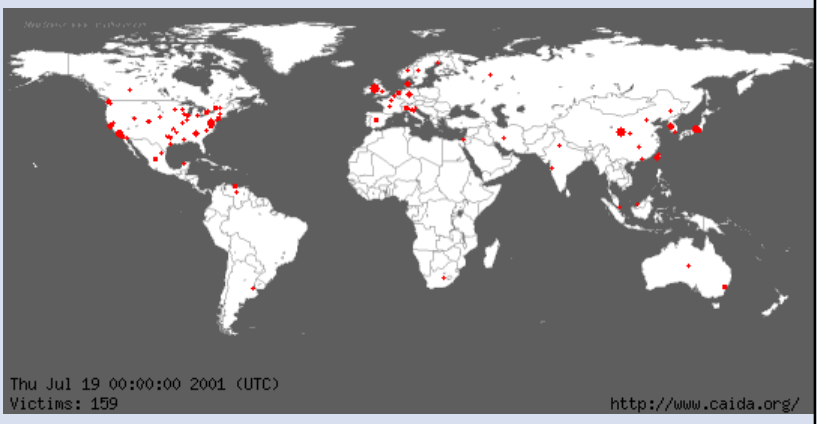
Incident Response: Was macht Sinn?

Roger Halbheer
Chief Security Advisor
Microsoft Schweiz GmbH
roger.halbheer@microsoft.com

Code Red (2001)



GO OUT IT-SECURITY HOSTING

klubschule MIGROS

Microsoft

VISANA Wir tragen Sorge.

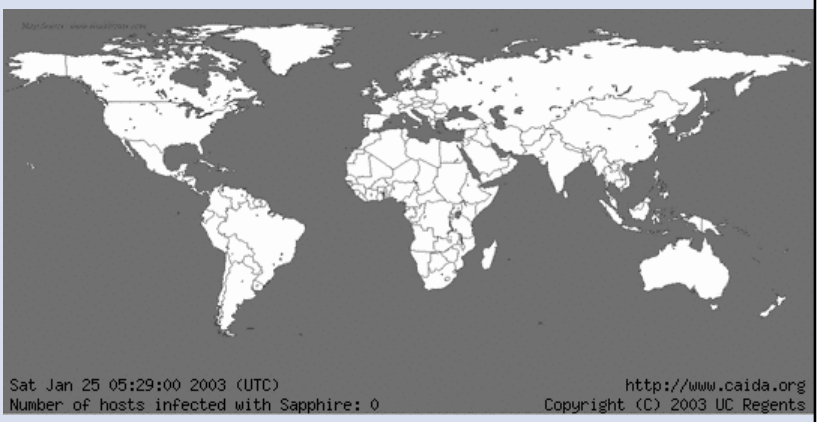
ca

IT - Security Forum #5

PROFESSIONAL COMPUTING

netzwoche

Slammer (2003)



86

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

Microsoft

VISANA Wir tragen Sorge.

