ne narzędzie oparte jest o matematyczny model symulacyjny układu gazowego, który umożliwia prowadzenie wielowariantowych obliczeń techniczno-ekonomicznych w celu określenia optymalnego planu produkcji. Model matematyczny wyposażony jest w algorytm optymalizacyjny pozwalający na określenie ekonomicznego punktu pracy układu kogeneracyjnego dla przyjętego kryterium optymalizacyjnego. Przedstawione narzędzie obliczeniowe jest precyzyjnym i wydajnym rozwiązaniem do celów planowania produkcji dla systemów energetycznych z turbinami gazowymi.

Mgr inż. Tomasz Turba, dr inż. Michał Podpora, Politechnika Opolska

Implementacja zagnieżdżonych honey-potów w infrastrukturę informatyczną przedsiębiorstwa jako składowa ochrony bariery dostępu do sieci wewnętrznej

Współczesne zabezpieczenie systemu informatycznego przedsiębiorstwa jest procesem nieskończonym w czasie opartym o infrastrukturę, kadrę i sporą dozę intuicji. Często stosowane są serwery typu honey-pot jako przynęty i jednocześnie możliwości obserwowania strategii działania hakera. Zabezpieczenia, specjaliści, wprawna analiza ruchu sieciowego nie wystarczają w przypadku wystąpienia luki typu zero-day o nierozpoznanych sygnaturach i anomaliach. Artykuł opisuje niekonwencjonalny sposób umieszczenia w sieci zagnieżdżonych serwerów honey-pot zapewniający wczesne reagowanie na możliwy incydent bezpieczeństwa jako wsparcie głównych technologii zabezpieczeń (firewall, systemy IDS, proxy) oraz administratora bezpieczeństwa informacji w walce z rozwijającą się branżą przestępstw komputerowych.

Wstęp

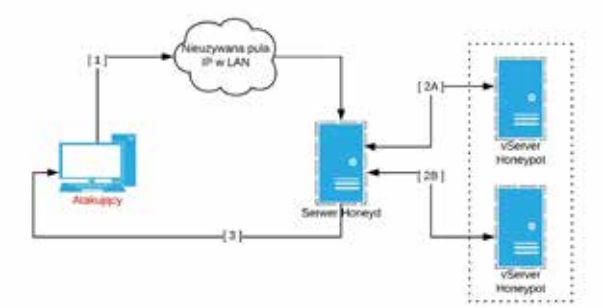
Zgodnie z raportem CERT [1] z roku na rok liczba odnotowywanych incydentów wzrasta. Nie oznacza to wcale, że na świecie jest coraz więcej zagrożeń, pomimo, że jest to prawda. Oznacza to, że świadomość użytkowników, administratorów Systemów Informatycznych (SI) jest coraz większa i nie boją się oni wejść w otwartą walkę z przestępcami, wspomagając się zespołem reagowania CERT Polska [2]. Na tym podłożu można uznać, że w globalnym krajobrazie bezpieczeństwa sieciowego, Polska odniosła sukces. Kolejnym etapem jest powszechne szkolenie administratorów aby przynajmniej potrafili sobie poradzić z zakresem osłony swoich SI przed lukami opisanymi i sklasyfikowanymi. Doprowadzenie systemu do najnowszej aktualizacji jest ważne, ale niestety nie zawsze wystarcza [3]. Najlepszą bronią przeciwko komputerowym przestępcom jest niekonwencjonalne podejście do ochrony systemu. W przypadku gdy zabezpieczenia są znane i typowe na etapie rekonesansu, przestępca będzie w stanie przygotować działania otwierające mu drogę do włamania [4]. Na pomoc administratorom przychodzi wąskie grono specjalistów zajmujących się technologią Honey-pot [5].

Honey-pot na przykładzie Kippo i Honeyd

Honey-pot jest techniką bezpieczeństwa komputerowego umożliwiającą detekcję, przechwycenie oraz zatrzymanie potencjalnego włamywacza. Wykorzystując policyjną metodę „żądła" lub „wędki" [6] opierającej się na podpuszczaniu włamywacza, podawania mu pewnych danych, które ocenia za prawdziwe, służby bezpieczeństwa informatycznego mogą zareagować na powstały atak, nawet jeżeli napastnik wykorzystał lukę typu zero-day. Napastnik nie jest podłączony do prawdziwego systemu, a zaledwie do jego lustrzanej, odciętej kopii, w której symuluje się pewne działania, mające na celu jak najdłużej utrzymywać przekonanie prawdziwości włamania w umyśle przestępcy. Im dłużej próbuje on dany system złamać, tym więcej czasu służby bezpieczeństwa mają na jego namierzenie. W przeciętnych przedsiębiorstwach mechanizm ten nie jest wykorzystywany zbyt często ze względu na potrzebę zaawansowanej wiedzy administratora, a ponadto jest to metoda stosunkowo młoda.

