Filtr antyspam to nie wszystko - rozwiązania Clearswift MAILsweeper

Grzegorz Blinowski

G.Blinowski@cc.com.pl

CC Otwarte Systemy Komputerowe Sp. z o.o.

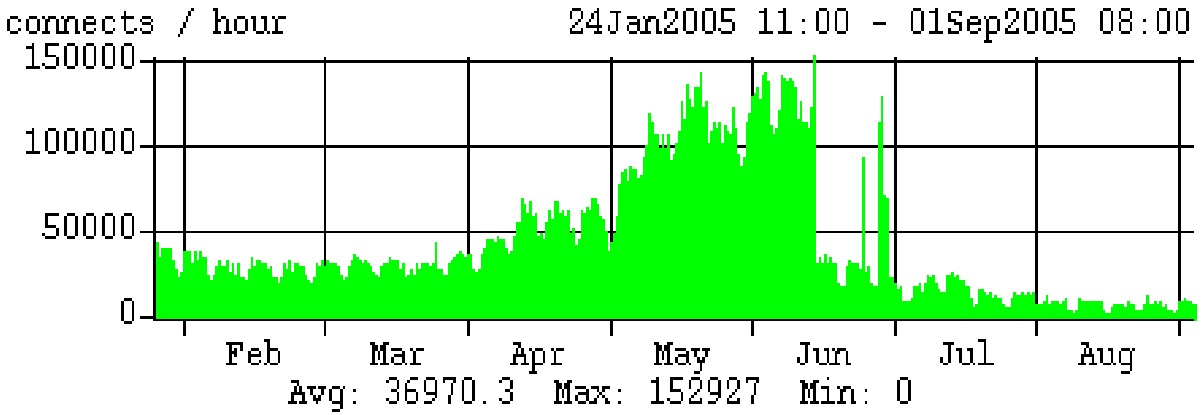
Agenda

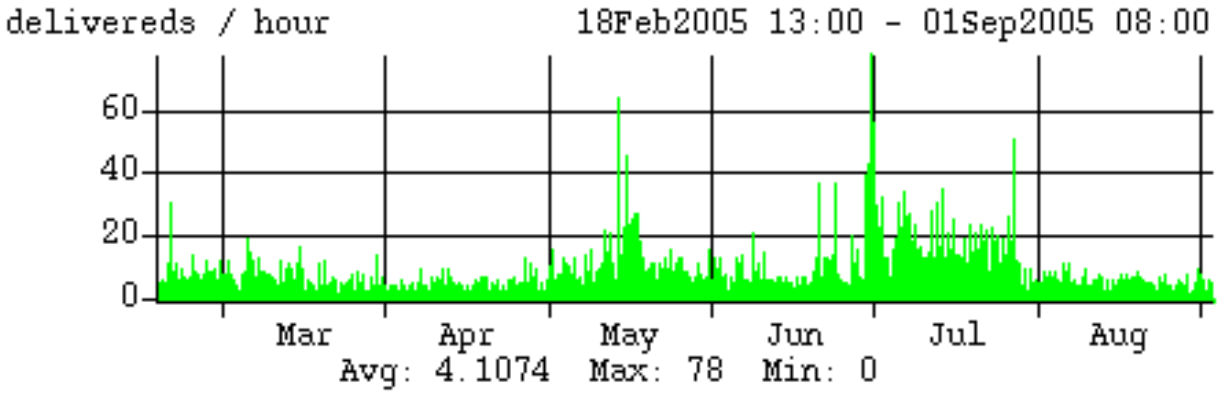
- Klasyfikacja zagrożeń:
  - Spam,
  - Robaki, Spyware i Phishing,
- Aktualne “trendy” w zagrożeniach sieciowych
- Zagrożenia dla firm i instytucji – e-mail *wychodzący*
- Jak się bronić?
- O firmie Clearswift
- Przegląd produktów Clearswift

SPAM

- Kto Otrzymuje więcej e-mail spamowych niż Bill Gates?
- Bill Gates otrzymuje 4 miliony wiadomości spamowych rocznie (11/2004), to:
  - 11 tys. wiadomości dziennie
  - 456 wiadomości na godzinę
- Jef Poskanzer zarządzający domeną (i firmą) **`acme.com`** otrzymuje: o.k. 1 miliona wiadomości spamowych dziennie

Statystyki poczty dla domeny acme.com





Stosowane rozwiązania:

- ze względów finansowych własne- bazujące na open source
- odrzucanie spamu już w fazie połączenia SMTP (e-mail spamowy nie jest zazwyczaj w całości przyjmowany)
- filtry: blacklist, whitelist, greylist, bayes

SPAM - prawda i mity

- Przetwarzanie spamu jest kosztowne (zwiększa koszt eksploatacji infrastruktury) - **NIEPRAWDA**
  - koszt przesłania wiadomości e-mail wynosi dla typowej firmy 0,00
  - poza skrajnymi przypadkami nieuniknione przyjmowanie spam-u przez serwer e-mail nie wymaga zwiększenia jego mocy (znacznie większe obciążenia wywołują wirusy e-mail oraz "świąteczne przesyłki okolicznościowe"
  - uwaga - powyższe nie dotyczy firm ISP
- Spamerzy zawsze skłaniają nas do kupowania produktów lub usług (co definiuje "spam") - nie zawsze
  - spam: religijny, polityczny, osobisty - "tragiczny", itd.

SPAM - prawda i mity

- Przepisy zakazujące spamowania mogą ograniczyć to zjawisko - nieprawda - spam jest ponad-państwowy
- Sankcje nakładane na spamerów powinny "boleć" - nieprawda - jak dotąd przypadki osądzenia i skazania spamerów są marginalne
- problem spamu rozwiązany zostanie przez odpowiednie rozwiązania techniczne narzucone przez największych (...ego?) producentów oprogramowania - nieprawda - proponowane rozwiązania spotykają się z b. znacznym "społecznym oporem", żaden producent nie kontroluje też w wystarczającym stopniu infrastruktury serwerów i klientów e-mail w skali światowej
- przypadki spamowania należy aktywnie zwalczać "ogień - ogniem" - nieprawda - metoda nieskuteczna

SPAM - prawda i mity

- Spam powoduje znaczny spadek produktywności pracowników - prawda, wiele niezależnie prowadzonych badań to potwierdza, straty w skali globalnej wynoszą dziesiątki mld Euro, na spam dziennie marnowane jest:
  - 10 min / przeciętnego użytkownika
  - 40 min / pracownika działu IT
- Spam powinien być zwalczany przez dostawców internetu (ISP) - prawda, choć (na razie?) nie rozwiąże to problemu w skali globalnej
- Protokół SMTP powinien zostać zmodyfikowany tak aby wykluczyć spam lub przynajmniej go zredukować - prawda, o ile rozwiązanie stanie się oficjalnym standardem, na pewno nie nastąpi to w ciągu kilku najbliższych lat

SPAM - metody walki

- **Filtry bayesowskie**: skuteczne i dokładne, "Wyścig zbrojeń", nie uwzględniają wolumenu
- **Filtry domenowe**: mało skuteczne, blokują legalne e-maile
- **Czarne listy**: efektywne (serwer nie przyjmuje wiadomości), czarne listy są mało wiarygodne
- **Szare i Białe listy**: b. efektywne i b. skuteczne, b. niewygodne dla użytkowników
- **Cyfrowy podpis**: potencjalnie skuteczne, brak infrastruktury i standardu
- **E-znaczki**: potencjalnie b. skuteczne, brak infrastruktury i standardu

SPAM - metody walki

- **Bunt konsumentów -** skuteczny w wąskiej grupie przypadków, ogólnie - nieskuteczny
- **Kontratak** - nieskuteczny i często nielegalny
- **Blokowanie przez ISP** (także ISP peering) - coraz skuteczniejsze, musi być wdrożone przez znaczący % firm ISP w skali globlanej
- **Opt-out** (akwizytorom dziekujemy) - propozycja, obecnie brak standardu i metody wymuszenia
- **Tagowanie** - "znak jakości" - "mail nie jest spamem" - propozycja, obecnie brak standardu i metody wymuszenia
- **Zakazy & standardy prawne na poziomie państwowym** - brak perspektyw i skuteczności tam gdzie wdrożono

Klasyfikacja pozostałych zagrożeń

- **Wirus** - *program komputerowy zdolny do samo-kopiowania, wymagający programu - nosiciela, dzięki któremu może funkcjonować i mnożyć się. Może, ale nie musi, posiadać wbudowanych funkcj złośliwych, nie jest zdolny do samodzielnego funkcjonowania*
- **Worm** - *program komputerowy zdolny do samo-kopiowania, **nie** wymagający programu-nosiciela, przenosi się przez sieć komputerową wykorzystując najczęściej systemowe mechanizmy transferu danych.*
- **Trojan** - *program komputerowy maskujący się jako nieszkodliwa aplikacja lub całkowicie ukrywający swoje istnienie, z założenia pełni funkcje destrukcyjne lub szpiegowskie*

