NAUKI PODSTAWOWE
CZASOPISMO TECHNICZNE
TECHNICAL TRANSACTIONS
FUNDAMENTAL SCIENCES
WYDAWNICTWO POLITECHNIKI KRAKOWSKIEJ
1-NP/2012
ZESZYT 18
ROK 109
ISSUE 18
YEAR 109

JERZY M. ZACZEK*

EWOLUCJA ZAGROŻEŃ SIECIOWYCH MOTOREM EWOLUCJI SIECIOWYCH SYSTEMÓW BEZPIECZEŃSTWA

NETWORK SECURITY IMPROVEMENT DRIVEN BY THREATS EVOLUTION

Streszczenie

Pojawienie się nowej usługi sieciowej, nowego protokołu sieciowego czy też zmiana podejścia do korzystania z sieci, stanowią nowe wyzwania dla potencjalnych agresorów. Ich realizacja w postaci nowych technik i metod ataków spotyka się z natychmiastową reakcją producentów rozwiązań zabezpieczeń sieciowych. Wprowadzone przez nich zmiany/ulepszenia motywują z kolei agresorów do zwiększenia wysiłków dla znalezienia obejścia nowych zabezpieczeń. I tak domyka się swoiste sprzężenie zwrotne, będące od lat motorem ewolucji sieciowych systemów bezpieczeństwa. W artykule przedstawiono rozwój systemów zabezpieczeń, poczynając od prostych bezstanowych zapór ogniowych aż po najnowsze rozwiązania klasy XTM. Prezentacja spodziewanych w przyszłości kierunków rozwoju zarówno metod ataków, jak i adekwatnych zabezpieczeń oraz wpływ tzw. czynnika ludzkiego na (nie)skuteczność sieciowych systemów bezpieczeństwa stanowi domknięcie całości artykułu.

Słowa kluczowe: bezpieczeństwo sieci, zapora ogniowa, zagrożenia, techniki ataków

Abstract

Implementation of new network services and/or protocols or even change of the rules the network is used by, acts as a challenge for potential aggressors. The new techniques and methods of attacks face each other with immediate response from the vendors of network security solutions. Changes and improvements introduced by them give the aggressors a boost for finding a way around. Briefly presented way from simple stateless firewalls up to sophisticated XTM appliances, shows the evolution of security solutions. Finally, the article presents expected trends for the future security threats and solutions.

Keywords: security threat, network security, firewall, UTM, XTM

* Dr inż. Jerzy M. Zaczek, Wydział Fizyki, Matematyki i Informatyki, Politechnika Krakowska.

1. Wstęp

W początkowym okresie rozwoju sieci komputerowych podstawowym aspektem, na jaki zwracano uwagę w procesie ich projektowania i budowy, były mechanizmy komunikacji. Jedynym celem, jaki przyświecał twórcom pierwszych protokołów sieciowych, było uzyskanie możliwie efektywnej wymiany informacji. Zagadnienia związane z bezpieczeństwem komunikacji (o ile w ogóle uwzględniane) odsuwane były zdecydowanie na dalszy plan – dostatecznie dużo problemów sprawiał sam proces odpowiedniego zaprojektowania i stworzenia podstaw działania sieci. Szybko jednak okazało się, że takie podejście było błędne, a jego efekty negatywnie wpłynęły na bezpieczeństwo transmisji danych, czego skutki odczuwane są do dnia dzisiejszego – ciągle bowiem wykorzystywane są protokoły sieciowe stworzone we wczesnych latach 70. ubiegłego stulecia.

Wraz z rozwojem sieci komputerowych, szczególnie globalnej sieci Internet, zaczęły powstawać i rozwijać się różnego rodzaju zagrożenia zewnętrzne, rozpowszechniające się wraz z jej wykorzystaniem. Bardzo szybko okazało się, że konieczne jest zabezpieczenie się także przed tego typu zagrożeniami. Popularność przeprowadzania ataków z wykorzystaniem sieci komputerowych szybko rosła. Wynikało to z faktu przyłączania do sieci coraz większej liczby komputerów bez dbałości o ich bezpieczeństwo. W początkach rozwoju sieci ilość użytkowników oraz dostępnych zasobów była na tyle niewielka, że wszelkiego rodzaju zachowania niepożądane nie miały sensu. Wraz ze wzrostem dostępnych zasobów zwiększała się częstotliwość przeprowadzanych ataków.

2. Historia zabezpieczeń sieciowych

Rozwój sieci komputerowych spowodował, iż zaczęto w nich umieszczać (i udostępniać) na tyle cenne zasoby, że nieuniknione stały się próby dostępu do nich także osób nieuprawnionych. Spowodowało to konieczność stworzenia metod zabezpieczania zasobów sieciowych. Dla umiejscowienia rozwoju systemów bezpieczeństwa w historii sieci komputerowych warto przytoczyć kilka faktów z początkowej historii rozwoju sieci Internet [1]:

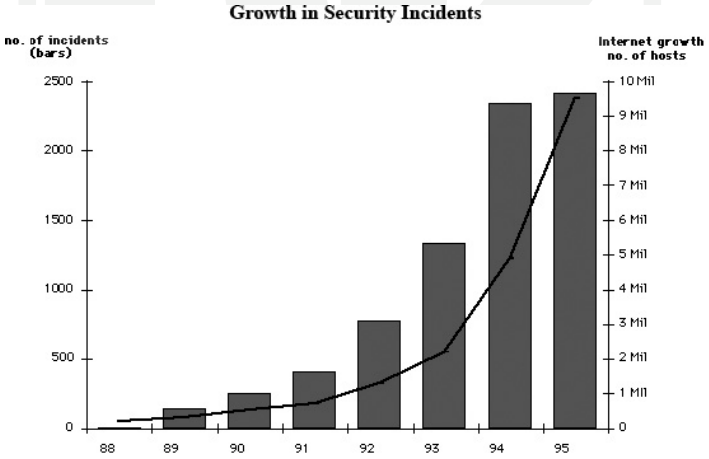
- 1969 powstaje sieć ARPAnet (ang. *Advanced Research Projects Agency Network*) uznawana za bezpośredniego prekursora sieci Internet
- 1981 stworzona zostaje sieć CSNET (ang. *Computer Science NETwork*)
- 1983 stworzona zostaje brama (ang. *gateway*) pomiędzy ARPAnet a CSNET; fakt ten uważa się za początek istnienia Internetu takiego, jakim znamy go dzisiaj
- 1984 powstaje system nazw domenowych DNS (ang. *Domain Name System*)
- 1985 rejestracja pierwszej nazwy domenowej (domeny) symbolics.com
- 1987 powstaje jeden z pierwszych artykułów w szeroki sposób omawiający tematykę filtrowania ruchu sieciowego [2]
- 1988 w sieci pojawia się pierwszy wirus, który zaraża dużą liczbę komputerów (blisko 6000 maszyn, czyli około 10% ówczesnej sieci)
- 1994 w wersji 1.1 jądra systemu operacyjnego Linux zaimplementowana zostaje funkcjonalność filtrowania pakietów

