PIOTR CICHOCKI

Współczesne rozwiązania wielosilnikowe

Stopień trudności

Zagadnienia związane z bezpieczeństwem systemów komputerowych w przedsiębiorstwach nabrały ogromnego znaczenia w ciągu ostatnich lat. Powodem zaistniałej sytuacji stał się wzrost ilości różnych typów złośliwego oprogramowania oraz metod rozpowszechniania go w sieci Internet.

Dzięki temu wielosilnikowe systemy antywirusowe oraz antyspamowe zaczynają odgrywać na świecie coraz większą rolę w procesie ochrony systemów komputerowych. Niestety, na podstawie obserwacji stwierdzono, iż poziom świadomości dotyczący istnienia takich rozwiązań jest nadal zbyt niski wśród polskiej kadry zarządzającej oraz niewielkiej liczby administratorów. Producenci rozwiązań wielosilnikowych prześcigają się w konstruowaniu nowych, zapewniających dużą elastyczność konfiguracji oraz prostych w administracji systemów zabezpieczeń.

Celem artykułu jest omówienie rozwiązań wielosilnikowych oraz zwrócenie uwagi na podstawowe korzyści płynące z ich zastosowania.

Według informacji FBI Crime and Security Survey z 2006 roku, na 98% przedsiębiorstw posiadających oprogramowanie antywirusowe, 84% zostało zainfekowanych przez wirusy. Co jest przyczyną zaistniałej sytuacji?

Gdy na świecie pojawiły się pierwsze złośliwe programy a zaraz za nimi pierwsze programy antywirusowe, niewiele osób przypuszczało, że rozwój wirusów nastąpi w tak gwałtowny sposób. Pierwsze wirusy, pomimo niewielkich szkód jakie mogły spowodować, wstrząsały opinią publiczną oraz budziły nie tylko niepokój, ale wywoływały sensację a w mediach można było usłyszeć o pierwszym wirusie komputerowym. Czasy kiedy na jeden czy dwa wirusy wystarczał program antywirusowy aktualizowany co kilka tygodni odeszły w niepamięć. Zarówno autorzy szkodliwego oprogramowania, jak również producenci oprogramowania AV, prześcigają się w pomysłach, Ci pierwsi na skuteczny atak, drudzy na skuteczną obronę. W środku tej walki pojawiają się użytkownicy końcowi (administratorzy, użytkownicy zdani na łaskę administratorów, lub też użytkownicy domowi). Bezpieczeństwo posiadanych systemów komputerowych, sieci lokalnych, korporacyjnych czy wreszcie domowych, zależy od świadomych wyborów dokonywanych przez wymienione, przykładowe grupy użytkowników końcowych. Czy użytkownicy końcowi powinni decydować się na uzależnienie od jednego producenta oprogramowania antywirusowego? Jeśli zależy im na elastyczności rozwiązań, niezależności, bezpieczeństwie danych oraz poprawieniu reakcji na zagrożenia to zdecydowanie powinni zastanowić się nad rozwiązaniem opartym na co najmniej kilku silnikach antywirusowych różnych producentów.

Dlaczego wiele silników?

Przede wszystkim stosowanie rozwiązań wielosilnikowych umożliwia korzystanie z wielu szczepionek w momencie wykrycia nowego złośliwego programu. Pomimo, iż producenci oprogramowania antywirusowego oraz antyspamowego zapewniają, że czas reakcji na nowe zagrożenia jest wysoki, w rzeczywistości nie jest tak zawsze. Nie zdarza się, aby jeden producent oprogramowania, za każdym razem

Z ARTYKUŁU DOWIESZ SIĘ

- czym są wielosilnikowe rozwiązania antywirusowe oraz antyspamowe,
- jakie korzyści płyną z ich zastosowania,
- jak walczyć z wyciekiem informacji poprzez wiadomości e-mail,
- jak działają niektóre techniki antyspamowe,
- jak działają rozwiązania wielosilnikowe,
- jak zapewnić bezpieczeństwo zgodnie z normą ISO 27001.