Kippo jest jednym z przykładów implementacji komputerowego systemu honey-pot, umożliwiającym pełną interakcję napastnika z fałszywym systemem. Zapewnia logowanie w czasie rzeczywistym wszystkich działań włamywacza, wraz z adresacją i statystykami. Najważniejszymi cechami są: pełne odzwierciedlenie systemu operacyjnego dystrybucji linuksa opartej o Debiana z możliwością poruszania się po nim, dodawaniem, usuwaniem i modyfikacją plików. Możliwość utworzenia fałszywej kopii konfiguracji, całkowicie „wiarygodnej" z punktu widzenia hakera (np. m.in. możliwość podłożenia fałszywego pliku haseł użytkowników - /etc/passwd). Pełne zapisywanie przebiegu interakcji napastnika z powłoką systemu (wraz z zapisaniem plików, które ściągał na serwer) - w odseparowanym miejscu na serwerze. Odczyt interakcji może odbywać się już w czasie rzeczywistym incydenty lub po jego zamknięciu.

Łącząc możliwości Kippo razem z platformą do wirtualizacji honeypotów - Honeyd, istnieje możliwość masowego wdrożenia instalacji wielu dozorców w różnych fragmentach pseudo-newralgicznych w SI przedsiębiorstwa.

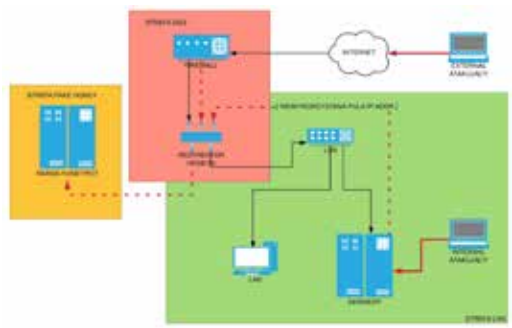


Rys. 1. Typowy schemat implementacji serwera Honeyd opartego o wirtualizację usług

Na rys. 1 został przedstawiony schemat logiczny sieci z zaimplementowaną prostą wersją serwera Honeyd połączonego ze zwirtualizowanymi usługami (serwerami) Kippo. Podejście wirtualizacyjne pozwala zwiększyć skuteczność ochrony sieci informatycznej ze względu na fakt, że minie stosunkowo więcej czasu zanim atakujący zrozumie, że jest w odseparowanej sfałszowanej sieci, dając w ten sposób czas administratorom sieci na dogłębne prześledzenie i monitorowanie kroków napastnika.

Implementacja wersji złożonej

Typowy schemat implementacji serwera Honeyd opartego o pojedyńczą wirtualizację usług jest rozwiązaniem z założenia dobrym, jednakże w celu poprawy skalowalności rozwiązania oraz zapewnieniu większej niezawodności - powinno się wdrażać wersję złożoną. Bezpieczeństwo informatyczne w przedsiębiorstwie powinno być rozumiane jako ciągły proces [7] i w taki sam sposób należy potraktować implementację złożoną, która w jak najszerszym spektrum scenariuszy da administratorowi czas na działanie i ochronę infrastruktury przedsiębiorstwa. Na rys. 2 przedstawiono schemat logiczny sieci komputerowej z zaimplementowaną wersją złożoną farmy honey-pot wraz z centralnym urządzeniem decydującym o transmisji - redyrektorze Honeyd. Jest to pojedynczy serwer usługi Honeyd decydujący o poprawności transmisji w sieci, pełniący rolę czujnika IPS (ang. Intrusion Prevention System). W momencie rozpoznania ruchu jako anomalii (np. poprzez analizę nagłówków transmisji porównując sygnatury lub wykorzystując wcześniej zebrane wzorce gdy sieć działała bez zakłóceń) redyrektor decyduje czy potencjalny ruch przekierować na farmę fałszywych serwerów czy do serwerów rzeczywistych. Wygodnym rozwiązaniem jest połączenie skanowania transmisji z wykrywaniem nieautoryzowanych adresów IP z puli lokalnej, które celowo zostały pozostawione jako nieużywane.