Znacznie wcześniej (na przełomie lat 80. i 90.) funkcjonalność taka pojawiła się w systemie operacyjnym UNIX. Pojawiło się wiele implementacji filtrowania pakietów, pierwszej

funkcjonalności dedykowanej zagadnieniom bezpieczeństwa sieci [3]. Wiele firm rozpoczęło produkcję i sprzedaż opartych na niej programowych rozwiązań typu zapora sieciowa (ang. *firewall*), przeznaczonych do zastosowań komercyjnych [4].

Pierwsze firewalle były zaporami bezstanowymi (ang. *stateless firewall*). Zajmowały się analizą wyłącznie nagłówków pakietów, nie potrafiły zatem przypisać danego pakietu sieciowego do konkretnej sesji i każdy filtrowany pakiet traktowały jako osobny byt. Decyzja o przepuszczeniu lub odrzuceniu pakietu podejmowana była w zasadzie wyłącznie w oparciu o adresy nadawcy i odbiorcy. Firewalle drugiej generacji były już filtrami stanowymi (ang. *stateful firewall*). Potrafiły przypisać poszczególne pakiety sieciowe do określonych sesji. Wymagało to utrzymywania w pamięci maszyny tablicy połączeń sieciowych, co przy ograniczonej ilości pamięci, a dużej liczbie połączeń mogło stanowić poważny problem. Fakt ten był podstawą jednego z pierwszych ataków, jakie przeprowadzane były na systemy ochrony. Były to ataki typu DoS (ang. *Deny of Service*), których celem było unieszkodliwienie filtra pakietów poprzez przepełnienie tablicy połączeń.

Z czasem okazało się, że rozwiązania programowe nie są wystarczające. Różnorodność stosowanego sprzętu (rozwiązania tego typu były często instalowane na już posiadanych przez użytkowników komputerach), ich różna, często niewystarczająca wydajność obliczeniowa, niewystarczająca ilość pamięci operacyjnej oraz wysoka zawodność doprowadziły – w sytuacji lawinowo rosnącej liczby incydentów bezpieczeństwa (rys. 1.) – do powstania sprzętowych rozwiązań systemów bezpieczeństwa. Jednymi z pierwszych rozwiązań, jakie pojawiły się na rynku w 1996 roku, były urządzenia o nazwie Firebox firmy Seattle Software Labs [5] (wcześniej Mazama Software Labs, zaś od 1997 roku WatchGuard® Technologies – firma, która jest do dzisiaj jednym z czołowych producentów rozwiązań bezpieczeństwa). Również w 1996 roku powstał pierwszy firewall stworzony na bazie układu ASIC przez chińskiego inżyniera Ken Xie [6]. Założył on firmę Fortinet, w której wciąż pełni rolę prezesa. Firma ta, podobnie jak WatchGuard® Technologies, nadal pozostaje w czołówce producentów rozwiązań bezpieczeństwa.



Rys. 1. Wzrost liczby incydentów bezpieczeństwa w latach 1988-1995 [7]

Fig. 1. Growth in Security Incidents [7]

Rozwiązania sprzętowe wraz z upływem czasu ewoluowały. W niedługim czasie wyposażone zostały w dodatkowe funkcje bezpieczeństwa. Urządzenia bezpieczeństwa realizujące jedynie filtrowanie pakietów nie zapewniały należytego poziomu zabezpieczenia, co wynikało z ewolucji zagrożeń. W roku 2004 Charles Kologdy pracownik firmy International Data Corporation, zaproponował termin UTM (ang. *Unified Threat Management*) na określanie zintegrowanych rozwiązań bezpieczeństwa. Termin ten został przyjęty przez środowisko i jest powszechnie stosowany. Urządzenie, które może być nazywane tym terminem, musi oprócz funkcjonalności filtrowania pakietów realizować także dodatkowe funkcje bezpieczeństwa, takie jak:

– filtrowanie ruchu sieciowego oprogramowaniem antywirusowym,
– ochrona antyspamowa,
– ochrona przed włamaniami (ang. *Intrusion Detection System* oraz *Intrusion Prevention System*),
– filtrowanie treści w protokole http (ang. *Web Blocking*).

W roku 2008 tenże sam Charles Kologdy zaproponował nową nazwę dla urządzeń realizujących większą liczbę funkcjonalności niż rozwiązania klasy UTM – XTM (ang. *eXtensible Threat Management*). Określeniem XTM oznacza się zintegrowane rozwiązania bezpieczeństwa, które oprócz funkcjonalności realizowanej przez urządzenia UTM muszą także zapewniać (co najmniej):

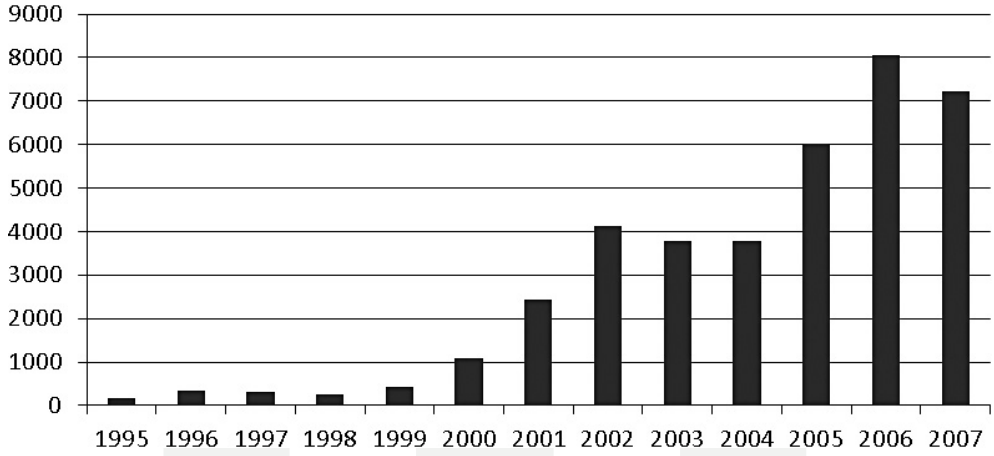
– centralne logowanie i korelację zdarzeń,
– kontrolę dostępu do zasobów sieciowych,
– zarządzanie zagrożeniami,
– ochronę bazującą na reputacji.