Klasyfikacja zagrożeń

- Współczesne "wirusy" (w tym te najbardziej znane i najbardziej destrukcyjne) to twory hybrydowe będące kombinacją klasycznego wirusa i worma, a także coraz częściej trojan-a

- **RAT** - *Remote Access Trojan - Trojan posiadający funkcje zdalnego dostępu - atakujący może przejąć kontrolę nad zarażoną maszyną*
- **Spyware** – *dowolne oprogramowanie działające bez zgody (i wiedzy) użytkownika gromadzące i przesyłające siecią informacje o nim.*
- **Keylogger** - *oprogramowanie typu spyware (lub część składowa większego pakietu spyware) gromadzące informacje o znakach wpisanych z klawiatury*

Robaki hybrydowe

"Standardem" jest obecnie robak hybrydowy:

- wiele wektorów infekcji
  - e-mail (dziury w Outlook)
  - strony WWW (dziury w IE), atakowanie IIS
  - pliki .exe, atakowanie udziałów sieciowych
  - inne dziury w systemie operacyjnym (LSAS, ostatnio PnP)
- wiele metod rozprzestrzeniania się
- wbudowane mechanizmy trojan - typowo możliwość sterowania przez (zmodyfikowane) IRC

Robaki hybrydowe c.d.

- Wbudowane mechanizmy automatycznego poszukiwania informacji (*harvesting*):
  - adresy e-mail,
  - hasła, S/N i klucze zainstalowanych programów, itp.
- "botnet" - sieć zainfekowanych maszyn
- szybkie mutowanie - kod źródłowy często jest modyfikowany przez niezależne grupy (osoby)
  - dlatego warianty B, C, AB, AC, … robaków, np.: W32/Netsky-AC
- Szybki rozwój technik ukrywania kodu (stealth, rootkit) - manipulacje na poziomie kernela systemu operacyjnego mogą praktycznie uniemożliwić wykrycie robaka nawet przez zaawansowane narzędzia

Spyware

- Infekcja:
  - E-mail / IM (Worm) - sekretna instalacja
  - FUI (Fake User Interface) - fałszywy komunikat o błędzie skłania użytkowników do instalacji oprogramowania zawierającego spyware (programy "przyśpieszające działanie Internetu", itp.
- Funkcje:
  - keyloger, backdoor / trojan
  - przejęcie kontroli na kamerą/mikrofonem, faksmodemem
  - logowanie odwiedzanych url-i i ściąganych plików
  - logowanie sesji chat/IM
  - zrzuty ekranu
  - automatyczne łączenie z internetem
  - wysyłanie informacji poprzez e-mail
  - zmiany konfiguracji przeglądarki / klienta poczty
  - autoupdate spyware-u

Spyware

- Serwis Spyware-Guide.com podaje:
  - 20/08/2004: **444** programy typu spyware
  - 02/09/2005: **1596** programów typu spyware
- Spyware w ciągu ostatnich 2 lat stał się głównym narzędziem hakerskim
- W **Polsce** 3 duże banki posługują się statycznymi hasłami jako jedynym mechanizmem weryfikacji dostępu do systemu e-bankingu (tzn. nie stosują "zdrapek" lub tokenów)
  - w przeciągu ostatniego roku na masową skalę włamywano się do kont klientów co najmniej dwóch z tych banków
  - w jednym przypadku na pewno (w drugim prawdopodobnie też) posłużono się specjalnie spreparowanym spywarem pozyskującym hasła dostępowe do serwisów bankowych

Myfip - szpiegostwo "przemysłowe"

- **Myfip** (W32.Myfip.K) - robak wykryty 08.2004
- Mało szkodliwy - nie podejmuje żadnych działań destrukcyjnych, generuje mały ruch sieciowy - prawdopodobnie dlatego długo pozostawał niezauważony
- Infekcja:
  - E-mail / Outluk - dziura **iframe**
  - znajduje i zaraża udziały dyskowe SMB (jako iloveyou.txt.exe)
  - nie propaguje się dalej przez SMTP
- Znajduje i odsyła przez FTP pliki typu: pdf,doc,mdb oraz pliki programów CAD
- Analiza zachowania wykazuje, że wirus został opracowany w celu wykradania (a następnie odsprzedaży) zadań egzaminacyjnych

Phishing

- Połączenie klasycznych technik spamerskich i inżynierii społecznej
- Rozsyłane są e-maile mające skłonić użytkownika do podania numeru i PIN-u karty kredytowej lub informacji umożliwiającej dostęp do usług on-line:
  - e-banking
  - serwisy inwestycyjne
  - serwisy aukcyjne (E-bay)
- Klasyczny przykład: "***CitiBank scam***"
- Użytkownik jest skłaniany do kliknięcia na poprawnie wyglądającym linku, w rzeczywistości jest kierowany do serwisu hakerskiego:
  - http://www.citibank.com:ac=piUq3027qcHw003nfuJ2@sd96V.pIsEm.NeT/3/?3X6CMW2I2uPOVQW

CitiBank Scam

Subject: Citibank regular verification of the accounts. [Tue, 29 Jun 2004 12:
From: Citibank <users-support23@citibank.com>
Date: 6/29/2004 9:31 AM
To: cc@cc.com.pl

citi

Dear client of

As the Tech
We kindly ask
your access to

https://web.da

We are gratef

Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

<html> <A HREF="https://web.da-us
<map name="FPMap0"><area coords="0, 0, 610, 275" sha
href="http://%31%34%38%2E%32%34%34%2E%39%33%
</map><img SRC="cid:part1.00000008.01050603@user-s
</A> <font color="#FFFFF0">Will do it

----------=_000806060209090200070002
Content-Type: image/gif;
name="substitutionary.GIF"
Content-Transfer-Encoding: base64
Content-ID: <part1.00000008.01050603@user-supports23
Content-Disposition: inline;

R0lGODlhaQIUAfTOAAECAAAAgMDAwMDcwKbK8AAAQOAgQAAggEBAgEBggGBggOBggICAgOCAgICAwKCg
wOCgwKDAwP/78P8AAAAA/////wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACH5BAQAAAAALAAA
AABiAhMBAAX/YCWOZGmeowQ1S2u0bSOhdG3feK7vfO//wKBwSCwaj8ikcslsIsHiULw2RKrU5eEKd2y+16
v+CweEwum2tQq1ptyJ7f8Lh8Tq/b73CVdC3drxczeIKDhIWGh4iJO2IWBg0QgSIqUY1uipeYmZqbnJ0oa

Citibank customers details confirmation - Microsoft Internet Explorer provide...

please confirm

ATM/Debit Card (CIN)
Checking account linked to your ATM/Debit Card (if you have)
PIN
Saving account linked to your ATM/Debit Card (if you have)
User ID* (if you have)
First and Last Name
Password (if you have)
Social Security Number (SSN)
Business Code for CitiBusin (if you have)
Expiration date for Credit Card
Date Of Birth (DOB)
CVV2 code for Credit Card (if you have)
E-mail address

http://148.244.93.9:4903

sign on
Need help?
Forgot Your PIN?

* You must enter User ID if you use MyCiti, Citi Cards or Citi Business

Citigroup Privacy Promise Terms & Conditions Copyright © 2004 Citicorp

CLEA
The MIMEsw

Podsumowanie - Phishing, scaming, etc.

- Metody działania phisherów zostały dość dobrze poznane:
  - podział obowiązków:
    - phisher: rozsyłanie spam-u
    - phisher: zbieranie informacji
    - casher: "spieniężenie informacji" (typowo: wykorzystanie uzyskanych danych kart kredytowych)
    - casher i phisher dzielą się zyskiem
- Podobny schemat obowiązuje w przypadku botnetów
- Autorom wormów (patrz np. ostatni przypadek W32.Zotob) nie zależy na rozgłosie, lecz ma maksymalizacji korzyści finansowych

Nowe trendy

- (Jednak!) robaki na platformy mobilne (Symbian, Pocket PC, etc.)
  - Gartner (http://www.gartner.com/DisplayDocument?doc_cd=127808) twierdzi że mamy jeszcze 2 lata względnego spokoju
  - ta prognoza wydaje się nazbyt optymistyczna
  - Bluetooth - coraz bardziej popularny i dziurawy
  - podobnie WiFi
  - gdzie nasza komórka może złapać wirusa
    …. ???