CO POWINIENEŚ WIEDZIEĆ

- znać podstawowe zagadnienia związane z bezpieczeństwem informatycznym.

dostarczał jako pierwszy szczepionkę na wszystkie, nowopojawiające się typy zagrożeń. Biorąc pod uwagę fakt, iż wirusy mogą rozprzestrzeniać się z zawrotną prędkością, chociażby drogą poczty elektronicznej, nigdy nie ma pewności, że akurat producent, którego silnik został zastosowany, zareaguje w krótkim czasie na zaistniałe zagrożenie (Tabela. 1). Czas reakcji na zagrożenia rozsyłane w poczcie elektronicznej w podziale na różnych producentów). Problem tzw., wąskiego gardła, czyli uzależnienia od jednego silnika, zostaje wyeliminowany, a szansa na zidentyfikowanie nowego wirusa, w krótkim czasie, znacznie wzrasta w przypadku stosowania wielu silników.

Organizacja *VirusBulletin*, której działalność polega na prowadzeniu analiz programów antywirusowych różnych producentów w oparciu o najbardziej niebezpieczne wirusy oraz publikowaniu raportów, wykazuje, iż nie ma na świecie silnika antywirusowego, który byłby doskonały i przeszedł wszystkie testy z bardzo dobrym wynikiem. Producenci oprogramowania wykorzystują różne algorytmy identyfikujące wirusy. W związku z tym faktem, wirusy znalezione przez poszczególne mechanizmy analizy heurystycznej mogą posiadać różne nazwy. Ponadto w rozwiązaniach wielosilnikowych mogą znajdować się obok siebie silniki producentów, których siedziby zlokalizowane są w bardzo odległych miejscach globu, w różnych strefach czasowych. Dzięki temu wzrasta szansa otrzymania w szybkim czasie odpowiedniej szczepionki i zmniejszenie ryzyka zainfekowania systemów komputerowych. Ponadto rozwiązania wielosilnikowe obejmują wszystkie typy systemów komputerowych. W tradycyjnych rozwiązaniach producenci często wymagają zakupu wersji dedykowanej dla konkretnego systemu komputerowego.

Omawiana sytuacja może być kłopotliwa i nadszarpnąć budżet firmy, która zakupując konkretne oprogramowanie antywirusowe lub też antyspamowe, nie przewidziała, iż zmiana systemu serwerowego lub też klienckiego pociągnie za sobą wykupienie nowej licencji na oprogramowanie chroniące przed zagrożeniami.

Tabela 1. *Czas reakcji na szkodnika Trojan-Downloader-14439*

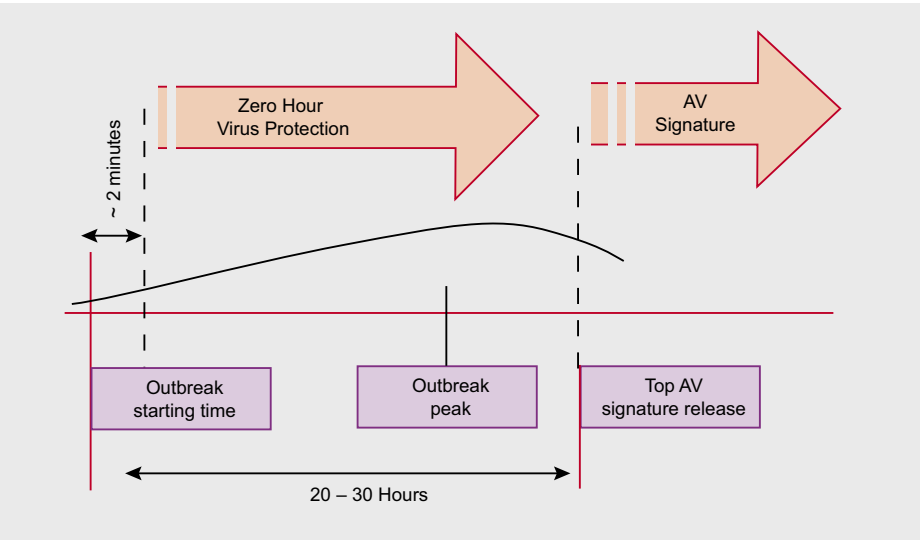
Oprogramowanie	Czas reakcji (H:M)
CA eTrust	95:34
Kaspersky	4:27
McAfee	16:11
Microsoft	29:56
NOD32	10:21
Sophos	5:46
Symantec	17:13
Trend Micro	75:44

