IT Sicherheit

IHK-Kollegentreff - 9. Mai 2006

Jochen Savelberg - Euregio.Net AG
jochen@euregio.net

Übersicht

- Backup-Strategien
- Anti-Viren und Anti-Spam-Schutz
- Sicherheit von Websites
- Firewalls

Backup-Strategien

- Wie hat die Datensicherung zu erfolgen?

  Verfahren, Regelmässigkeit und Aktualität

- Wer ist für die Datensicherung verantwortlich?

  EDV-Abteilung, externer Dienstleister,...

- Wann werden Datensicherungen durchgeführt?

  Zeitplan (live, täglich, wöchentlich, nach/vor einer Programm-Installation,...)

Backup-Strategien

- Welche sollen Daten gesichert werden? Abhängig von:
  - der Art der Daten: maschinell wiederherstellbar (Programme), manuell wiederherstellbar (Originale vorhande) oder unersetzlich (keine Originale)
  - dem Wert der Daten: welcher Investition ist notwendig für die Sicherung und Wiederherstellung,
  - der Änderungshäufigkeit der Daten: Bestriebssysteme und Software ändern selten, Datenbank ändern oft...
  - gesetzlichen Vorschriften: Rechnungen, Log-Dateien,...

Backup-Strategien

- Welches Speichermedium ist zu verwenden?
  - Lokale Partition oder 2. Festplatte im eigenen PC
  - RAID-System: RAID1 (Spiegelung), RAID5 (mit Parität)
  - Wechselmedien: CD, DVD, Laufbänder, Festplatten
  - Backup-Server im lokalen Netzwerk oder Internet

Backup-Strategien

- Wo wird die Datensicherung aufbewahrt?
  - Onsite (vor Ort): schneller Zugriff
  - Offsite (ausserhalb): Sicherheit vor Feuer, Diebstahl, Katastrophen. Bietet Redundanz.
- Wie lange sind Backups aufzubewahren?
  - gesetzliche Bestimmungen für Rechnungen, Log-Dateien
  - ab wann sind Datenbestände veraltet und überflüssig?

Backup-Strategien

- Wann und wie werden Datensicherungen auf ihre Wiederherstellbarkeit überprüft?
  - Daten zurück auf ein Test-System überspielen
  - Programme zur Integritäts-Prüfung verwenden
  - Reinigen der Leseköpfe von Wechselmedien
  - Erstmalige Überprüfung nach Einführung eines neuen Backup-Systems und danach vierteljährliche Überprüfung

Backup-Strategien

- Welche Backupstrategie wird angewandt?

  (a) vollständiges Backup am Wochenende

  (b) inkrementelles oder differenzielles Backup werktags um Mitternacht

- Abhängig von
  - der Grösse des Datensatzes
  - des Zeitaufwandes
  - der Wichtigkeit der Daten

Backup-Strategien

- Beispiel aus der Praxis:

  Euregio.Net setzt auf folgende Strategie:

  - Unterbrechungsfreie Stromversorgung
  - Server mit Hardware RAID1 oder RAID5-Systemen
  - Lokaler Backup-Server im Rechenzentrum für tägliche inkrementelle Backups
  - Redundante Server für DNS, E-Mail und teilweise Web
  - Offsite Backups in Wirtzfeld