Rys. 2. Schemat implementacji farmy fałszywych serwerów wraz z redyrektorem w strefie DMZ

W podobny sposób można wykorzystać, jako czujnik IPS, samego firewalla w strefie DMZ, który sam w sobie odfiltruje większą część szkodliwego ruchu. Firewall musi być urządzeniem potrafiącym zajrzeć do nagłówka warstwy aplikacji modelu DoD TCP/IP [8] w celu porównania sygnatur z ze znanymi zagrożeniami. W przypadku pojawienia się błędu zero-day, ruch anomalny przepuszczony przez firewall zostanie skierowany do redyrektora honeyd, który następnie przekieruje ruch na farmę honey-potów, klinując w ten sposób infekcję w odizolowanym środowisku.

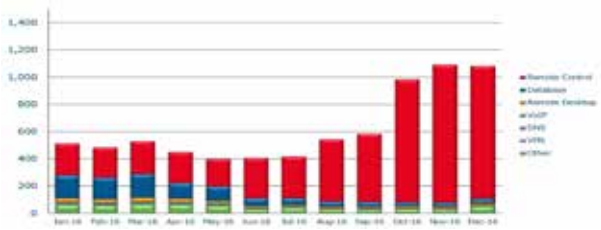
Obserwacja wyników

Po właściwej implementacji farmy serwerów honey-pot można je pozostawić do zbierania statystyk lub monitorować na bieżąco. W tabeli 1 przedstawiono statystyki z okresu jednego roku od implementacji opisywanej farmy, zawierające zestawy najczęściej próbkowanych loginów oraz haseł.

Tab. 1. Zestawienie statystyk próbowanych loginów, haseł oraz unikalnych połączeń IP

Najczęstsze loginy	Najczęstsze hasła	Największa liczba połączeń
root [8510]	password [6510]	202.99.89.69
admin [1440]	passw0rd [1720]	200.61.189.164
test [127]	admin [1335]	78.37.83.203
oracle [96]	toor [496]	218.108.235.86
nagios [49]	qwerty123 [447]	195.14.50.8
mysql [47]	1qazxsw2 [331]	218.80.200.138
guest [43]	12345 [302]	58.222.200.226
info [42]	test [127]	58.18.172.206
user [41]	aaaaaaaaa [40]	119.188.7.174
postgres [39]	p@ssw0rd [17]	119.42.148.10

Z powyższej tabeli można wywnioskować, że w większości przypadków stosowane metody ataku, rozpoczynane w fazie rekonesansu, realizowane są w sposób zautomatyzowany, prostymi narzędziami, wykorzystując typowe łańcuchy danych dla loginów i haseł. Na rys. 3 przedstawiono próby ataków na najczęstsze usługi dostępne na serwerach. Warto zwrócić uwagę, że od października 2016, statystyki znacznie wzrosły co jest prawdopodobnie wynikiem wysokiego skoku ceny kryptowaluty BitCoin na świecie. Przekłada się to bezpośrednio na próbę uzyskania zdalnego dostępu do systemu, więc wykres Remote Control znacznie przewyższa pozostałe próby.



Rys. 3. Statystyki z farmy honey-pot z wykonanych prób ataków na usługi dostępne na serwerach w Internecie

Podsumowanie

Implementacja farmy honeypotów daje możliwość administratorowi na zwiększenie czasu reakcji odpowiedzi na potencjalny atak. Pomimo, że wprawny włamywacz prawdopodobnie

stosunkowo szybko zorientuje się, że ma do czynienia z fałszywym systemem to jednak takie rozwiązanie w znaczący sposób wyklucza ataki automatyczne i wywołane przez script-kiddies (hakerów amatorów) co w znaczny sposób pozwala odsiać nadmierny ruch oraz komunikaty typu false-positive z firewalla. Przede wszystkim warto pamiętać, że proporcjonalnie do tego ile autor rozwiązania włoży wysiłku i zaangażowania w konfigurację i ukrycie farmy, tyle dostanie czasu na możliwą reakcję i ocenę rodzaju i powagi zaobserwowanego zagrożenia lub incydentu. Wartością dodaną rozwiązania jest fakt, że honey-pot stanowi podstawową i aktualną bazę wiedzy w jaki sposób system jest atakowany co daje możliwość zabezpieczenia chronionego systemu przed zaobserwowanymi technikami ataku. Przedstawione w niniejszym artykule statystyki wskazują, że trend prób włamań na typowe dane i usługi, pomimo nieustannego uszczelniania systemów, cały czas utrzymuje się na podobnym poziomie. Dopóki świadomość administratorów i użytkowników nie zostanie zwiększona w zakresie zabezpieczania samych siebie i urządzeń na których pracują dopóty wyszukiwarki typu shodan (http://shodanhq.com) będą gromadziły dane o podatnych urządzeniach, które mogły być skutecznie zabezpieczone po włożeniu niewielkiego wkładu własnego w konfigurację.