- *Podczas 10-tych Mistrzostw Świata w lekkiej atletyce w Helsinkach zauważono znaczący wzrost liczby infekcji wirusem* ***Cabir***
- *… tak samo podczas koncertów Live 8*

Negatywny PR i odpowiedzialność prawna

- Kontrola poczty *wchodzącej* to obecnie standard
- W ciagu najbliższego roku ważniejsza stanie się kontrola poczty *wychodzącej*
  - e-mail stał się głównym medium wymiany informacji pomiędzy pracownikami wewnątrz firmy oraz w relacjach firma-firma
  - nietrudno o pomyłki
  - zdarza się też działanie w złej wierze
  - koszty odpowiedzialności prawnej są olbrzymie!

Negatywny PR i odpowiedzialność prawna

- Pomyłki / incydenty
  - Prezes Boeing-a usunięty z powodu molestowania przez e-mail
  - Microsoft: "knife the baby" (w odniesieniu do QuickTime)
- Badania wykazały, że wśród kadry zarządzającej średniego i wyższego szczebla:
  - 70% otrzymywał e-mail o treści pornograficznej
  - 24% otrzymywało poprzez e-mail informacje poufne lub tajne
  - 64% otrzymywało wiadomości o treści "niepoprawnej politycznie"
- W grupie "Fortune 500":
  - w 27% firm miały miejsce pozwy o molestowanie seksualne
  - w **<u>każdym z przypadków</u> e-mail** był jednym z dowodów
  - odszkodowania rzędu dziesiątek tysięcy USD
  - w przypadku naruszenia praw autorskich koszty dochodzą do mln USD

Metody ochrony

- Sformułować, przestrzegać, uaktualniać **politykę bezpieczeństwa,** w szczególności w zakresie wykorzystania Internetu
- Organizować okresowe krótkie **szkolenia** dotyczące podstawowych zasad bezpieczeństwa IT
- Stosować restrykcyjną politykę dotyczącą instalacji oprogramowania przez użytkowników
- Stosować centralnie administrowany **system AV**
- Stosować centralny **system skanowania poczty/www**
  - wprowadzić silne restrykcje na typy załączników przesyłanych pocztą
  - zakazać przesyłania archiwów szyfrowanych hasłem
  - zakazać przesyłania plików wykonywalnych (exe, dll, ocx, scr, …)
  - stosować centralny skaner AV innego producenta niż skanery desktop
  - zakazać dostępu do zewnętrznych serwisów typu WebMail
- Stosować **centralny system antyspamowy** z sprzężeniem zwrotnym od użytkowników

Rozwiązania firmy Clearswift

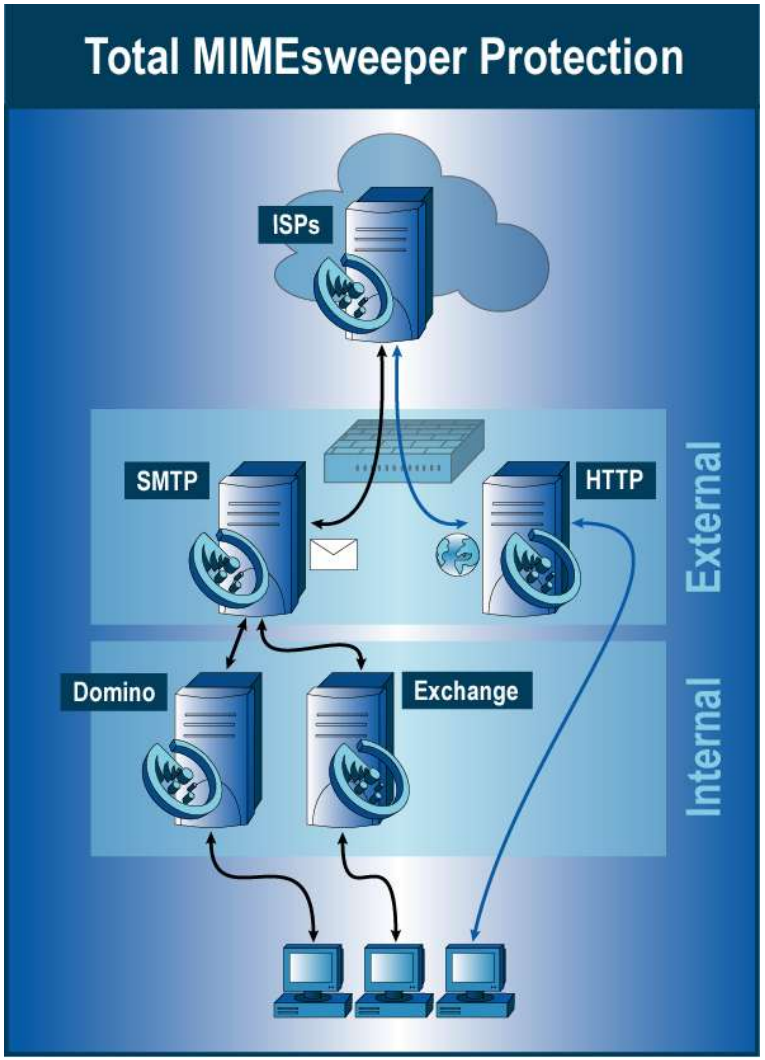
- Co to jest "**Clearswift**"?
  - Producent oprogramowania MIMEsweeper
  - #1 na światowym rynku produktów Content Security

- Obecny w: Wielkiej Brytanii (centrala), Francji, Niemczech, Szwecji, USA, Australii, Japonii

- 15,000+ klientów na całym świecie
  25 milionów użytkowników
  - 40 z 64 największych banków
  - Wszystkie z 10 nawiększych firm prawniczych
  - 70% firm z FTSE 200
  - 40% firm z grupy Global 500
  - 50% firm z grupy Global 100
  - 50% firm z grupy Fortune 500
  - Obecny w wielu dużych oraz średnich firmach i instytucjach w Polsce

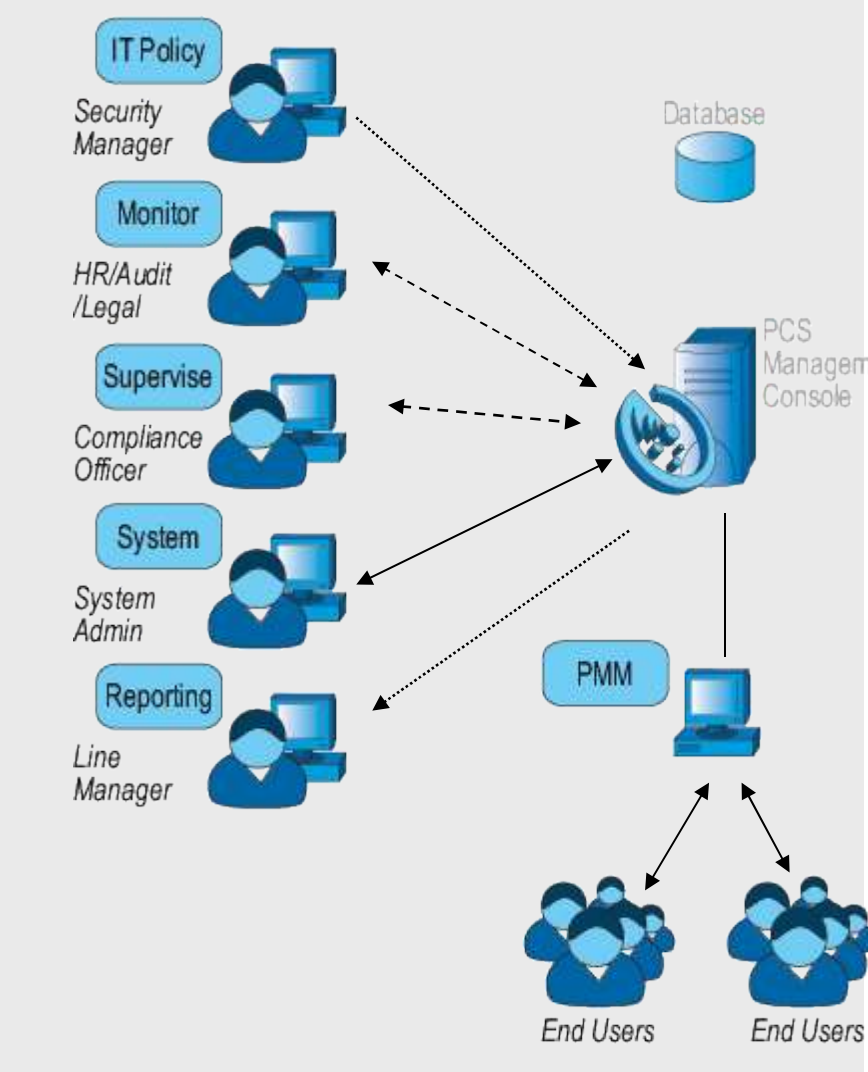
Kompleksowe rozwiązanie "Content Security"