W praktyce rozwiązania klasy UTM, czy XTM realizują znacznie większy zbiór funkcjonalności sieciowych, zapewniających możliwie wysoki poziom bezpieczeństwa. Aktualnie na rynku, w miejscu prostych rozwiązań typu firewall dostępne są właśnie tego typu rozwiązania.

3. Ewolucja zagrożeń motorem napędowym ewolucji zabezpieczeń sieciowych

Zagrożenia sieciowe ciągle ewoluują a ich ilość i różnorodność nieprzerwanie rośnie. Na rysunku 2 przedstawiony jest wykres wzrostu ilości skatalogowanych podatności w latach 1995 - 2007. Każda podatność może zostać wykorzystana w ataku. Im więcej znanych podatności, tym większe prawdopodobieństwo przeprowadzenia ataków, które wraz z upływem czasu stają się coraz bardziej wyrafinowane, korzystają z nowych technik i metod przeprowadzania. Ewolucja ataków jest wynikiem ewolucji systemów zabezpieczeń. Kiedy systemy zabezpieczeń zaczynają chronić przed zagrożeniami, atakujący tworzą nowe metody ataku. W efekcie tego następuje ewolucja systemów bezpieczeństwa, które w odpowiedzi na nowe typy ataków realizują nowe sposoby ochrony przed nimi. Jest to więc rodzaj specyficznego „sprzężenia zwrotnego" gwarantującego ciągły, nierozerwalnie ze sobą związany rozwój zarówno metod ataków jak i sposobów ochrony.

Powstaje pytanie: skąd bierze się aż tyle podatności, a co za tym idzie ataków? Powodów jest wiele. Po pierwsze podatności są najczęściej wynikiem błędów w oprogramowaniu. Tworzy się coraz więcej różnorodnego oprogramowania. Oprogramowanie to niejed-



Rys. 2. Ilość skatalogowanych podatności w latach 1995-2007 (opracowanie własne na podstawie [8])

Fig. 2. Total number of catalogued vulnerabilities, 1995-2007 [8]

nokrotnie jest bardzo zaawansowane technologicznie, a co za tym idzie skomplikowane. Im większa objętość kodu oprogramowania, tym większa jest szansa na popełnienie błędu, ponadto poziom jego skomplikowania zwiększa prawdopodobieństwo popełnienia błędu.

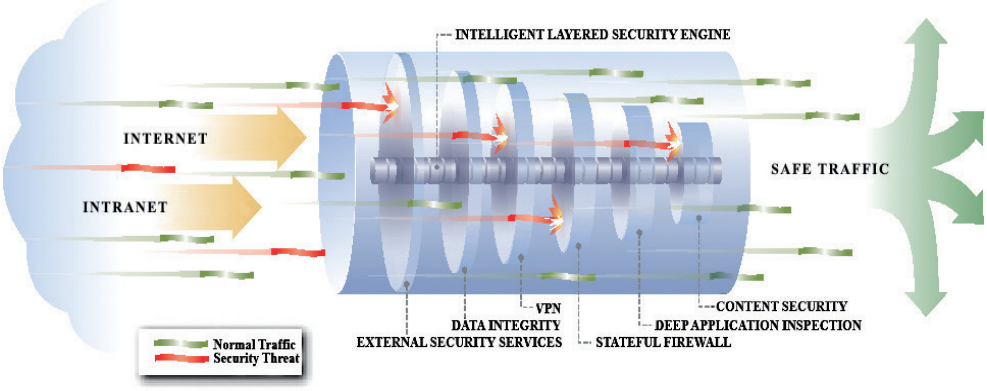
Podatności same w sobie nie powodują zwiększenia liczby ataków – gdyby nie zostały odkryte, nigdy nie zostałyby wykorzystane do ich przeprowadzania. Rodzi się więc kolejne pytanie: kto i po co wyszukuje takie podatności. Na pewno prace taką wykonują osoby, które dbają o jakość oprogramowania. Wyszukanie podatności przez te osoby nie skutkuje jednakowoż problemami z bezpieczeństwem, wręcz przeciwnie: ich działanie doprowadza do naprawy i usunięcia niebezpiecznych błędów. Inną grupą osób wyszukujących podatności są potencjalni włamywacze, pragnący wykorzystać podatności do przeprowadzenia ataku. Motywacja ich działania może być różna. Może to być chęć zemsty, chęć osiągnięcia jakiegoś celu politycznego czy religijnego, chęć uzyskania korzyści majątkowych, czy wręcz chęć udowodnienia, że potrafią przeprowadzić atak.

Zagrożenia od początków istnienia sieci Internet w dużym stopniu zmieniły się. Przede wszystkim przesunęły się wyżej w siedmiowarstwowym modelu sieci. Pierwsze zagrożenia dotyczyły głównie warstw sieciowej oraz transportowej. Przed tego typu zagrożeniami chroniły proste systemy typu *stateful firewall* (a w szczególnych przypadkach nawet *stateless firewall*). Gdy zaczęto je powszechniej stosować rozwinęły się inne metody ataków, które przeprowadzane są w wyższych warstwach, przede wszystkim w warstwie aplikacji. Paradoksalnie, rozwój sieci pozwalający na swobodny dostęp do zasobów w niej umieszczanych, spowodował obniżenie poziomu bezpieczeństwa. Pierwsze ataki przeprowadzane były przez osoby, które doskonale wiedziały, jak atak przeprowadzić. Musiały posiadać sporą wiedzę na temat pracy protokołów czy systemów sieciowych, by przeprowadzić atak. Tylko wybitne jednostki potrafią wyszukiwać podatności typu *Zero Day*. Podatności takie to podatności wcześniej nieznane, których wykorzystanie najprawdopodobniej pozwoli na przeprowadzenie udanego ataku. Ponadto osoby przeprowadzające ataki same tworzyły narzędzia służące do przeprowadzenia ataku, udostępniając je później innym osobom (także

z wykorzystaniem sieci). Kiedy narzędzia służące do przeprowadzania ataku stają się publicznie dostępne, są wykorzystywane przez osoby, które nie posiadają odpowiedniej wiedzy, by samemu zaplanować i przeprowadzić atak. Powoduje to, że znacznie większa liczba osób może próbować takie ataki przeprowadzać, co doprowadza do znacznego zwiększenia ich wolumenu. Sytuacja taka wymaga z kolei od systemów bezpieczeństwa istotnie większej mocy obliczeniowej, gdyż muszą one reagować na znacznie większą liczbę incydentów. Trend ten doprowadził do powstania wysoce specjalizowanych, sprzętowych rozwiązań zabezpieczających sieciowe systemy komputerowe.