Wyciek informacji poprzez pocztę elektroniczną

Według informacji opublikowanych w listopadzie 2007 r. przez firmę SOPHOS, 70% przedsiębiorstw obawia się o przypadkowe wysłanie wiadomości e-mail zawierającej poufne informacje do niewłaściwego adresata. Ponadto według informacji z tego samego źródła wynika, iż ok. 50% pracowników przyznało, iż zdarzyła im się taka sytuacja. Dla firm jest to niewątpliwie problematyczna kwestia, ponieważ pomyłka nawet jednego z pracowników, może doprowadzić do przechwycenia poufnych danych przez konkurencję, co z kolei może wiązać się ze stratami finansowymi lub kompromitacją firmy. Biorąc pod uwagę, iż obecnie w procesie wymiany informacji dużą rolę odgrywa komunikacja za pomocą poczty elektronicznej, rośnie również prawdopodobieństwo omyłkowego przesłania ważnych informacji do nieodpowiedniej osoby. Klienci biznesowi powinni przeciwdziałać temu zagrożeniu wszelkimi dostępnymi metodami. Dlatego też warto rozważyć zastosowanie technologii, która umożliwia w sposób elastyczny tworzenie reguł oraz nakładanie restrykcji na wychodzącą, jak również przychodzącą pocztę elektroniczną.

Techniki antyspamowe

Obecnie w rozwiązaniach wielosilnikowych umożliwiających blokowanie spamu stosowanych jest wiele technik antyspamowych. Omówiono kilka wybranych, najskuteczniejszych według autora artykułu. Pierwszą techniką, która umożliwia osiągnięcie dużej skuteczności w eliminowaniu spamu jest GreyListing, czyli tzw. szare listy. Mechanizm szarych list działa w następujący sposób: po wysłaniu wiadomości e-mail z serwera nadawcy, serwer adresata zwraca błąd tymczasowy, co wiąże się z chwilowym odrzuceniem wiadomości. W przypadku standardowej konfiguracji serwerów pocztowych, serwer nadawcy wysyła e-mail ponownie po ustalonym czasie. Z kolei spamerzy z reguły stosują metodę *wystrzelić i zapomnieć* (ang. *fire and forget*), dlatego ich narzędzia, serwery spamujące nie czekają na odpowiedź od serwera, do którego wysyłają wiadomość, a tym samym nie otrzymują informacji o błędzie. W związku z tym faktem, spam nie jest wysyłany ponownie do tego samego adresata. W uproszczonej technice szarych list rozpoznawanie wiadomości e-mail, które były już raz wysłane



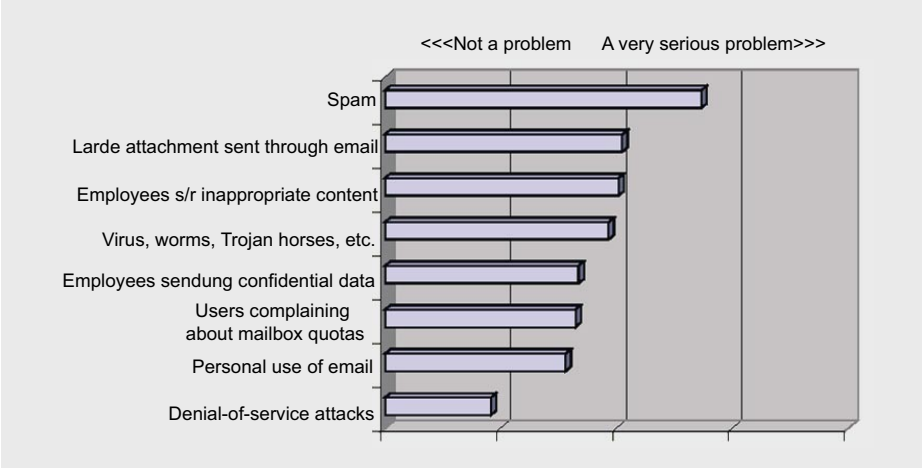
Rysunek 1. *Zero-hour protection – analiza statystyczna*