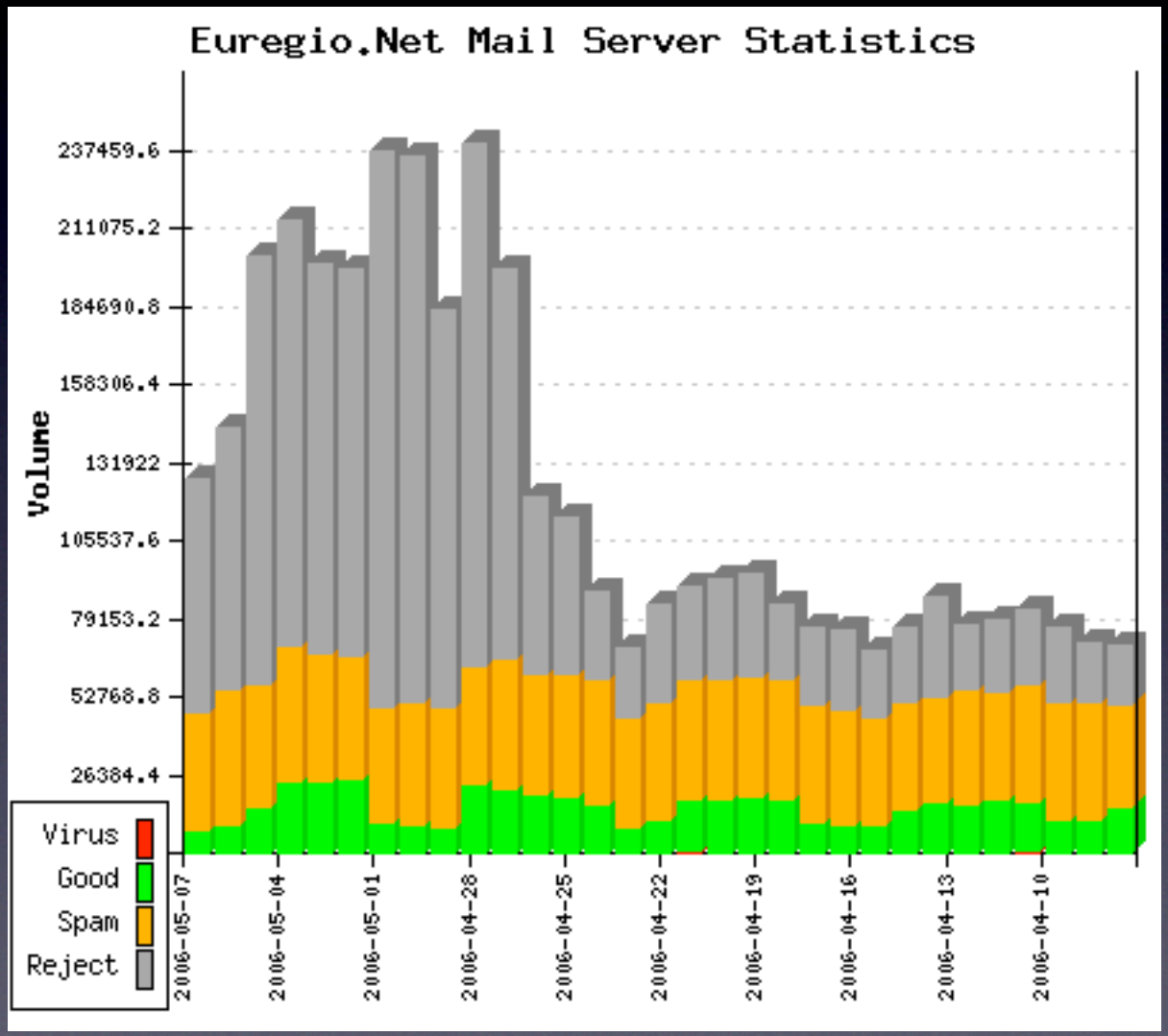
Backup-Produkte

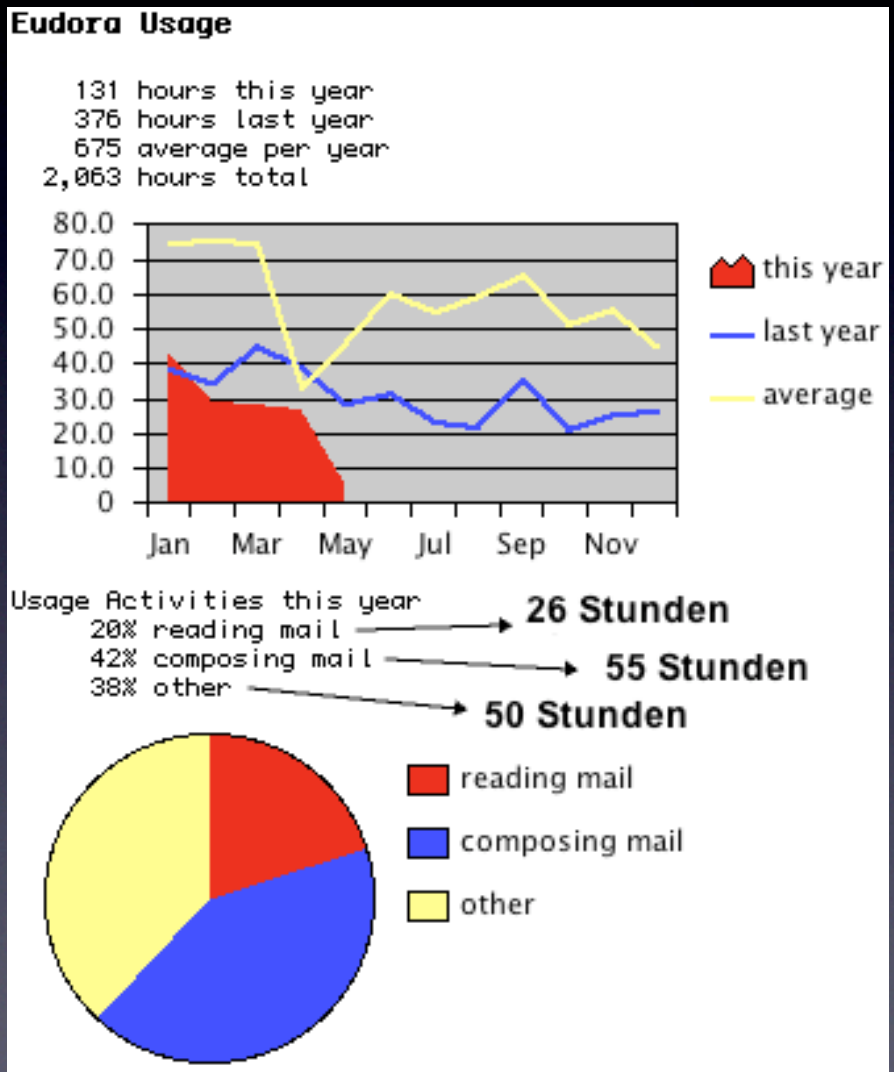
- www.emcinsignia.com: Retrospect, Netzwerk-Backup-Systeme
- www.symantec.com: BackUp Exec, LiveState
- www.lacie.be: Ethernet Disk
- www.prosofteng.com: Data Rescue

