bardzo często polegają na działaniach w obszarach bezpieczeństwa fizycznego, administracyjnego, proceduralnego, sieci automatyki przemysłowej czy też na aktywnym pozyskiwaniu informacji od osób zainteresowanych lub z portali społecznościowych.

Obrona przed nowymi metodami ataków

Architektura bezpieczeństwa stosowana jako pierwsza linia obrony zmienia się zbyt wolno w stosunku do coraz nowszych metod ataku, a w rezultacie zawodzi w przypadku zaawansowanych metod penetracji brzegu sieci. Attack Deception System (ADS), rozwiązanie polskiej firmy STM Solutions, jest implementacją nowego podejścia do bezpieczeństwa cybernetycznego – ang. „deception technology". Wywodzi się ono ze znanego mechanizmu „honeypot", którego celem jest zwabienie intruza do wydzielonego miejsca w infrastrukturze - pułapki - i odciągnięcie od strategicznych elementów infrastruktury o krytycznym znaczeniu dla funkcjonowania organizacji.

W ADS ustawiamy pułapki w formie specjalizowanych modułów bezpieczeństwa dla usług sieciowych (ADS Portspoof), sieci bezprzewodowej (ADS WiFi Client Analyzer), sieci SCADA (ADS HoneyNet SCADA) czy serwerów w DMZ (ADS HoneyNet DMZ) tak, aby zakamuflować rzeczywistą infrastrukturę i pozwolić atakującemu „włamać" się. Pierwsze próby rekonesansu są widoczne natychmiast. Postęp ataku jest monitorowany przez zespół SOC na bieżąco w konsoli ADS, a dostarczane dane mogą posłużyć do natychmiastowej analizy i zrozumienia ataku. Jednocześnie możliwe jest, z poziomu ADS, wpływanie na zachowanie atakującego poprzez np. wydłużanie czasu skanowania, prezentowanie kolejnych usług-pułapek czy realizację innego scenariusza skutkującego odkryciem atakującego. W tym samym czasie inne zespoły mogą przygotować najlepszy sposób zatrzymania przeciwnika.

Wykrywanie anomalii i działań nieautoryzowanych

ADS pozwala na detekcję anomalii i działań nieautoryzowanych w systemach teleinformatycznych, automatyki przemysłowej oraz z użyciem danych z systemów kontroli dostępu fizycznego i telewizji przemysłowej CCTV. Dzięki korelacji danych z tych środowisk w jednym miejscu całościowe zarządzanie bezpieczeństwem jest skuteczniejsze, a wykrywanie naruszeń – sprawniejsze.

Z poziomu ADS możliwe jest także weryfikowanie realizacji polityk bezpieczeństwa. Nasze obserwacje i doświadczenia w badaniu podatności firm na włamanie cybernetyczne pokazują, że np. hasło administracyjne, które nie jest zmieniane od wielu miesięcy czy (sic!) lat jest idealnym miejscem do nieskrępowanego prowadzenia działań przestępczych przez wiele tygodni.

Zaprojektowany w oparciu o doświadczenie z realnych ataków

Firma STM Solutions pomaga organizacjom podwyższyć poziom bezpieczeństwa m.in. poprzez prowadzenie audytów bezpieczeństwa i testów penetracyjnych black-box. Podczas takich autoryzowanych przez klienta działań zachowujemy się jak potencjalny atakujący. Wnioski i doświadczenia wykorzystaliśmy do zaprojektowania zestawu narzędzi wchodzących w skład ADS tak, aby ochrona była najbardziej skuteczna.

Wdrożenie dopasowane do organizacji

ADS jest zbudowany z elementu centralnego ADS Core, który odpowiada za zbieranie, analizę, korelację, prezentację danych o atakach i konfigurację połączonych z nim modułów bezpieczeństwa. W zależności od potrzeb organizacji wdrożenie ADS może być realizowane w formie serwera wirtualnego lub w architekturze rozproszonej pozwalającej na wykorzystanie wydajności sprzętu obsługującego dany komponent ADS Core.

KLUCZOWE KORZYŚCI

- **Obniżenie lub wyeliminowanie strat finansowych** – skuteczna detekcja zdarzeń przez skierowanie ataku na zastawione pułapki obniża ryzyko strat finansowych wskutek uszkodzenia danych, kradzieży informacji lub zakłóceń ciągłości biznesowej
- **Podniesienie poziomu zgodności** z wymaganiami norm lub branżowymi w zakresie bezpieczeństwa – np. RODO, Rekomendacja D, KRI czy ISO 27001 oraz ISO 22301
- **Usprawnienie procesu obsługi incydentów** - „sztuczne" wydłużenie czasu trwania i zakłócanie ataku przy obrazowaniu zdarzeń w trybie „near real-time" pozwala personelowi na analizę ataku i użytych narzędzi, w tym 0-day
- **Niskie koszty implementacji i utrzymania** w modelu dopasowanym do możliwości przedsiębiorstwa
- **Ochrona poczynionych inwestycji** - ADS jest uzupełnieniem narzędzi monitorowania bezpieczeństwa w SOC. Może być zintegrowany z posiadanymi systemami takimi jak SIEM lub jako samodzielne narzędzie
- **Eliminowanie „martwego pola obserwacji"** – ADS umożliwia tworzenie infrastruktury pułapek w zależności od potencjalnego wektora ataku i używanych komponentów systemów IT, OT i SKD; działanie pułapek pozwala na sterowanie zachowaniem atakującego i np. odkrycie jego tożsamości

CECHY WYRÓŻNIAJĄCE

- **Detekcja rekonesansu, obcej infrastruktury i ataków** na środowisko systemów kontroli dostępu fizycznego, IT i informatyki przemysłowej (OT) pozwala na objęcie ochroną całego przedsiębiorstwa
- **Oszacowanie stopnia zaawansowania ataku** – ADS odróżnia atak prowadzony automatycznie (maszynowo) i manualnie
- **Ciągłe, cykliczne testowanie** bezpieczeństwa urządzeń mobilnych
- **Unikalne moduły bezpieczeństwa** - Portspoof, Service Honeypot, WiFi Clients Analyzer, Fake BTS Detector
- **Dopasowany do polskich warunków** – projektując system ADS, uwzględniliśmy doświadczenia STM Solutions zdobyte podczas przeprowadzania autoryzowanych ataków hackerskich u polskich klientów
- **Optymalny kosztowo model licencyjny** - niezależny od ilości zbieranych danych i liczby zdarzeń na sekundę

Warszawa, Równoległa 2

+48 22 823 72 18

support@stmsolutions.pl