do serwera adresata, następuję po adresie IP serwera nadawcy. Poza tym zastosowano regułę kilkuminutowego odstępu czasowego przy odbieraniu przez serwer wiadomości pochodzących z tego samego adresu IP. Oznacza to, iż kilka e-maili wysłanych z identycznego adresu IP, jeden po drugim, bez zachowania wymaganej przerwy w czasie, spowoduje odrzucenie ich. W przypadku tej metody mogą nastąpić opóźnienia w dostarczaniu wiadomości e-mail, jednakże zauważono, iż rzadko kiedy jest to dostrzegane przez użytkowników końcowych.

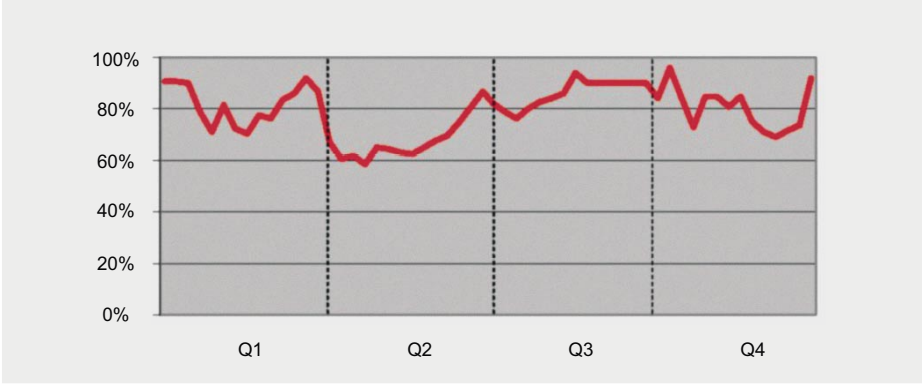
Kolejną techniką, która zasługuje na uwagę jest tzw. filtr Bayesian. Omawiana metoda filtrowania poczty elektronicznej oparta jest na nalizie statystycznej częstotliwości występowania określonych znaków lub wyrazów kluczowych we wszystkich przychodzących wiadomościach e-mail. Poza tym analizie poddawana jest cała treść wiadomości e-mail a skuteczność metody jest niezależna od języka. Przy założeniu, iż w określonym czasie do serwera adresata dotarła pewna ilość wiadomości e-mail charakteryzujących się specyficznym elementem, część z nich została zaklasyfikowana jako spam, a część jako bezpieczne wiadomości. Na podstawie ilości maili z obydwu grup jest dokonywana analiza a następnie dalsze zaklasyfikowanie wiadomości zawierających określone treści. Filtry bayesowskie potrafią wyfiltrować nawet do 99% spamu. Automatycznie dostosowują się do zmian w spamie i potrafią identyfikować spam poprzez analizowanie bezpiecznych wiadomości docierających do określonego adresata. W przypadku tychże filtrów istnieje konieczność dostosowania do własnych potrzeb, aby w przyszłości unikać błędnych klasyfikacji wiadomości e-mail.