Anti-Virus & Anti-Spam

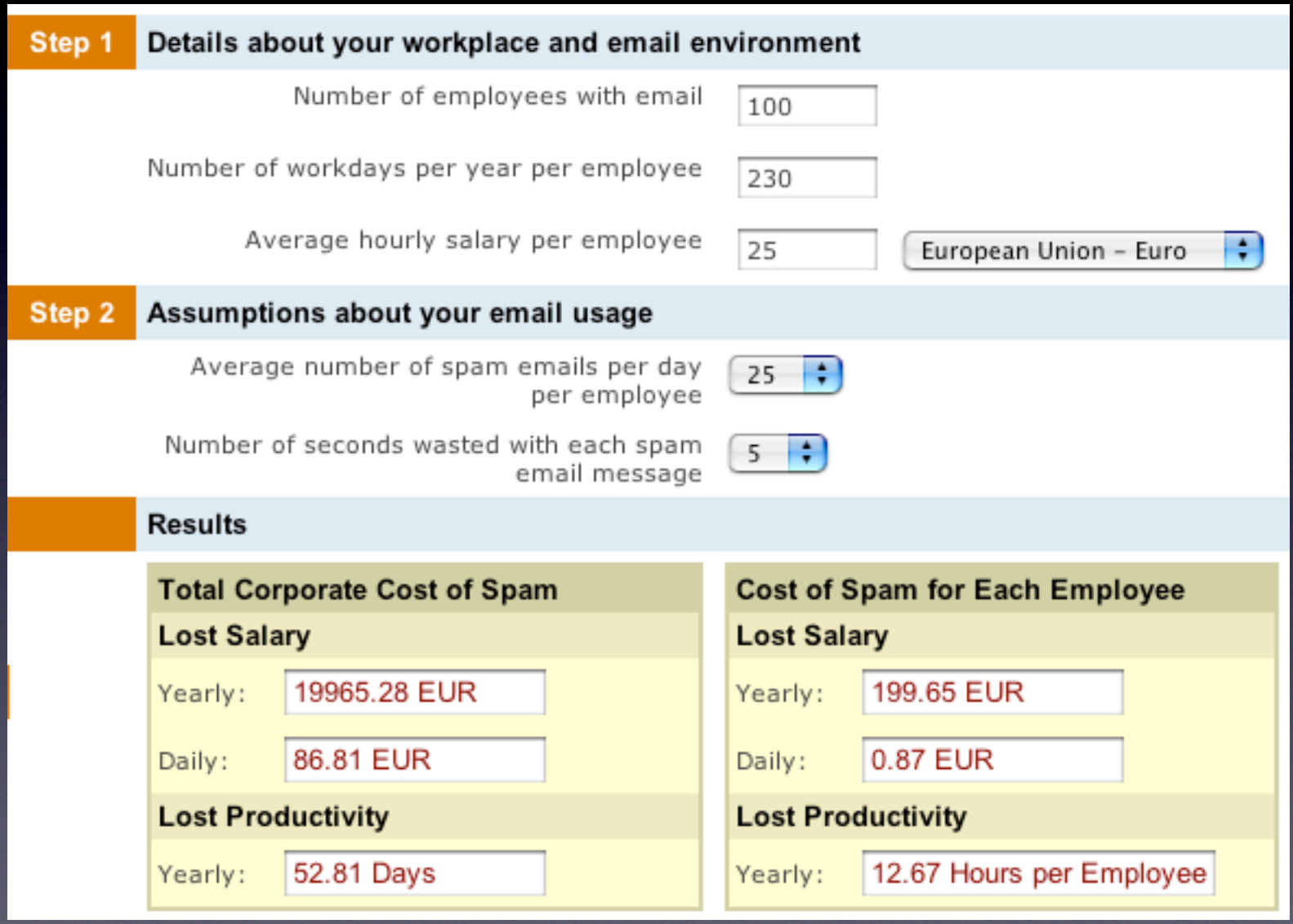
- 60 Milliarden Spam-Nachrichten pro Tag
- 180.000+ Gefahren (Viren, Würmer, Trojaner, Macro-Viren...) existieren derzeit
- Viren verbreiten sich per E-Mail, IM, Web, FTP, Wechselmedien, Raubkopien
- Spam und Viren verschlingen Unmengen an Zeit und Geld

