# BiN 2004 - Informacje o wystąpieniu

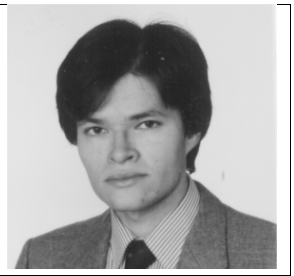
Grzegorz Blinowski,
**"Dlaczego z 80% przedsiębiorstw wyciekają poufne informacje i jak temu zaradzić... - produkty Clearswift"**

**Konspekt prezentacji**

- Klasyfikacja zagrożeń: Spam, Malware, Wirus, Worm, Trojan, RAT, Spyware, Phishing, Cyberwoozle, FUI, ...
- Spam, Wirusy, Trojany, Spyware - Aktualne "trendy"
- Analiza zagrożeń dla sieci korporacyjnej: Worm/Trojan, RAT, Spyware – kradzież danych, kradzież tożsamości, naruszeniebezpieczeństwa infrastuktury, szpiegostwo przemysłowe
- Jak się bronić?
- Clearswift MAILsweeper – jedno z ogniw łańcucha ochrony

## Informacja o prelegencie

**Dr Grzegorz J. Blinowski**
CC Otwarte Systemy Komputerowe Sp. z o.o.
Rakowiecka 36, 02-532 Warszawa
e-mail: Grzegorz.Blinowski@cc.com.pl
tel (22) 646-6873; faks (22) 606-3780



Grzegorz Blinowski Ukończył Politechnikę Warszawską, Wydział Elektroniki w 1993, doktorat z informatyki uzyskał w 2001 roku w Instytucie Informatyki na Wydziale Elektroniki i Technik Informatycznych Politechniki Warszawskiej za pracę z dziedziny rozproszonych systemów komputerowych. Studiował Informatykę na Politechnice Warszawskiej Wydziale Elektroniki oraz w Oxford Univeristy (Dep. of Engineering Science) w Wielkiej Brytanii.

Grzegorz Blinowski jest autorem kilkunastu publikacji naukowych oraz kilkudziesięciu artykułów w pismach związanych z branżą informatyczną, był także promotorem kilkunastu prac magisterskich i inżynierskich.

Grzegorz Blinowski od 1992 roku związany jest zawodowo z branżą informatyczną, jest założycielem i firmy "CC Otwarte Systemy Komputerowe" przekształconej w 2001 r. w spółkę z ograniczoną odpowiedzialnością.

# CC Otwarte Systemy Komputerowe Sp. z o.o.

**"CC"** jest firmą informatyczno - konsultingową działającą od 1995 roku. Firma specjalizuje się w rozwiązaniach z dziedziny **bezpieczeństwa** sieci komputerowych oraz rozwiązaniach dla Intranetów i Internetu.

**"CC"** zajmuje się produkcją własnego, wyspecjalizowanego **oprogramowania**.
Aplikacje i wdrożenia wykonywane są zgodnie z wymaganiami zamawiającego. Firma zapewnia wdrożenie, wsparcie techniczne oraz szkolenia.

**"CC"** posiada status:

- *Aladdin eSafe Partner*
- *CLEARSWIFT PremiumPartner*
- *CheckPoint VASP (Value Added Solution Provider)*
- *EMCO Software Partner*
- *F-Secure Partner*
- *H+BEDV Partner*
- *SUN Microsystems iForce Premier Partner*
- *StoneSoft Partner*
- *Vasco Partner*

**Lista oferowanych rozwiązań:**

"CC" Prowadzi sprzedaż i wsparcie techniczne produktów renomowanych producentów oprogramowania i systemów sieciowych m.in.:

- Aladdin
- ActivCard
- CheckPoint
- CISCO
- Clearswift
- EMCO Software
- Entrust
- Extreme Networks
- F-secure
- Guidance Software
- H+BEDV
- IPSwitch
- ISS
- nCipher
- NAI - McAfee
- NetManage
- Netscreen / Juniper
- Nokia Networks
- Sophos
- StoneSoft
- SUN Microsystems
- SurfCONTROL
- Symantec (produkty d. Axent)
- Tectia SSH
- TrendMicro
- Vasco
- WebSense
- WebTrends / NetIQ

Więcej informacji o firmie znajdziecie Państwo w Internecie, na stronach:
**http://www.cc.com.pl/**