Powstanie gotowych narzędzi służących do przeprowadzania znanych ataków spowodowało lawinowy wzrost ich liczby. Ochrona przed takimi atakami jest stosunkowo łatwa, gdyż wiadomo, jak są one przeprowadzane, a co za tym idzie, wiadomo, co powinno zostać zablokowane. Systemy, których zadaniem jest ochrona przed atakami, to tzw. systemy wykrywania włamań IDS (ang. *Intrusion Detection Systems*). W typowej postaci systemy te wyposażone są w zbiory sygnatur, które służą do wykrywania niepożądanych zachowań. Jeżeli aktualnie obserwowany ruch sieciowy pasuje do sygnatury, uznaje się, że przeprowadzany jest atak. O fakcie tym informowany jest administrator systemu, możliwe jest także automatyczne podjęcie akcji, np. zablokowanie ruchu sieciowego. Tego typu automatyzację podejmowanych działań, a co za tym idzie krótszy czas reakcji na zagrożenie, realizują systemy ochrony przed włamaniami IPS (ang. *Intrusion Prevention Systems*). Sprzętowe rozwiązania bezpieczeństwa, aby mogły zostać uznane za rozwiązanie klasy UTM, muszą być wyposażone w moduł IPS lub przynajmniej IDS.

Innym zagrożeniem, które zaczęło rozprzestrzeniać się w sieci, było (i jest nadal) wszelkiego rodzaju szkodliwe oprogramowanie, a więc wirusy, robaki, *malware*i inne. Oprogramowanie tego typu przenoszone było wcześniej na nośnikach danych – wykorzystanie sieci Internet do wymiany danych spowodowało, że czas rozprzestrzeniania się zagrożenia znacznie się skrócił, a liczba zarażonych komputerów wzrosła wielokrotnie. Odpowiedzią na to zagrożenie, ze szczególnym uwzględnieniem mechanizmu propaga-



Rys. 3. Wielopoziomowa struktura ochrony danych w systemach klasy UTM (opracowanie własne na podstawie [9])

Fig. 3. Multilayered Security Structure [9]

cji, było wyposażenie zintegrowanych systemów bezpieczeństwa w oprogramowanie antywirusowe. Pozwala to na skanowanie „w locie" ruchu sieciowego i ochronę przed niebezpiecznym kodem.

Podobne rozszerzenie funkcjonalności sprzętowych rozwiązań bezpieczeństwa nastąpiło w przypadku odpowiedzi na rosnące zagrożenie zalewem niechcianych wiadomości pocztowych (ang. *spam*). W celu ochrony użytkowników przed niechcianymi treściami, rozsyłanymi z użyciem poczty elektronicznej, wprowadzono ochronę antyspamową. Ochrona ta, realizowana na różne sposoby, ma na celu odfiltrowanie niechcianych wiadomości pocztowych i w zależności od kwalifikacji poszczególnych komunikatów, następuje (w typowych konfiguracjach) ich odrzucenie, oznaczenie lub przesłanie do kwarantanny.

Jak wcześniej wspomniano, wraz z powstawaniem kolejnych usług świadczonych w sieci Internet wzrosła liczba ataków przeprowadzanychw wyższych warstwach siedmiosegmentowego modelu sieci. Szczególnie chodzi tutaj o warstwę aplikacji. Konieczna stała się ochrona w tej warstwie, zwłaszcza najczęściej stosowanych protokołów, takich jak HTTP, SMTP, FTP, DNS, HTTPS, czy ostatnio także protokołów VoIP, a więc H.323 oraz SIP. Ochronaz wykorzystaniem proxy filtrujących pozwala na analizę nie tylko tego, czyw danym protokole przesyłane są dane, ale także jakie to są dane i jak są przesyłane. Przykładowo w proxy filtrującym dla protokołu HTTP możliwe jest zabronienie przesyłania danych w postaci dokumentów tekstowych. Proxy filtrujące będzie w stanie wychwycić tego typu dane i zablokować je, podczas gdy np. pliki typu PDF w dalszym ciągu będą mogły być przesyłane. Proxy filtrujące pozwala na kontrolę nie tylko treści przesyłanych danych, ale samego zachowania się protokołu, co pozwala np. na ograniczenie metod oraz poleceń protokołu stosowanych do przesyłania danych. Proxy filtrujące analizują transmisję w celu wykrycia, czy jest ona zgodna ze standardami danego protokołu. Jeśli odbiega od standardu, może zostać przerwana. Pozwala to na zabezpieczenie się przed próbami ukrycia ruchu sieciowego w innym, pozornie bezpiecznym protokole (tzw. steganografia sieciowa); przykładowo ukrywanie ruchu IP (a więc dowolnego ruchu w warstwach wyższych) w komunikatach DNS.

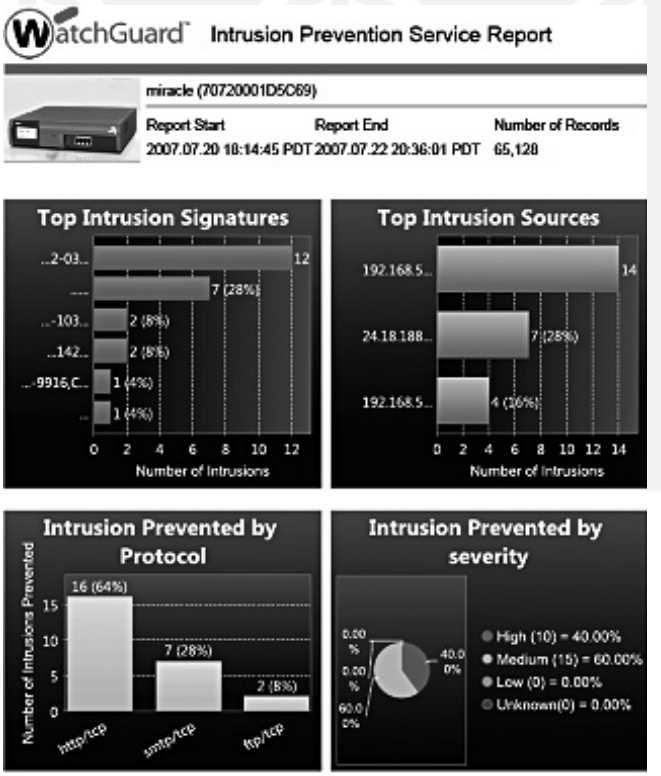
Sprawa filtrowania ruchu w warstwie aplikacji komplikuje się w przypadku wykorzystania bezpiecznej wersji jakiegoś protokołu, na przykład użycie HTTPS w miejsce HTTP. Filtrowanie treści przesyłanych w tego typu protokołach przeczy w istocie rzeczy samej ich idei — tworzeniu tych protokołów przyświeca idea uczynienia ich bezpiecznymi, czyli uniemożliwiającymi przechwycenie danych w trakcie transmisji. Aby możliwe było filtrowanie danych w protokole HTTPS, konieczne jest *de facto* prowadzenie w trakcie filtrowania działania analogicznego do ataku typu *Decryption-in-the-Middle*. Zintegrowane, sprzętowe rozwiązania bezpieczeństwa, przy odpowiedniej konfiguracji potrafiąw ten sposób filtrować protokół HTTPS na takim samym poziomie, na jakim jest to możliwe dla HTTP.