Anti-Virus & Anti-Spam





Anti-Virus & Anti-Spam



Step 1 Details about your workplace and email environment

Number of employees with email	100
Number of workdays per year per employee	230
Average hourly salary per employee	25 European Union – Euro

Step 2 Assumptions about your email usage

Average number of spam emails per day per employee	25
Number of seconds wasted with each spam email message	5

Results

Total Corporate Cost of Spam		Cost of Spam for Each Employee	
Lost Salary		**Lost Salary**	
Yearly:	19965.28 EUR	Yearly:	199.65 EUR
Daily:	86.81 EUR	Daily:	0.87 EUR
Lost Productivity		**Lost Productivity**	
Yearly:	52.81 Days	Yearly:	12.67 Hours per Employee

http://www.praetor.net/Marketing/spamcalc.htm

Anti-Virus & Anti-Spam

- Welchen Schutz gibt es auf dem eigenen PC?
  - Zugriff reglementieren und einschränken (auch für USB-Sticks, Wechselmedien,...)
  - Anti-Virus-Software (kommerziell oder gratis): nur effektiv wenn immer auf dem neuesten Stand
  - Spam-Filter: erstes Training durchführen, Lernfähigkeit aktivieren, separate E-Mail-Adressen verwenden, keine verdächtigen Anhänge öffnen, nicht auf Spam-Mails reagieren
  - Firewall: aktiviert und optimiert für das eigene System
  - Adware-Zerstörer: regelmässig aktualisieren/verwenden