Następną metodą antyspamową, która wydaje się być najbardziej wygodna jest zastosowanie heurystyki. Jest to metoda oparta na filtrach, które poszukują pewnych fraz, wyrazów, ciągów znaków pisanych wielkimi literami lub też innych elementów charakterystycznych dla spamu. Filtry heurystyczne umożliwiają wychwycenie spamu nawet w 90% sprawdzonych wiadomości. Wadą dotyczącą tychże filtrów jest fakt, iż zbudowane są na zestawie statycznych reguł. Każda zmiana w technikach spamerskich pociąga za sobą dopisanie nowych reguł. Na szczęście bazy reguł są automatycznie aktualizowane poprzez sieć Internet. Do zalet filtrów heurystycznych można zaliczyć możliwość szybkiego zainstalowania na serwerach pocztowych i natychmiastową gotowość do analizowania przychodzących wiadomości e-mail.

Należy zwrócić również uwagę na metodę antyspamową o nazwie *HashCash*. Jest to technika, która ma gwarantować, iż e-mail, który otrzyma adresat nie jest spamem. Związana jest z tzw. płaceniem za e-mail mocą procesora. W momencie wysyłania listu niezbędne jest wykonanie działania, które wymaga dość dużej pracy procesora. Proces ten jest w zasadzie nieodczuwalny dla nadawcy w przypadku wysyłania małej ilości e-maili. Odbiorca odbiera wiadomość i pochłania to po jego stronie małą ilość zasobów. Jednakże przedmiotowe działanie zostało skonstruowane w taki sposób, że wykonywane jest dla każdego odbiorcy. W związku z tym wysyłanie masowej ilości e-maili staje się bardzo trudne.



Rysunek 2. *Najważniejsze zagrożenia*



Rysunek 3. *Global spam levels*

Dostępność rozwiązań wielosilnikowych na rynku

Na świecie istnieje wiele systemów oferujących rozwiązania antyspamowe oraz antywirusowe m. in. *Easy Antispam's Email Protection Services* firmy Interjuncture Corp., *MessageLabs Anti-Spam* rozwiązanie oferowane przez firmę MessageLabs, *SMI!*, którego producentem jest firma M2 NET, *IronPort Anti-Spam* firmy IronPort Systems oraz inne.

Istnieje kilka sposobów instalowania/użytkowania rozwiązań do ochrony serwerów pocztowych:

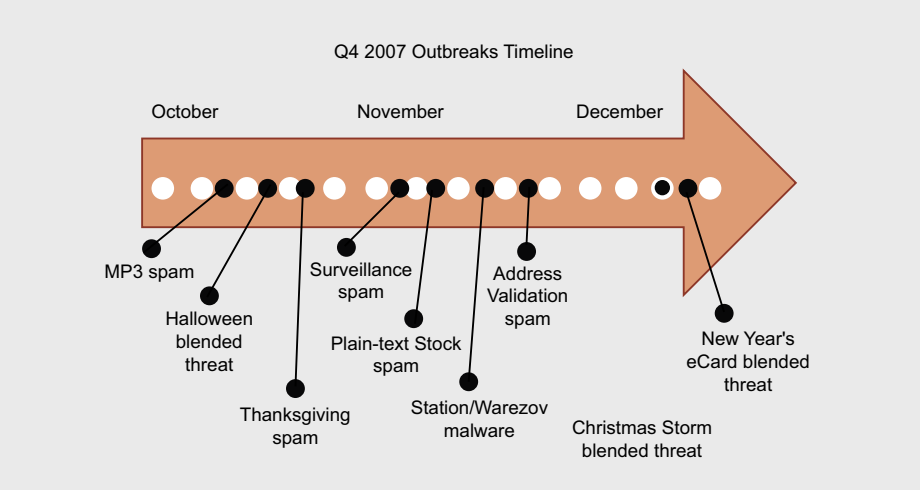
- Oprogramowanie może zostać zainstalowane na wydzielonym serwerze lub nawet na serwerze poczty w danej firmie. W celu zapobiegania obciążeniu serwera pocztowego zalecane jest instalowanie rozwiązań do ochrony SMTP na wydzielonym serwerze lub zastosowanie dedykowanego

serwera dostarczanego przez producenta. Rozwiązanie to może zostać zainstalowane przed lub za firewallem. W przypadku umieszczenia oprogramowania przed firewallem, należy odblokować na nim ruch z oprogramowania do portów TCP 80, 88, 25 oraz UDP 53. Zainstalowanie narzędzia przed serwerem pocztowym sprawia, że oprogramowanie działa jako MX, a jego zadaniem jest odebranie poczty (tym samym zachowuje się jak serwer pocztowy).