Korzystanie z nowych sposobów przesyłania danych (ogólnie: komunikowania się) w sieci powoduje powstanie nowych potencjalnych kierunków ataków. Celem tego typu nowych kierunków ataków mogą być wszelkiego rodzaju sieci P2P, komunikatory internetowe, a ostatnio zwłaszcza sieci i portale społecznościowe. Podstawowe problemy, jakie wynikają z ich wykorzystywania, to duża popularność, a co za tym idzie – duże zainteresowanie wśród potencjalnych intruzów.

Popularność ta wynika w dużej mierze z rodzaju treści przesyłanych w tych sieciach. Są one interesujące dla ich użytkowników ze względu na charakter (informacje o wydarze-

niach dotyczących jakiejś grupy społecznej czy dystrybucja oprogramowania w sieciach P2P) i tym samym stanowią potencjalny cel ataków. Innym problemem dotyczącym tej grupy protokołów sieciowych jest ich rozproszony charakter i pewna dowolność komunikacji. Aplikacje korzystającez tego typu protokołów komunikują się najczęściej w sposób bardzo elastyczny. Rzadko kiedy wykorzystywane są stałe porty czy adresy konkretnych serwerów. Najczęściej parametry te są zmienne. Pojawia się zatem problem filtrowania tego typu ruchu. Zazwyczaj nie da się go ograniczyć poprzez zablokowanie konkretnych portów czy adresów IP. Konieczne jest inne działanie, podobne do metod wykorzystywanych w systemach IDS, a więc wyszukiwanie w komunikacji sieciowej (na dowolnych portach) ruchu, który pasuje do danego protokołu. Analizowane są charakterystyczne cechy, pozwalające na rozróżnienie poszczególnych protokołów. Gdy ruch taki zostanie wychwycony, może zostać zablokowany. Urządzenia sprzętowe realizują tego typu zadania z użyciem funkcjonalności kontroli aplikacji (ang. *Application Control*).

Obrona przed wszelkiego rodzaju zagrożeniami możliwa jest oczywiście tylko w sytuacji, gdy zostaną one wykryte. Ma to szczególne znaczeniew przypadku nowych zagrożeń (zagrożenie już rozpoznane posiadają swoje sygnatury w systemach IPS). Wykrywanie zagrożeń wymaga z kolei nieustannego monitorowania sieciw celu analizy ruchu



Rys. 4. Przykładowe raporty systemu IPS (opracowanie własne na podstawie [9])

Fig. 4. IPS Reports – examples [9]

sieciowego. Analiza taka może udzielić odpowiedzi na pytanie, czy w sieci aktualnie przeprowadzany jest atak. Monitorowanie sieci, przede wszystkim ze względu na dużą ilość przesyłanych danych, nie jest zadaniem prostym. Konieczne jest wykorzystywanie wyspecjalizowanych narzędzi, których zadaniem jest zbieranie informacji o ruchu sieciowym, a następnie generowanie raportów obrazujących stan sieci. Raporty mogą wskazać nietypowe zachowania, świadczące o prowadzonym ataku. Zintegrowane rozwiązania zabezpieczające sieć komputerową wyposażane są w moduły zbierania informacji o ruchu sieciowym oraz moduły raportowania pozwalające na realizację ww. analizy. Na rysunku 4. przedstawiono przykładowe raporty generowane przez lidera [10] rynku rozwiązań IPS, firmę WatchGuard® Technologies.

W ostatnich latach można zaobserwować znaczny wzrost popularności urządzeń mobilnych. Organizacje (firmy) wyposażają swoich pracowníkóww urządzenia, które pozwalają na zdalną pracę z niemal dowolnego miejsca. Konieczne jest zapewnienie bezpiecznego kanału transmisyjnego pomiędzy urządzeniem mobilnym a zasobami znajdującymi się w siedzibie firmy. Funkcjonalność taka, wcześniej wykorzystywana do bezpiecznego łączenia rozproszonych geograficznie oddziałów firmy, realizowana jest przez tunele VPN. Sprzętowe rozwiązania zabezpieczania sieci umożliwiają zestawianie tuneli VPN pomiędzy różnymi urządzeniami bezpieczeństwa (w przypadku łączenia oddziałów) lub pomiędzy oprogramowaniem zainstalowanym na urządzeniu mobilnym, a urządzeniem bezpieczeństwa (zdalny pracownik).

4. Ewolucja zabezpieczeń sprzętowych

Jak wcześniej wspomniano, ewolucja zabezpieczeń sprzętowych wynikaz ewolucji zagrożeń i typów przeprowadzanych ataków, jako naturalna konsekwencja chęci ochrony przed nimi. Możliwe są dwie drogi rozwoju systemów zabezpieczeń. Pierwsza to tworzenie zintegrowanych systemów,w przypadku których jedno rozwiązanie sprzętowe realizuje wiele funkcji. Drugą możliwą drogą rozwoju jest tworzenie osobnych urządzeń realizujących pojedyncze funkcjonalności.