- Ochrona obejmująca wszystkie punkty styku sieci firmowej z Internetem



MIMEsweeper SMTP

- Ochrona "zero day" przed atakami sieciowymi (robaki, spam)
- Ochrona AV
- Centralne zarządzanie czterema (ośmioma) serwerami
- Obsługuje od 25 do … 100 000 użytkowników
- Unikalny, oparty na rolach mechanizm konfiguracyjny
- Użytkownicy sami mogą klasyfikować spam
- Opcja: system analizy i filtracji załączników graficznych



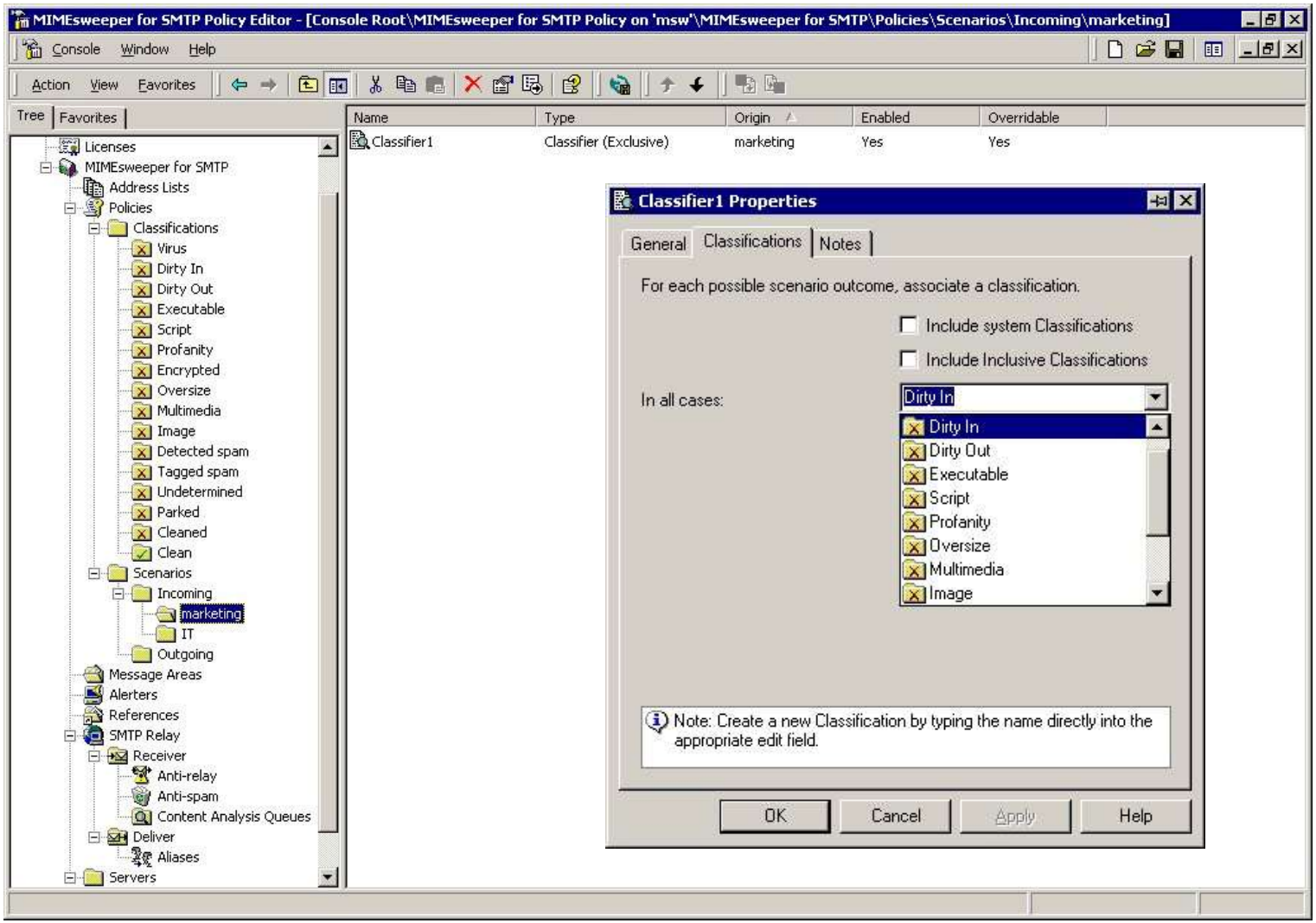
MIMEsweeper SMTP - przegląd funkcji

- Elastyczne definiowanie polityk bezpieczeństwa
  - Kreatory polityki bezpieczeństwa
- Zapobiega infekcjom wirusowym (współpracuje ze skanerami AV: F-Secure, H+BEDV, McAfee, Norman, Sophos, Symantec, ...)
- Antyspam
- Wykrywa złośliwy kod i złośliwe skrypty
- Wykrywa i usuwa załączniki wg. rzeczywistego typu pliku (np. MP3, gif/jpg, exe, itd.), a nie tylko wg. rozszerzenia i typu MIME
- Rekursywna dekompozycja załączonych archiwów
- Kwarantanna dla "podejrzanych" wiadomości
- Dodaje stopki

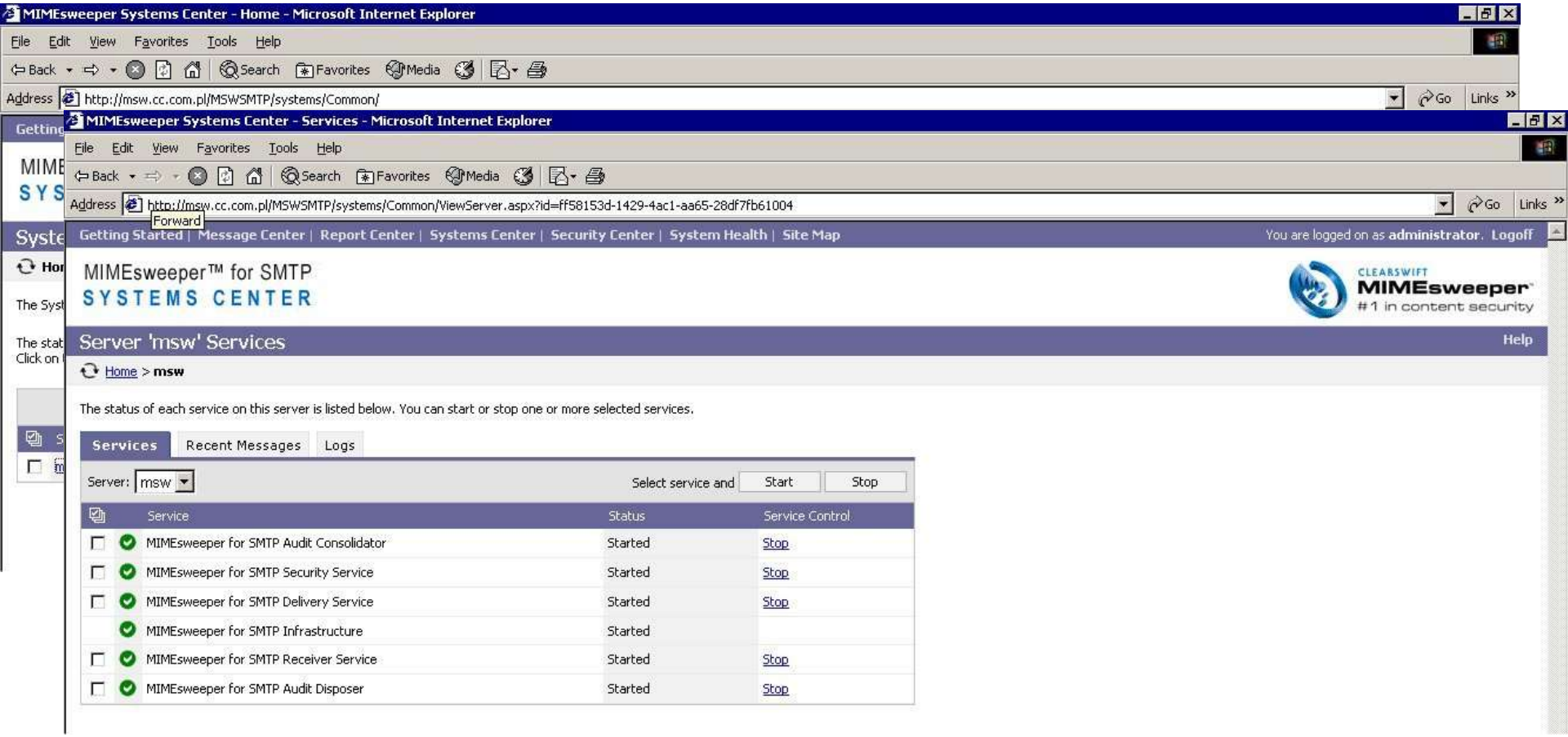
Zarządzanie

- Definiowane polityki bezpieczeństwa (MMC)
- Zarządzanie bieżącą pracą serwerów
  - monitorowanie stanu
  - monitorowanie kolejek
- Raportowanie
- Obsługa użytkowników końcowych