W przypadku zastosowania rozwiązania do ochrony konkretnego serwera pocztowego (np. Domino czy Exchange) oprogramowanie instalowane jest na serwerach poczty. Dedykowane oprogramowanie przechwytuje pocztę odbieraną przez mailbox serwera, a następnie rozpoczyna analizę poczty pod kątem kontroli treści oraz ochrony antywirusowej. W tym procesie stosowane są polityki i grupy reguł, które wcześniej zostały skonfigurowane przez administratora w danej firmie. Po zakończeniu analizy poczta, która została uznana za bezpieczną, zostaje doręczona do skrzynek. Oprogramowanie zintegrowane z konkretnym serwerem pocztowym realizuje również kontrolę treści.

Klienci mogą również zdecydować się na skorzystanie z zewnętrznej usługi. W standardowym wydaniu usługa zarządzalna polega na przekierowaniu poczty kierowanej do danego przedsiębiorstwa na serwery firmy, która oferuje tego typu usługi. Proces skanowania poczty jest realizowany przez oprogramowanie znajdujące się w kilku centrach danych zlokalizowanych w różnych krajach. Dzięki temu rozwiązaniu serwery firmy nie są narażone na bezpośrednie ataki i znacząco zmniejsza się obciążenie łącz telekomunikacyjnych (w listopadzie 2007 spam był odpowiedzialny za generowanie ponad 80% całego ruchu SMTP). W przypadku usługi list przechowywany jest na serwerach usługodawcy przez kilkaset milisekund, a w przypadku umieszczenia w kwarantannie – składowany jest on w szyfrowanej bazie danych, dedykowanej dla każdego klienta. Korzystając z usługi firma otrzymuje dwa niezależne serwery (główny i zapasowy), pozwalające na zachowanie ciągłości pracy przy jednoczesnej możliwości okresowej konserwacji i wyłączania jej serwerów. Wiadomości e-mail niedostarczone do serwerów pocztowych przedsiębiorstwa są kolejkowane na serwerach usługodawcy do momentu uruchomienia serwerów docelowych.

Omawiane rozwiązania wielosilnikowe umożliwiają zapobieganie wyciekowi informacji drogą poczty elektronicznej, realizują sprawdzanie poprawności protokołu SMTP, zapobiegają atakom dedykowanym dla konkretnych serwerów (ang. *identity spoofing*), są wyposażone w wiele metod antyspamowych (m. in. SPF, RBL i DNSRBL, HashCash, SURBL, Verifier, GreyListing, White & black IP lists, White & black address lists, Bayesian, Heuristic). Poza tym realizują również proces automatycznego sprawdzania istnienia nadawcy poprzez próbę połączenia lub sprawdzenie DNS przy dowolnym zagłębieniu. W przypadku większości rozwiązań wielosilnikowych poszukiwanie wirusów przeprowadzane jest dla treści wiadomości e-mail, zagnieżdżonych elementów MIME. Ponadto wykrywanie spamu jest realizowane przy pomocy modułów odpowiadających za sprawdzenie czy konto pocztowe, z którego przysłano wiadomość istnieje fizycznie na serwerze nadawcy. Sprawdzenie polega na wysłaniu wiadomości testowej do nadawcy. Rozwiązanie wielosilnikowe umożliwia zautomatyzowanie przeciwdziałania bombardowaniu e-mailami. Atakujący, który próbuje w powyższy sposób spowolnić lub unieruchomić pracę serwera poczty, zostaje odcięty na określony czas lub też zablokowany trwale. Poza tym można spotkać się z przydatnymi opcjami umożliwiającymi konfigurację identyfikującą i filtrującą załączniki według określonych rozszerzeń oraz zastosowanie konkretnych ustawień dla wskazanych użytkowników, np. zablokowanie wysyłania na zewnątrz plików z rozszerzeniem **.xls* określonym pracownikom lub też umożliwienie wysyłania plików o określonej wielkości w załącznikach. Interesującym elementem, który można dostrzec w rozwiązaniach wielosilnikowych, blokujących wiadomości z niechcianą zawartością jest możliwość binarnej analizy obrazów (np. filtrowanie przemycanych obrazków o treści pornograficznej przy zastosowaniu zaawansowanej technologii, której producentem jest firma LTU Technologies SA). W procesie analizy grafiki pierwszym etapem jest segmentacja obrazu. Technologia LTU wykorzystuje nieparametryczne, multiskalowalne podejście, dzięki czemu dzieli obraz na odpowiednie, wizualnie stabilne części. Dane wejściowe są analizowane pod kątem poszczególnych obszarów pikseli. Następnym etapem jest indeksowanie obrazu. Technologia LTU przypisuje podzielonemu obrazowi unikalny identyfikator nazwany podpisem (albo *zawartością DNA*). Zawartość DNA to zoptymalizowana kombinacja unikalnych cech tj. koloru, tekstury, kształtu, konfiguracji