Obie drogi rozwoju posiadają zalety i wady. W przypadku rozwiązań zintegrowanych jedną z zalet jest z pewnością uproszczone zarządzanie. Znacznie łatwiej i wygodniej jest zarządzać pojedynczym rozwiązaniem niż ich zbiorem. Zintegrowane rozwiązania ułatwiają także współprace pomiędzy poszczególnymi modułami. System IPS, realizując swoją rolę, musi wpływać na konfigurację zapory sieciowej (w celu zablokowania niepożądanego ruchu sieciowego). Realizacja tego zadania jest stosunkowo prosta w przypadku, gdy oba moduły pracują w oparciu o wspólną, zintegrowaną platformę. Nie bez znaczenia jest także aspekt ekonomiczny. Platformy zintegrowane są z reguły tańsze (zarówno w zakupie, jak i późniejszym utrzymaniu) od platform dedykowanych.

Podstawową wadą systemów zintegrowanych jest z kolei problem ich wydajności. Rozwiązania te muszą świadczyć jednocześnie wiele usług bezpieczeństwa, co niejednokrotnie wiąże się z koniecznością wykonywania licznych, złożonych obliczeniowo operacji (np. jednoczesne skanowanie w locie ruchu programem antywirusowym i szyfrowanie danych przesyłanych kanałem VPN). Odpowiedzią na problemy wydajnościowe może być rozdzielenie realizacji poszczególnych funkcjonalności na oddzielne, pojedyncze rozwią-

zania. Dedykowane rozwiązania oprócz większej wydajności posiadają także zazwyczaj większą funkcjonalność, niż moduły w platformach zintegrowanych. Podejście takie jest jednak znacznie trudniejsze w zarządzaniu i zdecydowanie droższe.

W praktyce okazuje się, że obrana została droga pośrednia. Tworzy się rozwiązania zintegrowane, realizujące równocześnie wiele funkcjonalności bezpieczeństwa. Jeśli jednak okazuje się, że rozwiązania takie nie są w stanie sprostać wymaganiom wydajnościowym, to albo tworzy się klastry takich urządzeń (w celu zwiększenia wydajności poprzez rozproszenie realizacji różnych zadań), albo do wykonywania zadania najbardziej obciążającego, czy też najbardziej istotnego z punktu prowadzenia działalności biznesowej danej organizacji, stosuje się dedykowane urządzenia. Przykładem takiego połączenia rozwiązań może być wykorzystanie zintegrowanego rozwiązania do ochrony zasobów oraz dedykowanego rozwiązania do tworzenia tuneli VPN dla użytkowników mobilnych.

Rozwiązania sprzętowe na przestrzeni lat ewoluowały od prostych zapór sieciowych, poprzez zintegrowane urządzenia klasy UTM, aż do rozwiązań XTM. Ewolucja ta, wymuszona rozwojem zagrożeń, powodowała dodawanie kolejnych funkcjonalności — produkty ewoluowały w taki sposób, by spełniać wymagania rynku. Część funkcjonalności została dodana w celu ułatwienia zarządzania (np. możliwość zarządzania produktem z wykorzystaniem różnych interfejsów), czy realizacji funkcji sieciowych, które nie mają bezpośredniego wpływu na bezpieczeństwo, jak na przykład obsługa tzw. kształtowania ruchu (ang. *traffic shaping*). Oprócz rozwiązań UTM czy XTM powstały inne grupy rozwiązań sprzętowych, dedykowane do wykonywania specyficznych funkcji. Przykładem tego typu rozwiązań są urządzenia SSL VPN Gateway czy Content Filtering.Te dwie klasy urządzeń są obecnie reprezentowane w portfolio wielu producentów.

Rozwiązania SSL VPN Gateway służą do zestawiania bezpiecznego kanału transmisyjnego z dowolnej maszyny (nawet niezaufanej) i z dowolnej sieci. Pozwalają z użyciem jedynie przeglądarki internetowej na uzyskanie bezpiecznego dostępu do chronionych zasobów. Rozwiązania te jednocześnie wyposażone są w funkcje pozwalające na analizę poziomu bezpieczeństwa maszyny, z której następuje połączenie. Tylko jeżeli maszyna ta spełnia postawione wcześniej warunki, połączenie zostanie zestawione, w każdym innym przypadku nie będzie to możliwe. Dodatkowo urządzenia tej klasy w momencie zakończenia zdalnej sesji wykonują wiele operacji w celu usunięcia wszelkich danych, które mogły zostać zapisane na komputerze (zarówno danych tymczasowych, jak i danych pobieranych przez użytkownika). Rozwiązania te tworzone są jako dedykowany sprzęt przede wszystkim po to, by zapewnić odpowiednią wydajność, umożliwiającą zestawianie dużej ilości (np. kilku tysięcy) jednoczesnych połączeń.

Inną klasą dedykowanych rozwiązań są rozwiązania Content Filtering. Podobnie jak w przypadku SSL VPN Gateway, podstawową motywacją tworzenia tego typu rozwiązań jako niezależnych urządzeń jest chęć zapewnienia odpowiedniej wydajności. Filtrowanie ruchu sieciowego w warstwach wyższych wymaga dużej mocy obliczeniowej (zwłaszcza gdy konieczne jest filtrowaniez wykorzystaniem programu antywirusowego czy antyspamowego). Dedykowane rozwiązania potrafią zapewnić odpowiednią wydajność, oferując dodatkowo możliwość skanowania przesyłanych treści w celu wykrycia incydentów wycieku danych. Pozwala to na ochronę przed nieuczciwymi pracownikami, którzy mogą próbować wyprowadzić cenne dane a także przed zwykłymi błędami pracowników, którzy cenne dane mogą (nieświadomie) przesłać np. pod omyłkowo podany adres poczty elektronicznej.

5. Spodziewany rozwój zabezpieczeń w przyszłości

Rozwój zabezpieczeń sprzętowych w najbliższym czasie będzie prawdopodobnie obejmował trzy główne kierunki. Po pierwsze rozwiązania sprzętowe muszą reagować na zmiany w komunikacji sieciowej. W ostatnim czasie wzrasta w sieci ruch wykorzystujący protokół IPv6. Część rozwiązań sprzętowych ciągle nie wspiera tego protokołu, niektóre wspierają go tylko częściowo. Przewiduje się, że w przeciągu najbliższych lat udział ruchu IPv6 będzie wzrastał – konieczne zatem będzie zabezpieczanie także tego typu ruchu sieciowego.