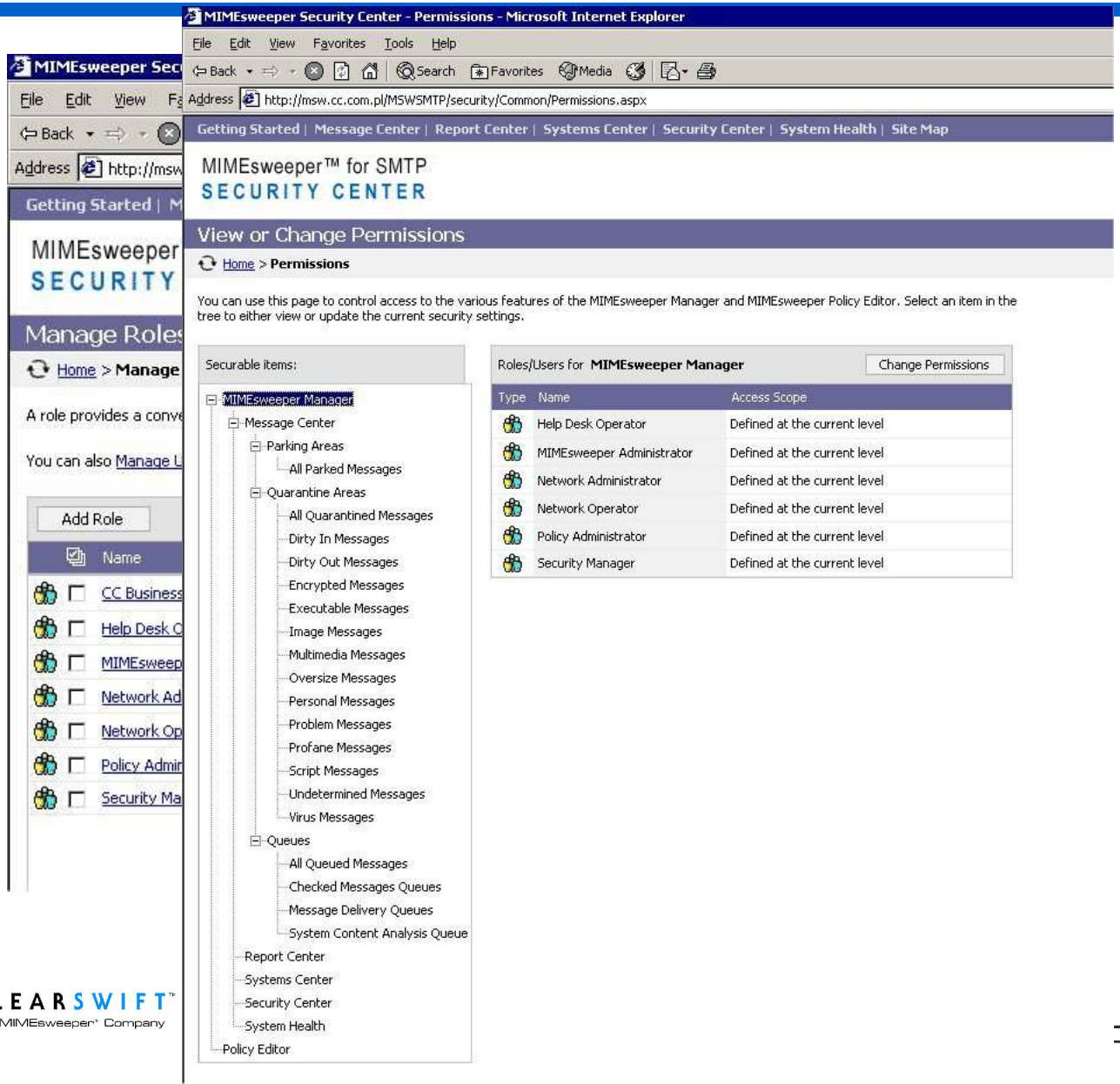
Definiowane polityki bezpieczeństwa



MIMEsweeper SMTP - Systems Center



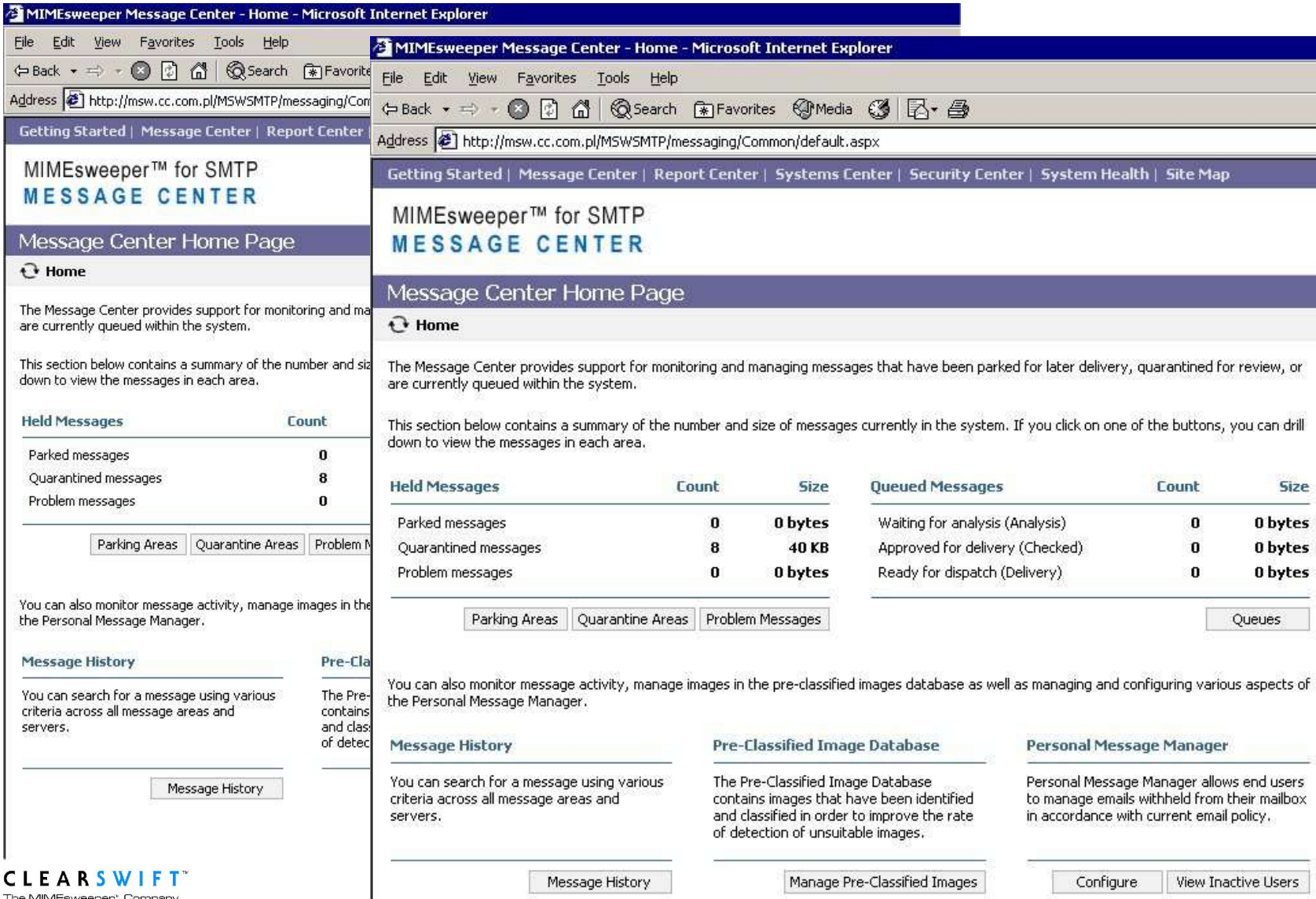
MIMEsweeper SMTP - Security Center



CLEARSWIFT
The MIMEsweeper Company

Content Security

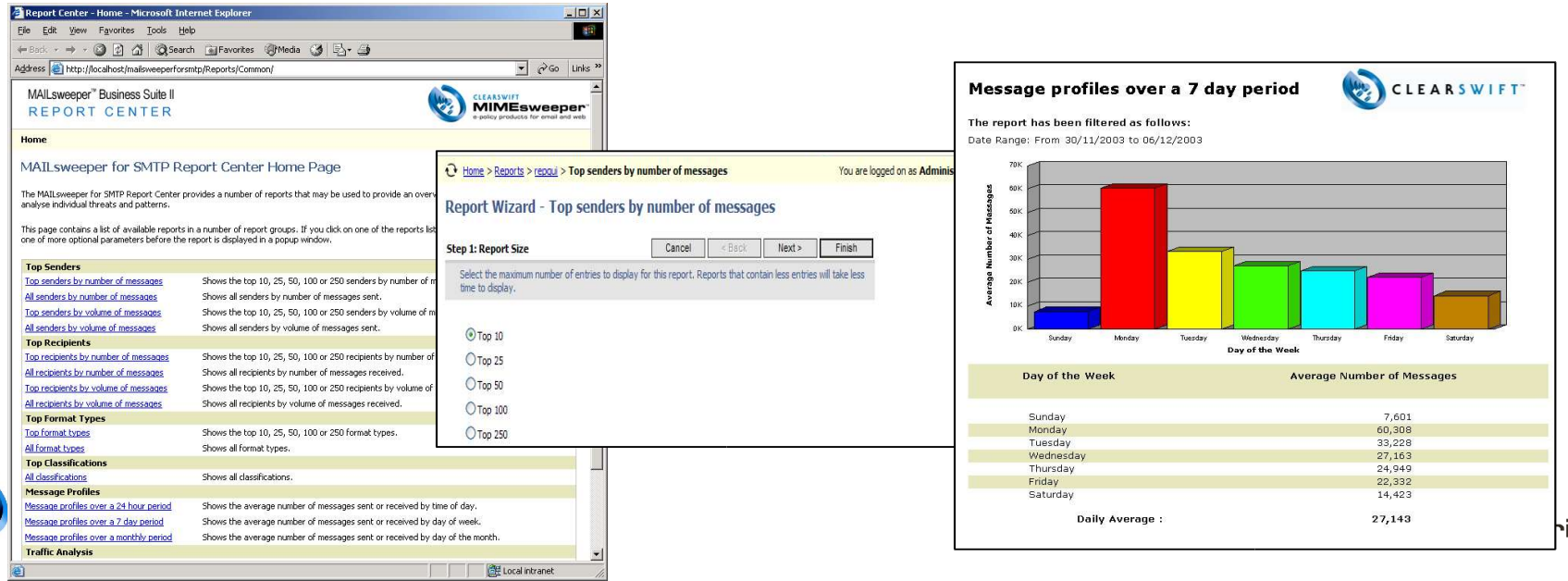
MIMEsweeper SMTP - Message Center



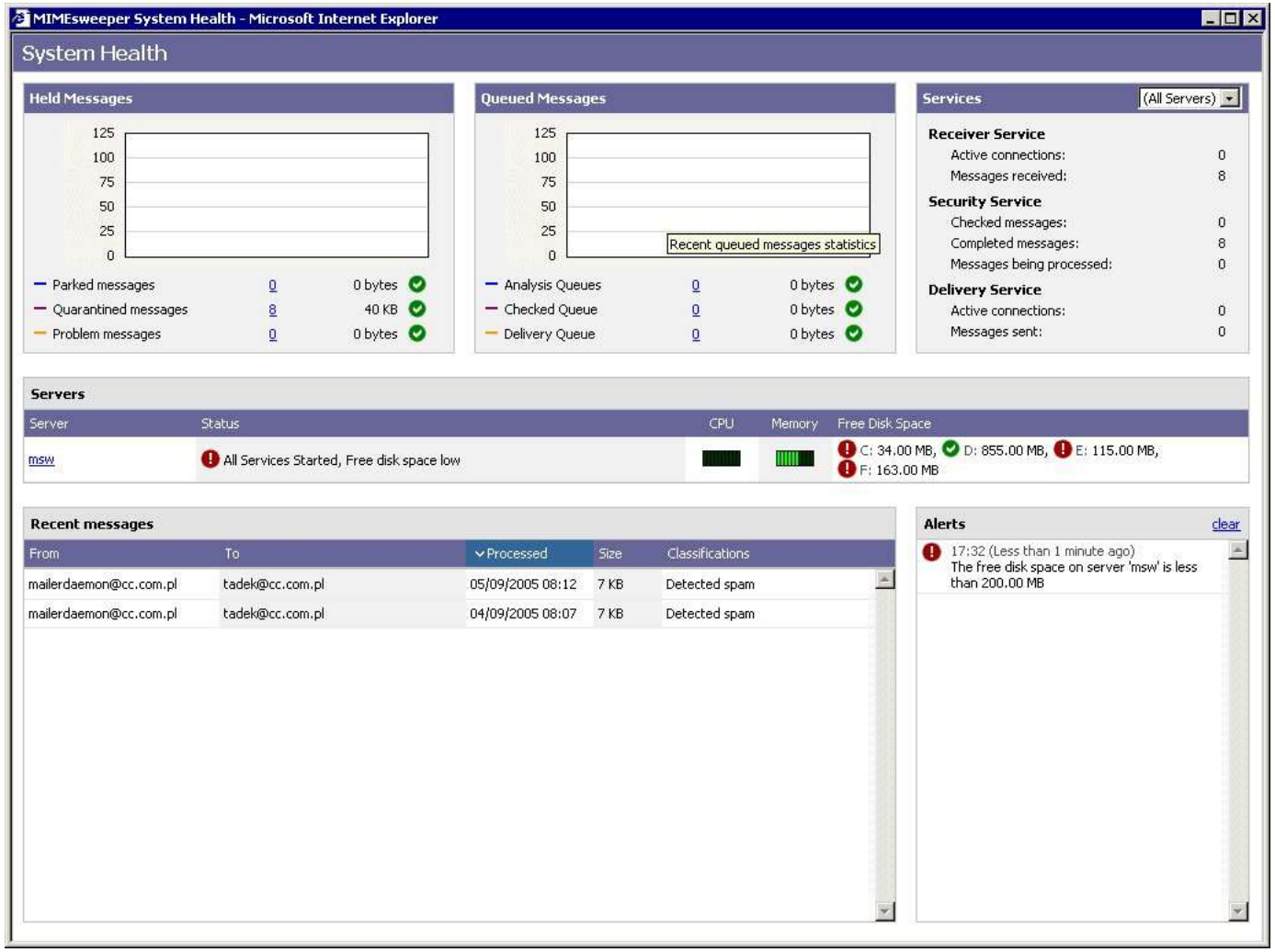
CLEARSWIFT
The MIMEsweeper Company

Raportowanie i audyt

- Pre-konfigurowane raporty
  - interfejs "tradycyjny" (Crystal Reports)
  - nowy interfejs WWW
- Szczegółowe raportowanie statystyk ruchu e-mail z wykresami
- Wbudowane raporty pozwalają szybko zlokalizować patologiczne zjawiska
- Raportowanie ułatwia też planowanie rozwoju i strojenie serwerów e-mail
- Nowość: logowanie do Oracle 9 (poprzednio MS SQL i MSDE)



