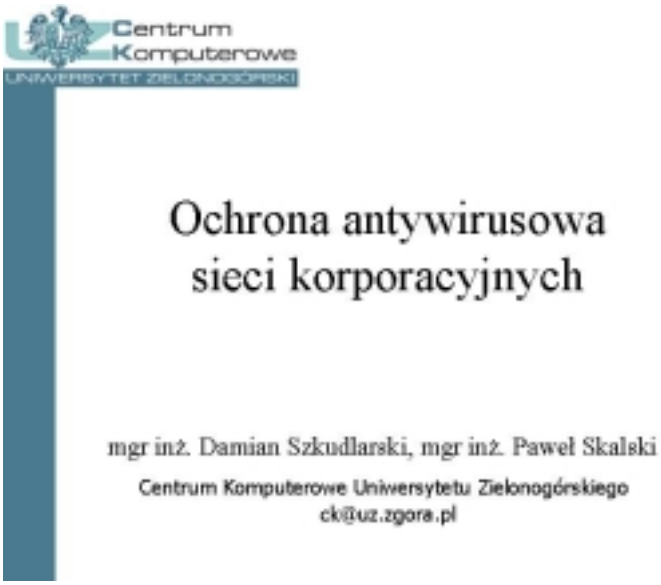
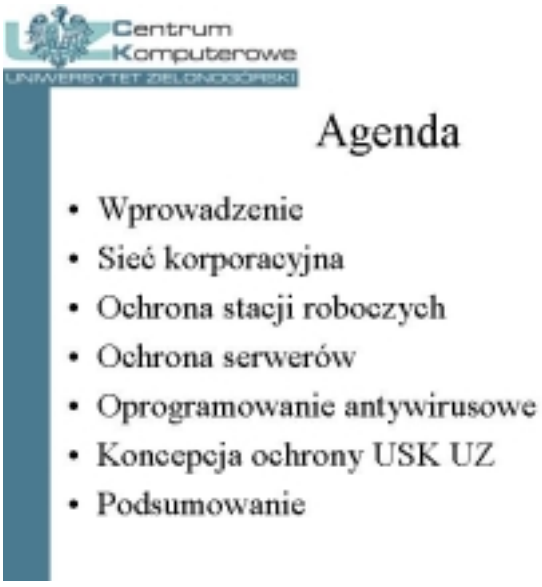
Ochrona antywirusowa sieci koporacyjnych

Damian Szkudlarski, Paweł Skalski
Centrum Komputerowe
Uniwersytet Zielonogórski

http://www.ck.uz.zgora.pl





Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI

Wprowadzenie

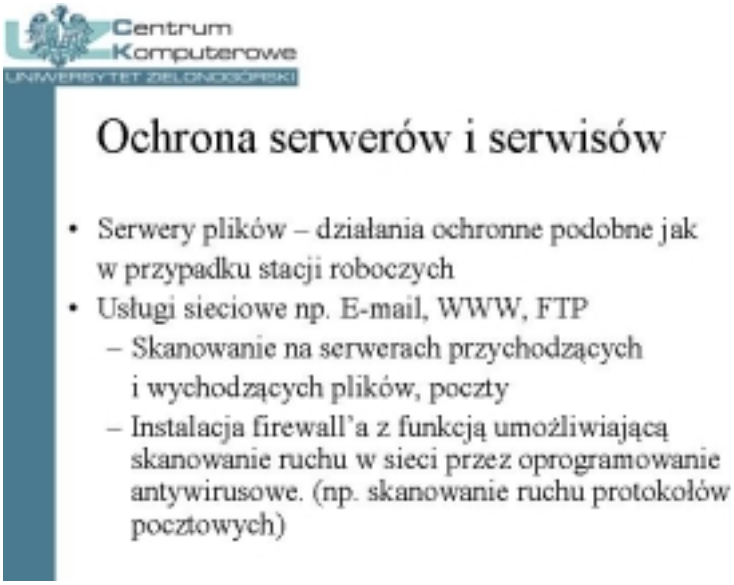
- Znaczny wzrost liczby wirusów rozpowszechnianych poprzez sieć Internet
- Łatwe rozpowszechnianie wirusów „pocztowych"
- Wzrost zagrożenia sieci korporacyjnych
- Zabezpieczenia antywirusowe sieci korporacyjnych
- Integracja oprogramowania antywirusowego z systemami Firewall