Kolejnym kierunkiem rozwoju będzie z pewnością reakcja na nowe zagrożenia. Jednym z takich zagrożeń są ataki typu APT (ang. *Advanced Persistent Threats*). Są to ataki charakteryzujące się wysoką skutecznością, wynikającą przede wszystkim z motywacji. Ataki przeprowadzane są w celu osiągnięcia dużych korzyści finansowych czy politycznych bądź też z pobudek religijnych. Jak wiadomo, są to jedne z najsilniejszych motywacji. Znane są z innych dziedzin sytuacje, gdzie takie właśnie motywacje pozwalają osiągać najtrudniejsze cele – są to w końcu motywacje działań doprowadzających ostatecznie do wybuchu wojen czy przeprowadzania ataków terrorystycznych.

Ataki APT wykorzystują bardzo wyrafinowane i nietypowe techniki propagacji zagrożeń. Są atakami prowadzonymi w sposób pozwalający na długotrwałe pozostawanie w ukryciu. Przeprowadzane są przeciwko dokładnie określonym celom – nie ma tutaj przypadkowości w wyborze celu. Są bardzo niebezpieczne, ze względu na bezwzględną skuteczność. Nie liczy się czasi poniesione koszty, a osiągnięty cel. Ataki tego typu przeprowadzane są przez specjalistów w tej dziedzinie. Tylko oni są w stanie tworzyć nowe metody rozprzestrzeniania się zagrożeń.

Ochrona przed atakami APT jest bardzo trudna. Wynika to z ich nietypowej metodologii i silnej motywacji agresora. Wydaje się, że rozwiązania sprzętowe muszą rozwinąć się w taki sposób, by pozwalać na wykrywanie ataków APT. Wykrywanie nieznanych wcześniej ataków jest zagadnieniem trudnym (podobnie jak tworzenie nowych metod czy technik ataku). Pomocne mogą się tutaj okazać systemy HoneyPot. Systemy te pozwalają realizować dwa podstawowe zadania. Po pierwsze mogą udostępniać potencjalnemu włamywaczowi treści, które on może uznać za cenne, a które w rzeczywistości takimi nie są. Systemy HoneyPot często udostępniają fałszywe dane, które mogą zainteresować włamywacza. Jego uwaga zostanie odwrócona od faktycznie istotnych zasobów, co pozwoli na bezpieczne śledzenie jego działań i w efekcie umożliwi jego identyfikację. Ponadto włamywacz, który zainteresuje się fałszywym systemem (systemy HoneyPot udają, że są tymi chronionymi), nie będzie atakował systemu chronionego. Śledzenie działalności włamywacza pozwala także na analizę technik jego działania, co perspektywicznie może posłużyć identyfikacji nowych zagrożeń. Wiedza zdobyta w ten sposób może także pozwolić na tworzenie i rozwijanie innych metod zabezpieczania się przed atakiem (np. stworzenie nowych sygnatur dla systemów IPS). Wydaje się, że narzędzia, które pozwolą na identyfikacje nowych, nieznanych wcześniej zagrożeń i metod ataków, stanowią przyszłą ścieżkę rozwoju zintegrowanych urządzeń zabezpieczających.

Trzecim ze spodziewanych kierunkiem rozwoju (który już został zapoczątkowany) jest realizacja dostępu do zasobów, opierająca się na tożsamości użytkowników [11]. Podstawowym elementem decydującym o tym, czy dane urządzenie ma uzyskać dostęp do zasobu, przestanie być jego adres IP. W coraz bardziej mobilnym świecie podejście takie traci

sens, gdyż bardziej istotny staje się fakt, kto danego urządzenia używa. Wydaje się, że naturalną konsekwencją takiego podejścia będzie wprowadzenie autentykacji na wszelkiego rodzaju urządzeniach. Część obecnych rozwiązań oferuje już autentykację, ale jest ona częstokroć niewygodna dla użytkowników (wymaga np. zalogowania się na dedykowanej stronie WWW). Rozwój w tej dziedzinie powinien doprowadzić do ułatwienia tego procesu, np. poprzez wprowadzenie metod transparentnej autentykacji (niektóre rozwiązania oferują już dzisiaj takie funkcje, jednakże tylko dla wybranych systemów autentykacji).

Dostęp do zasobów realizowany z wykorzystaniem tożsamości użytkowników to nie tylko zwiększenie poziomu bezpieczeństwa. To także zwiększenie łatwości zarządzania zasobami i możliwości monitorowania działalności użytkowników, a co za tym idzie łatwiejsze monitorowanie pracy sieci. Wszelkiego rodzaju raporty (tworzone równolegle z monitorowaniem) zawierać bowiem mogą nazwy użytkowników, a nie adresy IP. Ponadto rozprzestrzenianie się różnego rodzaju zagrożeń będzie utrudnione, gdyż dostęp do zasobów wymagać będzie dokonania wcześniejszej autentykacji. Również zarządzanie zasobami w pewnych warunkach może ulec ułatwieniu. Zależnie od tego, kto korzysta z danego urządzenia, może posiadać różne prawa dostępu – nie ma konieczności każdorazowego ich modyfikowania, gdy zmienia się użytkownik tego urządzenia.

6. Znaczenie ‘czynnika ludzkiego’ w systemach bezpieczeństwa

Systemy zabezpieczające zasoby dostępne w sieciach komputerowych są niezwykle istotne dla procedur ich ochrony przed niepowołanym dostępem. Niestety samo ich stosowanie, nawet w najbardziej świadomy i wyrafinowany sposób, nie uchroni zasobów przed nierozważnymi działaniami uprawnionych użytkowników. Systemy takie nie są w stanie w pełni zabezpieczyć przed nieuczciwą działalnością zaufanego pracownika lub jego szkodliwymi zachowaniami wynikającymi po prostu z nieświadomości. Typowym przykładem może być tutaj zalecane czy wręcz wymagane korzystanie z protokołu HTTPSw miejsce standardowego HTTP do komunikacji np. z systemami bankowości elektronicznej. Sam protokół nie zapewni bezpiecznego dostępu, jeśli użytkownik nie będzie korzystał z niego świadomie (czyli nie zweryfikuje poprawności certyfikatu). Nierozważne kliknięcie przycisku OK w pojawiającym się oknie dialogowym z informacją o nieprawidłowym certyfikacie może spowodować utratę nie tylko cennych informacji, ale także środków finansowych.

Podobne problemy dotyczą systemów zabezpieczających zasoby sieciowe. Nie pomogą żadne zabezpieczenia, jeśli użytkownicy systemów będą je omijaćw codziennej pracy, bo „utrudniają im pracę”. Systemy bezpieczeństwa powinny być tak projektowane, by nie wpływały negatywnie na komfort korzystaniaz systemu komputerowego — niestety nie zawsze jest to możliwe. Z jeszcze gorszą sytuacją mamy do czynienia w przypadku, gdy osoby uprzywilejowane w danej organizacji uważają, że pewne zasady ich nie dotyczą.