MIMEsweeper SMTP - System Health



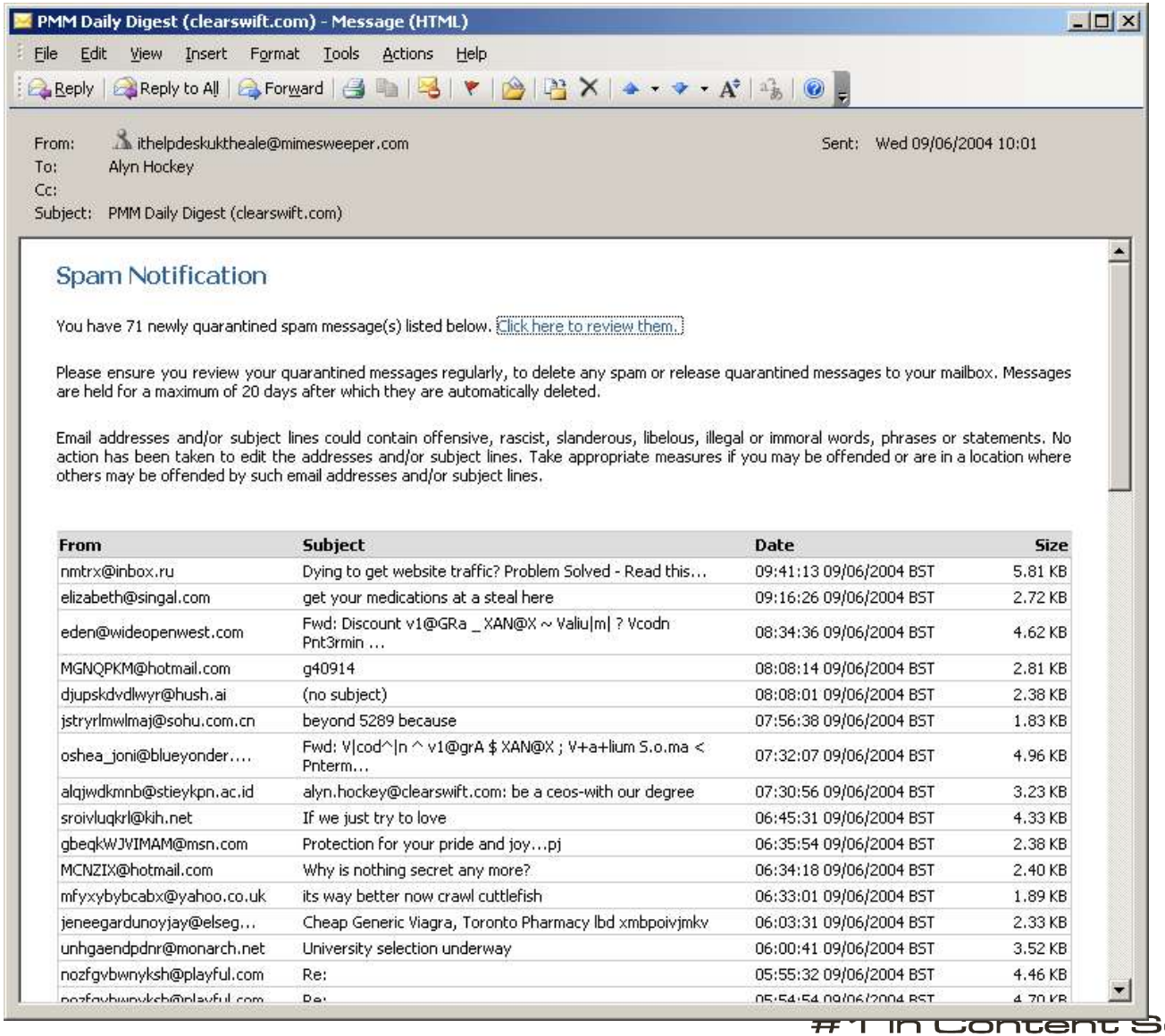
Mechanizmy antyspam

- Trzy mechanizmy detekcji:
  - wzorce (aktualizowana baza danych Spam-active)
  - filtry adaptacyjne - bayesowskie
  - listy RBL
- Współczynik wykrywalności: 98%
- false-positives: 1:10 000 (0.01 %)
- wydajność: do 200 000 wiadomości / godzinę dostępne w wersji MAILsweeper SMTP oraz w MAILsweeper Appliance

PMM - Personal Message Manager

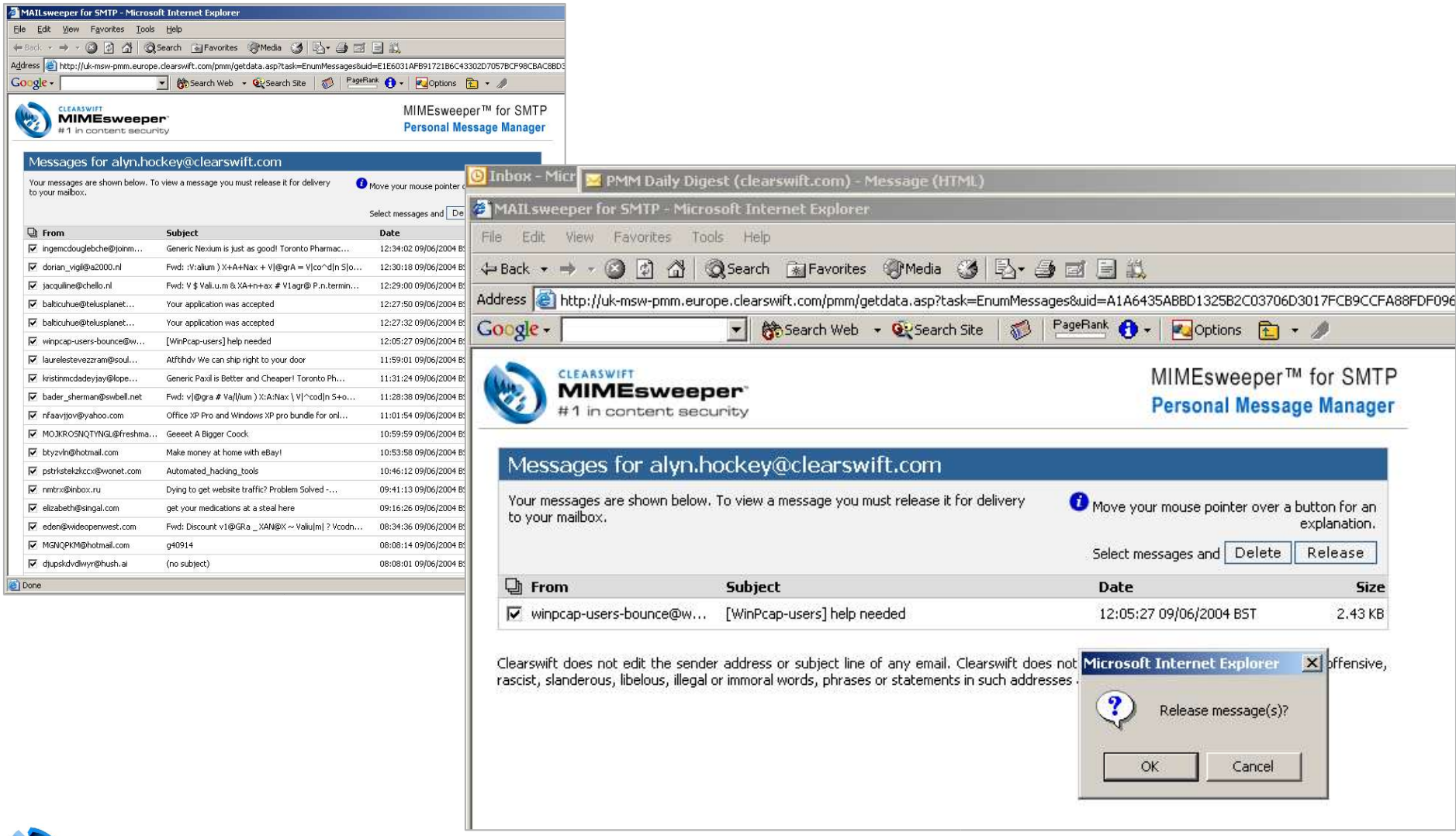
- Decyzje dotyczące spamu podejmowane są także przez użytkowników:
  - Filtr usuwa wiadomości jednoznacznie sklasyfikowane jako spam, lecz w przypadku wątpliwości decyzja należy do odbiorcy - wiadomość podlega kwarantannie
  - Odbiorca otrzymuje listę wiadomości wstrzymanych
  - Odbiorca "zwalnia" wiadomości, które chce otrzymać i kasuje pozostałe - zostają automatycznie uznane za spam
- Zalety:
  - Eliminacja klasyfikacji "false positive"
  - Sprawniejszy dopływ poczty do użytkownika
    - Użytkownik sam zarządza i defniuje spam
  - Odciążenie administratorów "auto help-desk"

PMM: użytkownik ogląda wiadomość ...