**kontakt:**

**Dział Techniczny:** **tech@cc.com.pl**
**Dział Handlowy:** **sales@cc.com.pl**

**ul. Rakowiecka 36, 02-532 Warszawa**
**tel. +48 22 646-68-73**
**fax +48 22 606-37-80**
**e-mail: office@cc.com.pl**

# Opis produktu

**MIMEsweeper** to rodzina produktów służących do ochrony sieci przed zalewem niechcianych, nielegalnych oraz szkodliwych danych zawartych w przesyłkach e-mail, stronach WWW i plikach dostępnych przez FTP. Z oprogramowania MIMEsweeper korzysta 20 milionów użytkowników w 15 tysiącach firm i instytucji na całym świecie.

W przeciwieństwie do produktów typu firewall MIMEsweeper analizuje dane przesyłane siecią, rozpoznaje typy przesyłanych plików, skanuje załączniki i archiwa, lokalizując i usuwając treści uznaną za szkodliwe - np. wirusy komputerowe lub materiały obsceniczne. MIMEsweeper nie jest alternatywą, lecz uzupełnieniem dla produktów firewall takich jak: CISCO PIX, CheckPoint Firewall-1, Symantec Enterpise Firewall, itp.

Do grupy produktów MIMEsweeper należą:

- MAILsweeper Business Suite II (d. MAILsweeper for SMTP)
- MAILsweeper for Exchange,
- MAILsweeper for Domino R5
- MIMEsweeper for Web

**MAILsweeper Business Suite - szczegóły techniczne**

MAILsweeper opiera się na koncepcji polityki bezpieczeństwa realizowanej poprzez tzw. scenariusze, czyli zbiory reguł klasyfikacji i filtrowania przesyłek. Reguły mają charakter hierarchiczny, tak że np. reguły szczegółowe mogą dziedziczyć własności z reguł ogólnych. Reguły mogą opierać sie nie tylko na zawartości przesyłki, ale także na informacji o użytkownikach i grupach użytkowników.

Identyfikacja i usuwanie wirusów z przesyłek E-mail:

- identyfikacja wirusów w załącznikach
- współpracuje z szerokim wachlarzem popularnych skanerów anty-wirusowych
- usuwanie wirusów z przesyłek

Ochrona przez niechcianymi przesyłkami (spam-em):

- **Nowość:** w wersji Business Suite: kompleksowe filtry antyspamowe funkcjonujące w oparciu o listy wyrażeń oraz metodę Bayesa (filtry samouczące się)
- blokowanie i usuwanie przesyłek na podstawie analizy pól nagłówka przesyłki

Usuwanie załączonych plików o niedozwolonych typach:

- rozpoznawanie typów załączników
- blokowanie (usuwanie) określonych typów załączników

Reakcja na inne nadużycia, takie jak: przekroczenie dozwolonego rozmiaru przesyłki, wystąpienie słów kluczowych, itd.:

- Wykrywanie słów kluczowych i fraz w treści przesyłki
- Różnicowanie reguł filtracji w zależności od nadawcy i odbiorcy
- "kwarantanna" dla podejrzanych przesyłek
- archiwizacja przesyłek
- funkcje alertu, raportowania i audytu

**MAILsweeper for Web - szczegóły techniczne**

- Usuwa wirusy z przesyłek
- Blokuje niedozwolone adresy URL
- Integruje się z oprogramowaniem firm trzecich blokującym adresy URL

- Zgodny z walidacją PICS (Platform for Internet Content Selection)
- Skanuje treść na podstawie słów kluczowych.
- Wykrywa i blokuje applety Java, komponenty ActiveX oraz ukryte formularze
- Usuwa wybrane typów danych, np.: audio, wideo, cookies, itd.
- Może pracować w środowiskach klastrowych
- Obsługuje autentykację użytkowników

**MAILsweeper i WEBsweeper:**

Współpracują z następujacymi skanerami wirusów:

F-Secure, HBED+V, McAfee VirusScan, Symantec Antivirus, Sophos Anti-Virus

Rozpoznają następujące typy dokumentów: CDA (.doc, .xls, .ppt etc) PDF, text; i plików: - JPEG, BMP, GIF, TIF, AVI, MPEG, WAV i inne

Rozpoznaja archiwa: BINHEX, CMP, GZIP, LZH, MIME, TAR, TNEF, UUE (wiele wariantów), ZIP (wiele wariantów).