Rysunek 4. *Q4 2007 outbreaks timeline*

w przestrzeni. Na końcu procesu obraz jest reprezentowany przez wektor liczbowy (zawartość DNA), w którym zakodowane są wszystkie szczegóły obrazu. W następnym procesie, tzw. klasyfikacji, zawartość DNA jest rozpoznawana przez moduły eksperckie zgodnie z ich bazą wiedzy. Moduły te wykorzystują najbardziej zaawansowane techniki rozpoznawania wzorców, takie jak: sieci neuronowe, funkcje z bazą radialną, estymację Bayesa czy maszynę wektorów wspierających. System ten przewyższa dotychczasowe techniki klasyfikacji obrazów ze względu na jego elastyczność i zdolność interaktywnego *uczenia się* od użytkownika, przy stałym poszerzaniu swojej bazy wiedzy. Warto zaznaczyć, że cały proces rozpoznawania obrazu, począwszy od jego segmentacji do określenia zawartości, dokonuje się w czasie rzeczywistym. Oprócz tego istnieje również możliwość szyfrowania newralgicznych informacji przesyłanych w wiadomościach e-mail oraz skanowania pod względem słów kluczowych. Poza tym, jak to bywa w przypadku oprogramowania antywirusowego oraz antyspamowego, istnieje możliwość tworzenia analiz w postaci wykresów i danych liczbowych w przedziałach czasowych określonych przez administratora. Standardowo technologie antywirusowe powinny być dostarczane przez kilka silników antywirusowych równocześnie, natywnie zintegrowane z oprogramowaniem. Wiadomości są skanowane przez wszystkie silniki jednocześnie. Każdy z silników zwraca informacje: *True* – oznajmiającą odnalezienie wirusa lub *False* – oznaczającą brak wirusa. W momencie, gdy przynajmniej jeden z silników rozpozna wirusa podejmowane są działania zgodne z utworzoną przez administratora polityką.

Aktualizacje oprogramowania umieszczane są zwykle na serwerze FTP, a informacje o nich można znaleźć na stronie WWW producenta. Klient sam pobiera poprawkę oraz instaluje ją u siebie na serwerze. W momencie pojawienia się problemów podczas aktualizacji oprogramowania, powinniśmy mieć możliwość skorzystania z pomocy telefonicznej, jak i bezpośredniej, oferowanej przez inżynierów producenta. Kolejna kwestia dotyczy sieci izolowanych. W przypadku tychże sieci większość oferowanych na rynku rozwiązań nie będzie w pełni realizować swojego zadania, ponieważ gros testów antyspamowych wymaga dostępu do sieci Internet (np. wymagana jest możliwość realizowania połączeń wychodzących na trzech, specyficznych dla testów, portach).