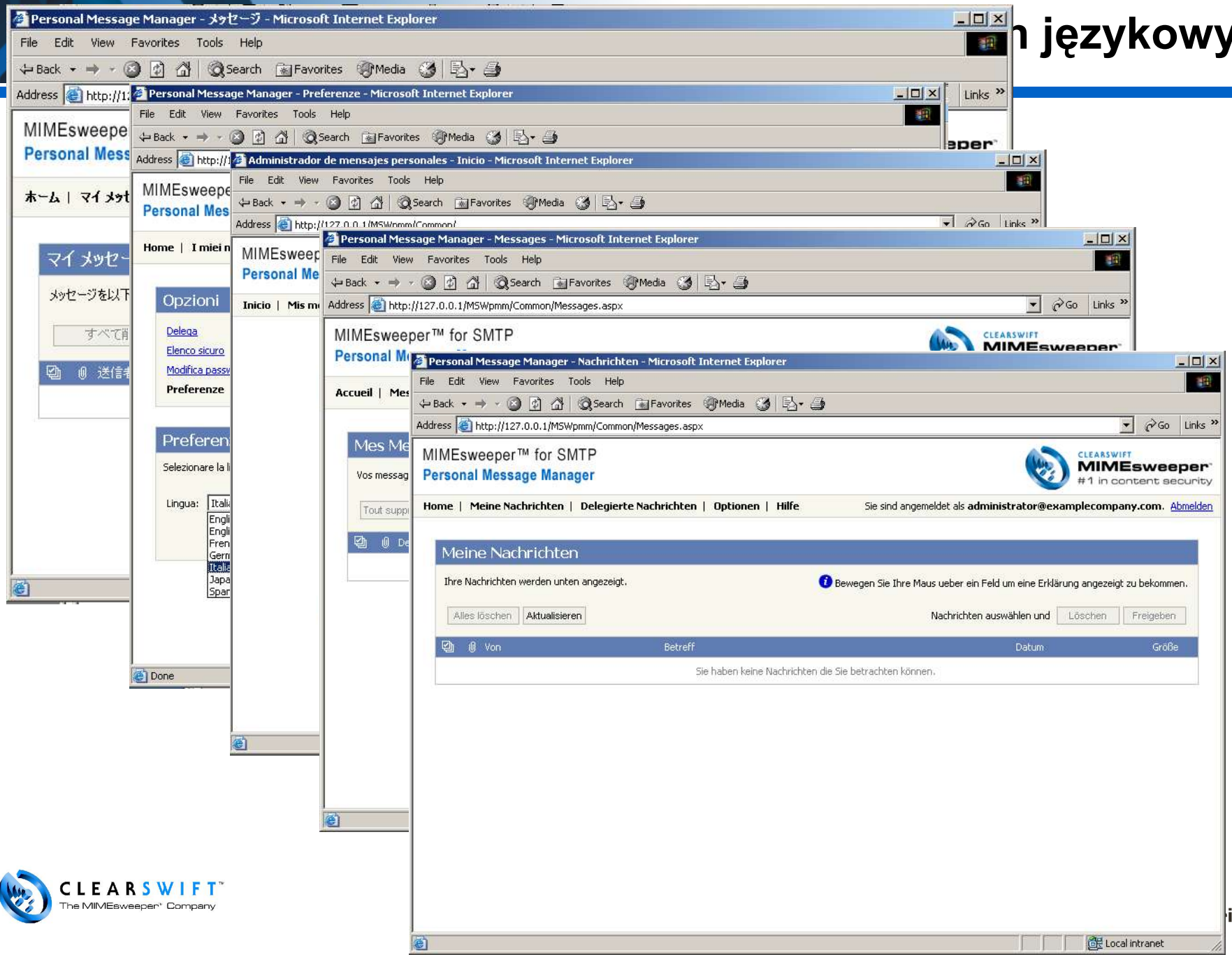


From	Subject	Date	Size
nmtrx@inbox.ru	Dying to get website traffic? Problem Solved - Read this...	09:41:13 09/06/2004 BST	5.81 KB
elizabeth@singal.com	get your medications at a steal here	09:16:26 09/06/2004 BST	2.72 KB
eden@wideopenwest.com	Fwd: Discount v1@GRa _ XAN@X ~ Valiu|m| ? Vcodn Pnt3rmin ...	08:34:36 09/06/2004 BST	4.62 KB
MGNQPKM@hotmail.com	g40914	08:08:14 09/06/2004 BST	2.81 KB
djupskdvdlwyr@hush.ai	(no subject)	08:08:01 09/06/2004 BST	2.38 KB
jstryrlmwlmaj@sohu.com.cn	beyond 5289 because	07:56:38 09/06/2004 BST	1.83 KB
oshea_joni@blueyonder....	Fwd: V|cod^|n ^ v1@grA $ XAN@X ; V+a+lium S.o.ma < Pnterm...	07:32:07 09/06/2004 BST	4.96 KB
alqjwdkmnb@stieykpn.ac.id	alyn.hockey@clearswift.com: be a ceos-with our degree	07:30:56 09/06/2004 BST	3.23 KB
sroivluqkrl@kih.net	If we just try to love	06:45:31 09/06/2004 BST	4.33 KB
gbeqkWJVIMAM@msn.com	Protection for your pride and joy...pj	06:35:54 09/06/2004 BST	2.38 KB
MCNZIX@hotmail.com	Why is nothing secret any more?	06:34:18 09/06/2004 BST	2.40 KB
mfyxybybcabx@yahoo.co.uk	its way better now crawl cuttlefish	06:33:01 09/06/2004 BST	1.89 KB
jeneegardunoyjay@elseg...	Cheap Generic Viagra, Toronto Pharmacy lbd xmbpoivjmkv	06:03:31 09/06/2004 BST	2.33 KB
unhgaendpdnr@monarch.net	University selection underway	06:00:41 09/06/2004 BST	3.52 KB
nozfgvbwnyksh@playful.com	Re:	05:55:32 09/06/2004 BST	4.46 KB
nozfgvbwnyksh@playful.com	Re:	05:54:54 09/06/2004 BST	4.70 KB

PMM: … i dokonuje wyboru



n językowych



CLEARSWIFT
The MIMEsweeper Company

MAILsweeper appliance

- Appliance stanowi uzupełnienie czysto softwarowej linii produktów
- Obejmuje: content security, antyspam i anty-wirus
- Platforma: Linux
- Ergonomiczny interfejs użytkownika (WWW)
- Bazuje na sprawdzonych (rozwijanych od kilkunastu lat) rozwiązaniach filtrujących Clearswift

MAILsweeper appliance

- **4 modele**:
  - CS500, < 500 skrzynek e-mail, 1U P4 2.8 Ghz, 2GB RAM,
  - CS1000, < 1000 skrzynek e-mail, 1U, 2 x Xeon 3 GHz, RAID, zasilacz hot-swap
  - EN10, > 1000 skrzynek e-mail, 1U, 2 x Xeon 3 GHz, RAID, zasilacz hot-swap
  - EN20, > 1000 skrzynek e-mail, 2 serwery: 2 U, 2 x Xeon 3 GHz, RAID, zasilacz hot-swap

- AV - Kaspersky
- Serwis:
  - roczny serwis i wsparcie w cenie (4 godz. on-site)
  - roczna subskrypcja baz AV i AS w cenie

MAILsweeper appliance

- Cechy wyróżniające produkt na tle konkurencji:
  - Filtrowanie dwukierunkowe - ruch wchodzacy i wychodzacy (w wielu przypadkach rozwiązania konkurencyjne wymagają stosowania dwu oddzielnych maszyn)
  - Ergonomiczny, wszechstronny interfejs zarządzający
  - "drobnoziarniste" zarządzanie polityką bezpieczeństwa
  - sprawdzony "engine" filtracji przeniesiony z MIMEsweeper SMTP

WEBsweeper

- Zarządzanie polityką bezpieczeństwa
- Intuicyjne GUI
- Autentykacja użytkowników (NT domain, LDAP, text)
- Dwukierunkowy cache
- Czyszczenie i regeneracja danych
- Analiza leksykalna (słowa klucz. i frazy)
- Architektura wielowątkowa
- Architektura skalowalna i odporna na błędy
- Wszechstronne logowanie i audyt
- Blokowanie adresów (sieciowa baza

URL categories

Adult / sexually explicit	Government & politics	Religion
Advertisements	Hacking	Remote Proxies
Arts & entertainment	Hate	Sex education
Business & economy	Health & medicine	Search Engines
Chat	Hobbies & recreation	Shopping
Computing & internet	Hosting Sites	Sports
Criminal skills	Job Search & career development	Streaming media
Drugs, alcohol & tobacco	Lifestyle & culture	Travel
Education	Motor vehicles	Usenet news / forums
Finance & investment	News	Violence / offensive
Food & drink	Personals & dating	Weapons
Gambling	Personal websites	Web-based email
Games	Real estate	
Glamour & intimate apparel	Reference	

Nagrody i wyróżnienia

- Rodzina MIMEsweepr otrzymała szereg prost nagród i wyróżnień:
  - MAILsweeper
    - For SMTP
      - SC Award Winner 2003, Best Content Security
      - Frost & Sullivan Award Winner 2002
      - SC Award runner up 2002, Best Content Security
      - SC Award Winner 2000, Best Content Security
    - For Domino
    - For Exchange
      - SC Award Winner 2000, Best Email Security Solu
    - Anti-spam Edition
  - MIMEsweeper for Web
    - Highly Commended, SC Awards for Best Internet Security Product", 2002
  - IMAGEmanager
    - SC Award Winner 2000, Best Content Security (jako PORNsweeper)

Referencje


CAP GEMINI
ERNST & YOUNG


THALES


Lloyds TSB


DEFENCE


DWP
Department for
Work and Pensions


NOKIA


Bank of America


CHASE


Continental
Airlines


ALCOA


AT&T


STANDARD LIFE


MARKS &
SPENCER


European
Commission


ABN·AMRO


NHS


Rolls-Royce


CL
CREDIT LYONNAIS


vodafone™


Pfizer


KPMG


Cadbury Schweppes


REUTERS

Dziękuję za uwagę!

Pytania?