Schemat sieci korporacyjnej

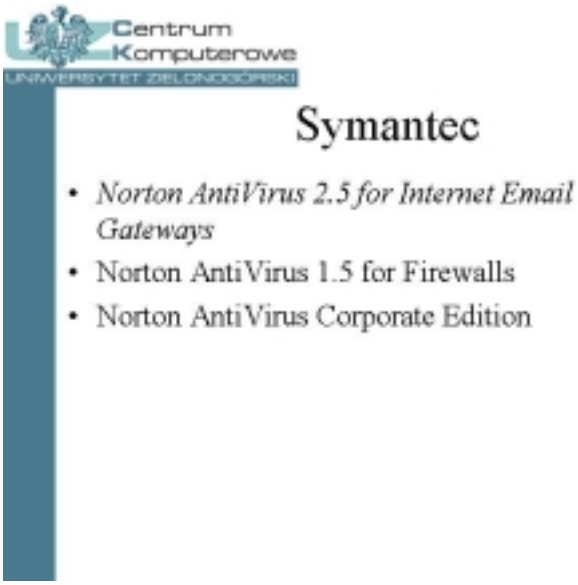
Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI

Ochrona stacji roboczych

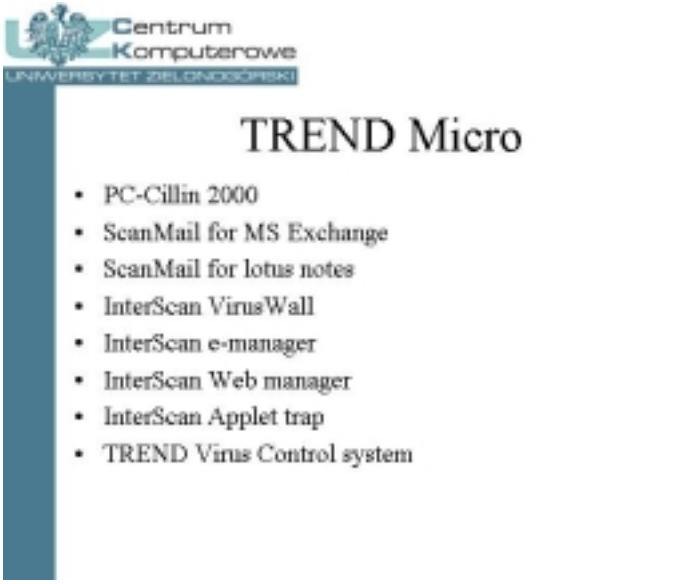
- Okresowe skanowanie zasobów dyskowych
- Ochrona antywirusowa w czasie rzeczywistym (on-access scanner)

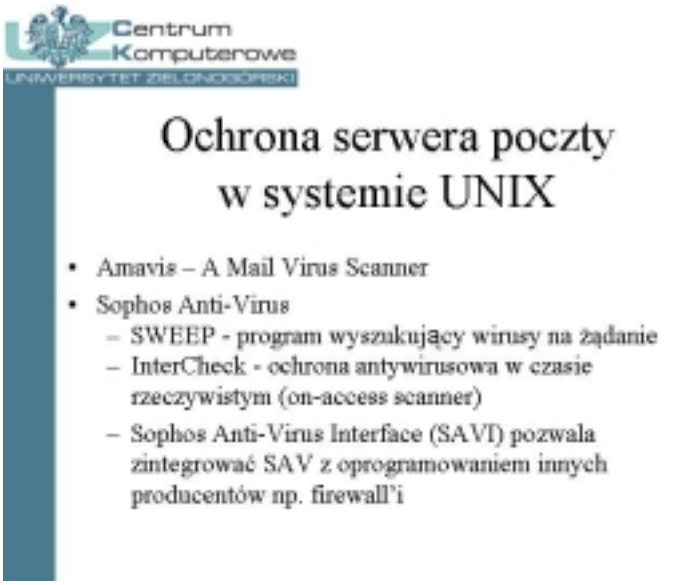

Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
Ochrona serwerów i serwisów
• Serwery plików – działania ochronne podobne jak w przypadku stacji roboczych
• Usługi sieciowe np. E-mail, WWW, FTP
– Skanowanie na serwerach przychodzących i wychodzących plików, poczty
– Instalacja firewall'a z funkcją umożliwiającą skanowanie ruchu w sieci przez oprogramowanie antywirusowe. (np. skanowanie ruchu protokołów pocztowych)


Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
Programy antywirusowe
1. Avast32
2. InoculateIT
3. AVK
4. NOD
5. F-MacroW
6. AVP
7. HMVS
8. Norton AntiVirus 2000
9. DrWeb
10. Access Macro Virus Scanner
11. F-Prot
12. PC-cillin
13. F-mIRC
14. F-Prot for Windows
15. F-Script
16. F-Secure
17. Scan
18. Sophos Anty Virus

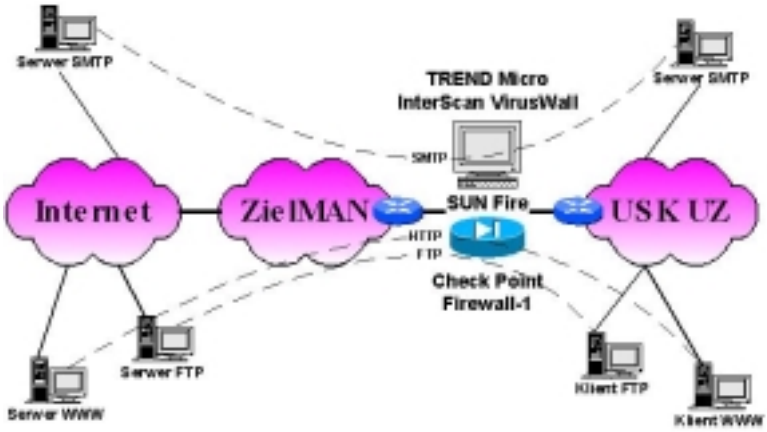

Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
Symantec
• Norton AntiVirus 2.5 for Internet Email Gateways
• Norton AntiVirus 1.5 for Firewalls
• Norton AntiVirus Corporate Edition


Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
Kaspersky
• Kaspersky™ Anti-Virus (KAV) for Linux Workstation
• Kaspersky™ Anti-Virus (KAV) for FreeBSD
• Kaspersky™ Anti-Virus (KAV) for Novell Netware
• Kaspersky™ Anti-Virus (KAV) for Linux Server
• Kaspersky™ Anti-Virus (KAV) for Windows NT Server
• Kaspersky ™ Anti-Virus dla Exchange
• Kaspersky™ Anti-Virus (KAV) for Workstation
• Kaspersky™ Anti-Virus Personal


Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
TREND Micro
• PC-Cillin 2000
• ScanMail for MS Exchange
• ScanMail for lotus notes
• InterScan VirusWall
• InterScan e-manager
• InterScan Web manager
• InterScan Applet trap
• TREND Virus Control system


Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
Ochrona serwera poczty w systemie UNIX
• Amavis – A Mail Virus Scanner
• Sophos Anti-Virus
– SWEEP - program wyszukujący wirusy na żądanie
– InterCheck - ochrona antywirusowa w czasie rzeczywistym (on-access scanner)
– Sophos Anti-Virus Interface (SAVI) pozwala zintegrować SAV z oprogramowaniem innych producentów np. firewall'i

Koncepcja ochrony antywirusowej dla Uczelnianej Sieci Komputerowej Uniwersytetu Zielonogórskiego



Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI

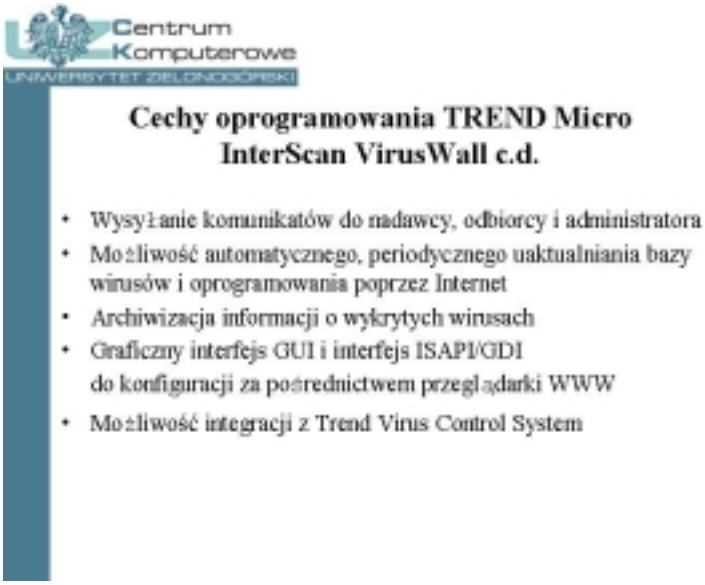
Koncepcja ochrony antywirusowej Uczelnianej Sieci Komputerowej Uniwersytetu Zielonogórskiego