W serwisie YouTube, pod adresem wskazanym w bibliografii: [9], autorzy niniejszej publikacji zamieszczają film prezentujący pełną instalację środowiska - oraz - obserwację pierwszej próby włamania i poczynań napastnika.

Literatura

[1] CERT: Raport Roczny z Działalności CERT Polska, ISSN 2084-9079, Warszawa, 2016

[2] http://www.cert.pl

[3] Redmiles E.: Why Installing Software Updates makes us WannaCry, The Conversion US, Scientific American, 2017

[4] Mansfield-Devine S.: Hacking on an industrial scale, Network Security, Elsevier, Issue 9, 2014, Str. 12-16

[5] Wang J., Zeng J.: Construction of large-scale honeynet based on Honeyd, Procedia Engineering, Elsevier, Volume 15, 2011, Str. 3260-3264

[6] Weiner K., Chelst K., Hart W.: Stinging the Detroit criminal: A total system perspective, Journal of Criminal Justice, Elsevier, Issue 3, Volume 12, 1984, Str. 289-302

[7] Adi K., Hamza L., Pene L.: Automatic security policy enforcement in computer systems, Computes and Security, Elsevier, Volume 73, 2018, Str. 156-171

[8] Pandya P.: TCP/IP Packet Analysis, Computer and Information Security Handbook (Second Edition), Morgan Kaufmann, 2013, Str. 499-512

[9] https://www.youtube.com/watch?v=v9kseYy5SII

Dr inż. Michał Podpora, mgr inż. Tomasz Turba, mgr inż. Agnieszka Różańska, dr inż. Aleksandra Kawala-Janik,
Politechnika Opolska

Przegląd zagadnień i zmian związanych z wdrożeniem w życie dyrektywy RODO/GDRP

Ochrona danych osobowych jest zagadnieniem, które w branży energetyki pozornie powinno interesować jedynie podmioty zajmujące się dystrybucją i sprzedażą energii. Pozornie, ponieważ dyrektywa RODO reguluje znacznie więcej niż dotychczasowe przepisy z 1995 r., wprowadzając zupełnie nowe podejście w zakresie prywatności, ochrony danych osobowych i bezpieczeństwa systemów informatycznych. Rozporządzenie RODO przez wielu przedsiębiorców jest uważane za niejasne i nie zawierające konkretnych zaleceń - m.in. ze względu na to, by najnowsze przepisy były jak najmniej zależne od ciągle postępującego rozwoju technologicznego, a także od specyfiki przetwarzania danych w danym przedsiębiorstwie. W niniejszym artykule autorzy postarają się przedstawić zarówno wybrane elementy dyrektywy, jak również ogólną techniczną koncepcję bezpieczeństwa systemów informatycznych - w odniesieniu do specyfiki branży energetycznej.

Wstęp

Europejska reforma ochrony danych osobowych, zwana potocznie jako reforma RODO [1], zaczyna obowiązywać od dnia 25 maja 2018 r. Dyrektywa ta ma za zadanie unowocześnienie regulacji o ochronie danych osobowych, gdyż poprzednie rozporządzenie, obowiązujące od 1995 r., ma coraz mniejsze zastosowanie praktyczne z powodu postępującej cyfryzacji.

Rozporządzenie RODO wnosi szereg zmian w regulacjach o ochronie danych osobowych. Jedną z ważniejszych zmian jest przenoszenie danych - każdy obywatel ma prawo wystąpić do przedsiębiorcy z żądaniem przekazania mu pliku w formacie *.pdf wraz z informacjami, jakie dane dotyczące jego osoby są wykorzystywane w tej firmie. Pozwoli to na łatwą kontrolę danych jakie są udostępniane między firmami i dzięki temu będzie można łatwiej kontrolować co będzie działo się z danymi osobowymi przetwarzanymi przez dany podmiot.

Trudności we wdrożeniu i utrzymaniu

Głównym zadaniem administratora danych osobowych ma być bezwzględne dostosowanie Systemów Informatycznych (SI) tak, aby dokładając wszelkiej staranności kontrolować te dane w sposób rzetelny i stabilny. W razie powstania żądania osób, których dane dotyczą - aby można było je w sposób kontrolowany i bezpieczny m.in. usunąć lub przekazać do innego usługodawcy. Wraz z wprowadzeniem w życie RODO powstaje również obowiązek udzielenia wszelkich informacji na temat danych osobowych zainteresowanego podmiotu oraz udzielenia mu odpowiedzi w terminie 30 dni od daty złożenia zapytania. W łatwy sposób można sobie wyobrazić paraliż instytucji publicz-