Bezpieczeństwo zasobów to nie tylko zabezpieczanie ich przy użyciu wyrafinowanych rozwiązań, to także korzystanie z nich przy zachowaniu odpowiednich reguł. Wyobraźmy sobie sytuację, w której dyrektor dużego działu firmy zapomniał swojego hasła. Do tego załóżmy, że jest to człowiek nieznoszący sprzeciwu, nerwowo reagujący na wszelkiego rodzaju odmowy czy utrudnienia ze strony podwładnych. Kiedy osoba taka zapomni hasła, zapewne natychmiast zadzwoni do działu IT w celu zmiany swojego hasła. Pracownik IT nie

powinien takiej operacji przeprowadzać przez telefon, bez wcześniejszej identyfikacji rozmówcy. Oczywiście zdenerwowany szef może zacząć krzyczeć na podwładnego i wymusić na nim działanie (np. poprzez groźbę). Zachowanie takie, niestety nagminnie obserwowane, stanowi wielkie zagrożenie, ponieważ może zostać wykorzystane do przeprowadzenia ataku socjotechnicznego w celu uzyskania dostępu do zasobów. Przykłady tego typu można mnożyć. Osoby zainteresowane takimi historiami kieruję do lektury książki [12].

Wnioski z powyższych rozważań nasuwają się same. Oprócz stosowania zabezpieczeń fizycznych (do których należą wszelkiego rodzaju systemy bezpieczeństwa) konieczne jest wprowadzenie ściśle zdefiniowanychi bezwzględnie przestrzeganych procedur bezpieczeństwa. Konsekwentne wdrożenie zasad postępowania i żelaznej reguły mówiącej, że nikt w żadnej sytuacji nie może ich omijać pozwalają unikać wszelkiego rodzaju nietypowych zachowań, które zazwyczaj dają możliwość przeprowadzenia natychmiastowego i skutecznego ataku sytuacji. Niezwykle istotna jest także edukacja. Pozwala ona na świadome korzystanie przez przeciętnego pracownika z systemów komputerowych,z zachowaniem podstawowych zasad bezpieczeństwa. Pozwala także wytłumaczyć użytkownikom, po co stosuje się konkretne zabezpieczenia. Użytkownicy, gdy będą rozumieli w jakim celu są stosowane, zapewne przestaną je postrzegać jako problemw wykonywaniu codziennych obowiązków, a co za tym idzie – przestaną je obchodzić.

Rys. 5. „The Info-Tech UTM Vendor Landscape" (opracowanie własne na podstawie [10])

Fig. 5. „The Info-Tech UTM Vendor Landscape" [10]

7. Wnioski

Rozwój sieciowych systemów zabezpieczeń, poczynając od prostych bezstanowych zapór ogniowych kończąc na najnowszych rozwiązaniach klasy XTM, jest ewidentnie wymuszany przez ewolucję technik i metod ataków, spotykającą sięz natychmiastową reakcją producentów rozwiązań zabezpieczeń sieciowych. To swoiste sprzężenie zwrotne, będące od lat motorem ewolucji sieciowych systemów bezpieczeństwa powoduje ich dynamiczny rozwój. Na rynku dostawców tego typu rozwiązań trwa nieustanny wyścig, którego pozytywnym wynikiem są coraz lepsze i skuteczniejsze systemy.

Mnogość oferowanych rozwiązań wymusza jednak zachowanie dużej staranności przy ich doborze do konkretnych potrzeb, przez świadomego zagrożeń użytkownika. Pomocą mogą tu być publikowane przez specjalizujące sięw ich (rozwiązań) ocenie organizacje. Na rysunku 5 przedstawiono syntetyczny obraz wniosków płynących z ostatniego (sierpień 2011) raportu Info-Tech Research Group [10], pozycjonującego dostawców rozwiązań klasy UTM. Zgodnie z wynikami tego badania firma WatchGuard® Technologies uzyskała zaszczytny tytuł „UTM Champion and Value Award Winner".

Artykuł zgłoszony do publikacji w grudniu 2011.

Literatura

[1] Żenkiewicz J., *Powstanie i rozwój internetu: kalendarium*, Uniwersytet Mikołaja Kopernika, Uczelniane Centrum Informatyczne, 2004, http://www.umk.pl/~zenkiewicz/kalendarium.

[2] Mogul J.C., Rashid R.F., Accetta M.J., *The Packet Filter: An Efficient Mechanism for User-level Network Code*, Proceedings of the 11th Symposium on Operating Systems Principles, ACM SIGOPS, Austin, Texas, November 1987.

[3] Kostick Ch., *Building a Linux firewall*, Linux™ Journal, Issue 24, April 1996, http://www.linuxjournal.com/node/1212/print.

[4] Staff L.J., *Mazama Packet Filter*, Linux™ Journal, Issue 14, June 1995, http://www.linuxjournal.com/article/1102.

[5] *New Internet Firewall Security System Sets Benchmarks for Low Cost, Easy Installation/Management and Flexible Deployment*, The Free Library by Farlex, Seattle, WA, July 1996, http://www.thefreelibrary.com/new+internet+firewall+security+system+sets+benchmarks+for+low+cost,...-a018521940.

[6] *Executive Management*, Fortinet (NASDAQ: FTNT), http://www.fortinet.com/aboutus/management.html.

[7] Longstaff T.A., Ellis J.T., Hernan S.V., Lipson H.F., McMillan R.D., Pesante L.H., Simmel D., *Security of the Internet*, The Froehlich/Kent Encyclopedia of Telecommunications, vol. 15., Marcel Dekker, New York, 1997, 231-255.

[8] Statystyki organizacji CERT dostępne on-line: http://www.cert.org/stats/.

[9] *Fireware XTM. The next generation of network security runs in the family*, WatchGuard® Technologies, October 2011, http://www.watchguard.com/products/fireware-xtm.asp .

[10] Info-Tech Research Group, *The Info-Tech UTM Vendor Landscape*, August 2011, http://www.infotech.com/research/it-vendor-landscape-storyboard-unified-threat-management.

[11] Gold S., *The Future of the Firewall*, Network Security, Volume 2011, Issue 2, February 2011, Pages 13-15.

[12] Mitnick K., Simon W.L., *Sztuka podstępu. Łamałem ludzi, nie hasła*, Helion, Gliwice 2003, ISBN: 83-7361-116-9