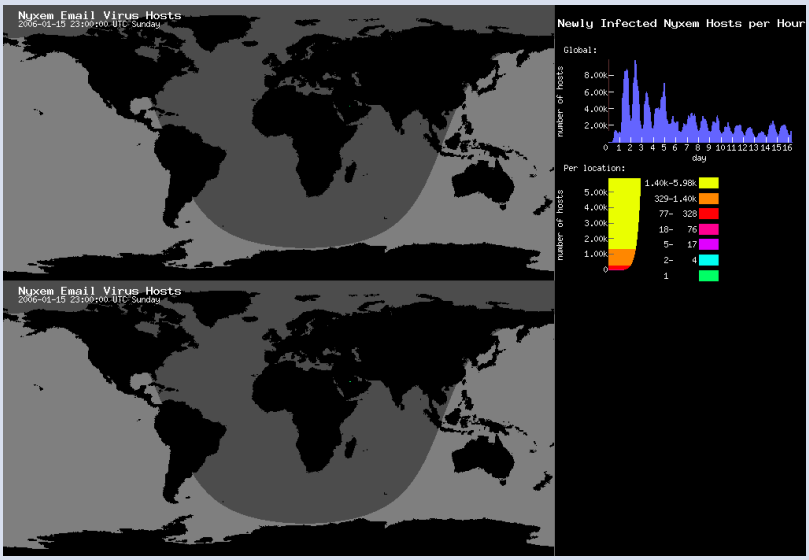
ca

IT - Security Forum #5

PROFESSIONAL COMPUTING

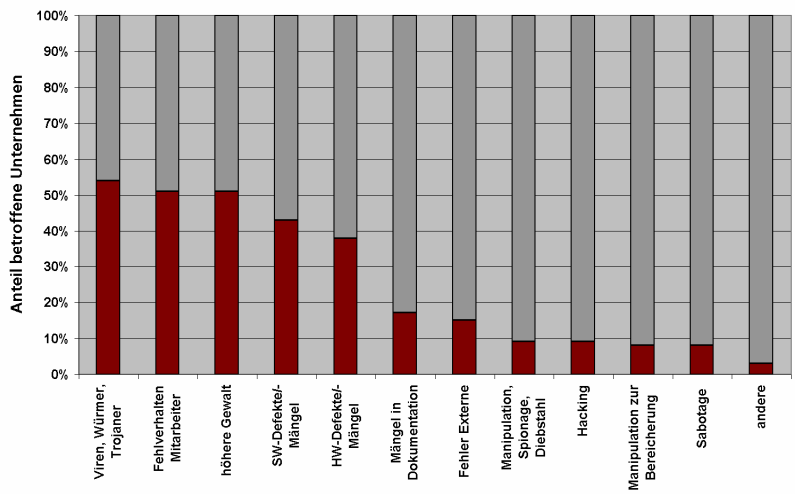
netzwoche

Nyxem



87

Passiert das wirklich alles?



Quelle: KES/Microsoft-Sicherheitsstudie 2004
(Umfrage unter 160 mittelständischen und grossen Unternehmen, v.a. Deutschland)

88

Welche Veränderungen werden erwartet?

Ursachen	*heute*	*in Zukunft*
Fehlverhalten Mitarbeiter	1	2
Viren, Würmer, Trojaner	2	1
Manipulation, Spionage, Diebstahl	3	4
SW-Defekte/-Mängel	4	5
Hacking	5	3

Quelle: KES/Microsoft-Sicherheitsstudie 2004
(Umfrage unter 160 mittelständischen und grossen Unternehmen, v.a. Deutschland)

89

IT - Security Forum #5

Mit wenig bereits viel erreichen!

1 Verantwortlichkeit
2 Backup
3 Virenschutz
4 Internetverbindung
5 Software warten
6 Mobile Computing
7 Passwörter
8 Benutzerrichtlinien
9 Sensibilisierung
10 Ordnung

10-Punkte-Programm
des Vereins InfoSurance

Quelle: http://www.infosurance.ch
direkt: http://www.infosurance.ch/de/kmu.htm

IT - Security Forum #5

Incident Response

- Wie abhängig sind Sie von Ihrer IT?
- Wie lange darf ein Ausfall dauern?
- Können Sie noch vollständig mit Papier arbeiten?
- Wie schnell kriegen Sie wieder Hardware?
- Wie schnell ist Ihr Partner verfügbar?
- Wie schnell Ihr Internet Service Provider?
- Was brauchen Sie in diesem Zusammenhang?
- Wie umfassend muss ein „Business Continuity Plan“ sein?
- Forensische Analyse/Strafverfolgung?
- …

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

Microsoft

VISANA Wir tragen Sorge.

ca

IT - Security Forum #5

PROFESSIONAL COMPUTING

netzwoche

Business Continuity

- Erarbeiten Sie einen minimalen „Business Continuity Plan“
  - Szenarien und den Einfluss auf Ihr Geschäft
  - Notfall-Plan
    - Ziele
    - Anforderungen
    - Team
    - Abhängigkeiten
  - Pflege
  - Training/Übung

92