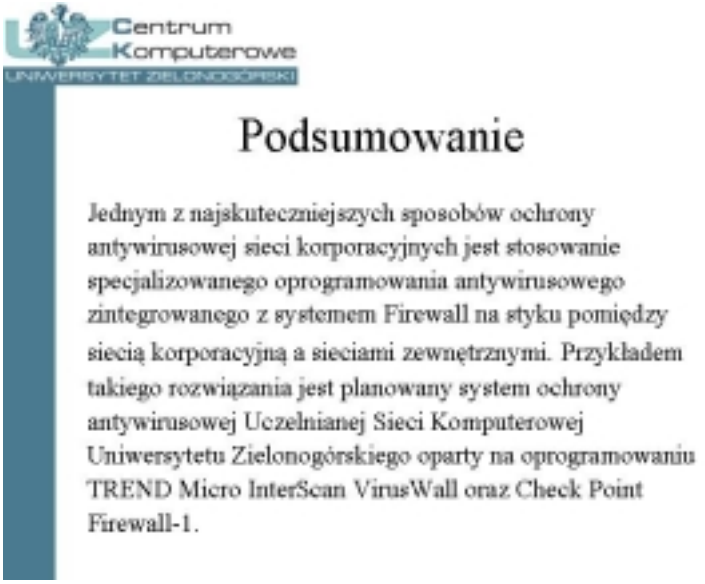
- Platforma sprzętowa **SUN Fire 280R**
- Oprogramowanie **TREND Micro InterScan VirusWall**
  - E-mail VirusWall
  - Web VirusWall
  - FTP VirusWall
- Współpraca z oprogramowaniem **Check Point Firewall-1**

Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI

Cechy oprogramowania TREND Micro InterScan VirusWall

- Pełna zgodność ze specyfikacją CVP, gwarantująca współpracę z Check Point FireWall-1
- Skanowanie przychodzących i wychodzących listów SMTP i ich załączników w czasie rzeczywistym
- Skanowanie ruchu HTTP i FTP w czasie rzeczywistym
- Automatyczne "leczenie" zainfekowanych plików
- Wykrywanie niebezpiecznych kontrolek ActiveX i apletów Java. Opcjonalne blokowanie wszystkich kontrolek ActiveX i apletów Java
- Wykrywanie i usuwanie znanych i nieznanych wirusów makr "w locie"


Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
Cechy oprogramowania TREND Micro InterScan VirusWall c.d.
• Wysyłanie komunikatów do nadawcy, odbiorcy i administratora
• Możliwość automatycznego, periodycznego uaktualniania bazy wirusów i oprogramowania poprzez Internet
• Archiwizacja informacji o wykrytych wirusach
• Graficzny interfejs GUI i interfejs ISAPI/GDI do konfiguracji za pośrednictwem przeglądarki WWW
• Możliwość integracji z Trend Virus Control System


Centrum Komputerowe
UNIWERSYTET ZIELONOGÓRSKI
Podsumowanie
Jednym z najskuteczniejszych sposobów ochrony antywirusowej sieci korporacyjnych jest stosowanie specjalizowanego oprogramowania antywirusowego zintegrowanego z systemem Firewall na styku pomiędzy siecią korporacyjną a sieciami zewnętrznymi. Przykładem takiego rozwiązania jest planowany system ochrony antywirusowej Uczelnianej Sieci Komputerowej Uniwersytetu Zielonogórskiego oparty na oprogramowaniu TREND Micro InterScan VirusWall oraz Check Point Firewall-1.