Archiwizacja i składowanie (ISO 27001)

W celu zapewnienia bezpieczeństwa (o czym mówi norma ISO 27001) należy archiwizować wszystkie wychodzące i przychodzące wiadomości e-mail. Kompleksowe rozwiązania do ochrony serwerów pocztowych umożliwiają archiwizację całej przesyłanej i odbieranej korespondencji lub tylko jej wybranych fragmentów. Poczta powinna być przechowywana w co najmniej dwóch różnych miejscach. Powinniśmy mieć także możliwość składowania danych na dedykowanych nośnikach (choćby na taśmach) poprzez np. IBM Tivoli Storage Manager, a także możliwość nagrywania paczek ok. 3,5 GB danych na DVD. Norma bezpieczeństwa ISO 27001 zaleca przechowywanie kopii poczty elektronicznej przez kilka lat. Często tylko wtedy ustalenia poczynione drogą elektroniczną można traktować jako wiążące.

Zastosowanie omawianych rozwiązań jest pomocne przy wdrażaniu polityki ochrony informacji zgodnej z normą ISO/IEC 27001.

Bezpieczeństwo informacji w świetle prawa

Bezpieczeństwo informacji w Polsce jest postrzegane głównie jako ochrona informacji niejawnych oraz danych osobowych. W każdej firmie znajdują się dane, które powinny podlegać ochronie. Ich wyciek lub utrata może pociągnąć za sobą szereg niekorzystnych skutków dla organizacji. Każda firma dbająca o bezpieczeństwo danych osobowych oraz informacji niejawnych powinna posiadać politykę bezpieczeństwa, jak również system zarządzania bezpieczeństwem informacji. Zagadnienia dotyczące bezpieczeństwa danych osobowych reguluje ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Natomiast kolejnym aspektem związanym z bezpieczeństwem, a zarazem ochroną osób prywatnych przed komercyjnym spamem, jest ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Zgodnie z art. 10 tejże ustawy zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Ustawa uznaje tę czynność za czyn nieuczciwej konkurencji. W myśl ustawy z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny, posłużenie się pocztą elektroniczną w celu złożenia propozycji zawarcia umowy może nastąpić wyłącznie za uprzednią zgodą konsumenta. Jednak w codziennej pracy mamy do czynienia ze spamem, a prawo nadal jest łamane. Dlatego tak ważne jest uświadomienie przedstawicielom kadry zarządzającej, jak również administratorom, jak ważne jest stosowanie optymalnych metod zabezpieczeń przed szkodliwym działaniem spamerów.

Podsumowanie

Rozwiązania omówione w artykule wskazują na wiele zalet systemów kompleksowych, posiadających szerokie możliwości konfiguracji oraz zapewniających przejrzysty, przystępny interfejs. W procesie zapewniania bezpieczeństwa firmy należy stawiać na systemy, które umożliwiają stosowanie technologii wielu producentów, wpływając na zmniejszenie ryzyka wystąpienia infekcji systemów komputerowych i jednocześnie na zredukowanie do zera prawdopodobieństwa nierozpoznania nowych zagrożeń. Każda firma, która jest świadoma wagi informacji w niej przetwarzanych, powinna stawiać na stosowanie rozwiązań gwarantujących utrzymanie bezpieczeństwa informacji na wysokim poziomie.

Piotr Cichocki
Z wykształcenia inżynier. Jest cenionym dziennikarzem zajmującym się tematyką bezpieczeństwa systemów teleinformatycznych. Obecnie pracuje jako specjalista w Wydziale Informatyki Urzędu Lotnictwa Cywilnego w Warszawie. Na swoim koncie ma wiele osiągnięć, do których można zaliczyć współpracę z Migut Media S.A., E-Security Magazine, CM LIM Sp. z o. o., a także z publicznymi oraz niepublicznymi dostawcami usług rynku pracy. Jego hobby to bezpieczeństwo systemów informatycznych, testy urządzeń typu appliance, muzyka, kompozycje, instrumenty klawiszowe, realizacja dźwięku, pływanie.
Kontakt z autorem: *cichocki.piotr@gmail.com*