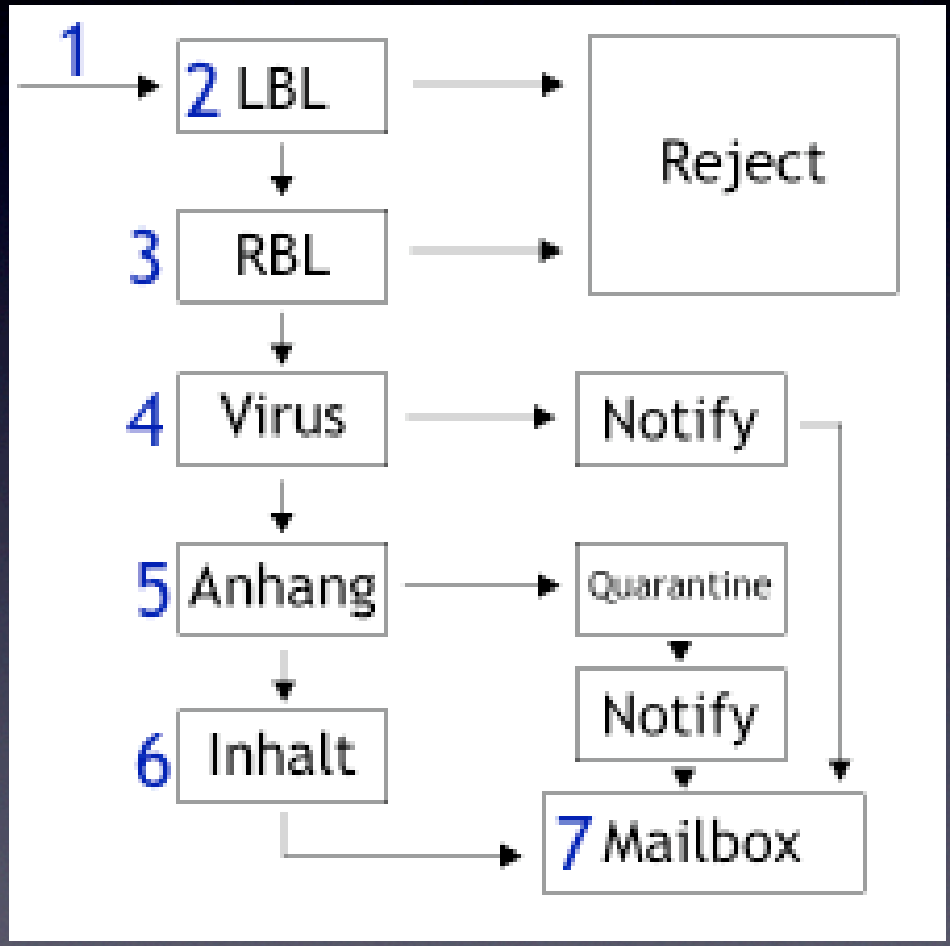
Anti-Virus & Anti-Spam

Welchen Schutz gibt es im Netzwerk?

- Netzwerk-Server (auch Mail-Server)
  - globale Spam-Filter und Anti-Viren Scanner
  - Zugriffsrechte limitieren, offene Relays schliessen
  - SPF (Sender Policy Framework) einrichten
- Netzwerk-Perimeter (Border)
  - Zugang von aussen sperren/limitieren
  - Spam-Firewalls einsetzen
  - externe Filter-Dienste einsetzen

Anti-Virus & Anti-Spam

- Wie funktionieren Filter?
- Einsatz von schwarzen Listen (LBL = Local Black List - RBL = Realtime Black List)
- Analyze der Nachrichten und Anhängen auf Viren
- Analyse der E-Mail durch eine Vielzahl Regeln



Anti-Virus & Anti-Spam

- Der Kampf gegen Viren und Spam ist eine Sisyphus-Arbeit, die sehr zeitintensiv ist. Spammer und Viren-Autoren lernen ständig hinzu, um bestehende Filter zu umgehen.
- Externe Dienstleister können E-Mails filtern und analysieren, jedoch sollte jeder PC mit der entsprechenden Anti-Viren-Software ausgestattet sein.

Anti-Virus & Anti-Spam

- Beispiel aus der Praxis:

  Euregio.Net setzt auf folgende Systeme:

  - FortiGate Anti-Virus und Anti-Spam Appliance
  - MailScanner mit ClamAV
  - POSSE (Eigenentwicklung)
  - Symantec Norton Anti-Virus, McAfee Virex
  - Real-Time Blacklists (RBL): SpamHaus, ORDB, SORBS, DNSBL, DSBL, spamcop.net
  - Lokale Blocklisten

Anti-Virus & Anti-Spam

- http://de.wikipedia.org/wiki/Computervirus
- http://de.wikipedia.org/wiki/Spam
- http://www.clamav.net
- http://www.freeav.de
- http://www.spybot.info
- http://www.symantec.com
- http://www.mcafee.com
- http://www.sophos.com
- http://www.trendmicro.com
- http://www.barracudanetworks.com
- http://www.fortinet.com

Website Sicherheit

- Physischer Schutz vor unbefugtem Zugriff
- Hardware und Betriebssystem optimieren
- Zugriffsrechte limitieren
- Software-Audit und Aktualisierung
- Absicherung durch intelligente Programme
- Analyse und Verfolgung von Angriffen

Website Sicherheit

- Physischer Schutz vor unbefugtem Zugriff
  - Überwachung des direkten Zugriffs: Hardware, Tastatur, Maus, Monitor, serielle Schnittstelle, Wechselmedien
  - Absicherung gegen Feuer, Wasser, Überspannung
- Hardware und Betriebssystem optimieren
  - ausreichend RAM installieren
  - RAID1 oder RAID5
  - Backup-Strategie erstellen
  - letzte System-Updates und Patches

Website Sicherheit

- Zugriffsrechte limitieren
  - nur authorisierte Zugriffe auf das komplette System
  - verschiedene Niveaus von starken Passwörtern
  - Verschlüsselung verwenden wenn verfügbar
  - Netzwerkzugriff pro IP-Adresse limitieren
- Software-Audit und Aktualisierung
  - Überprüfung der installierten (OpenSource) Software
  - Installation und ständige Aktualisierung der letzten Versionen

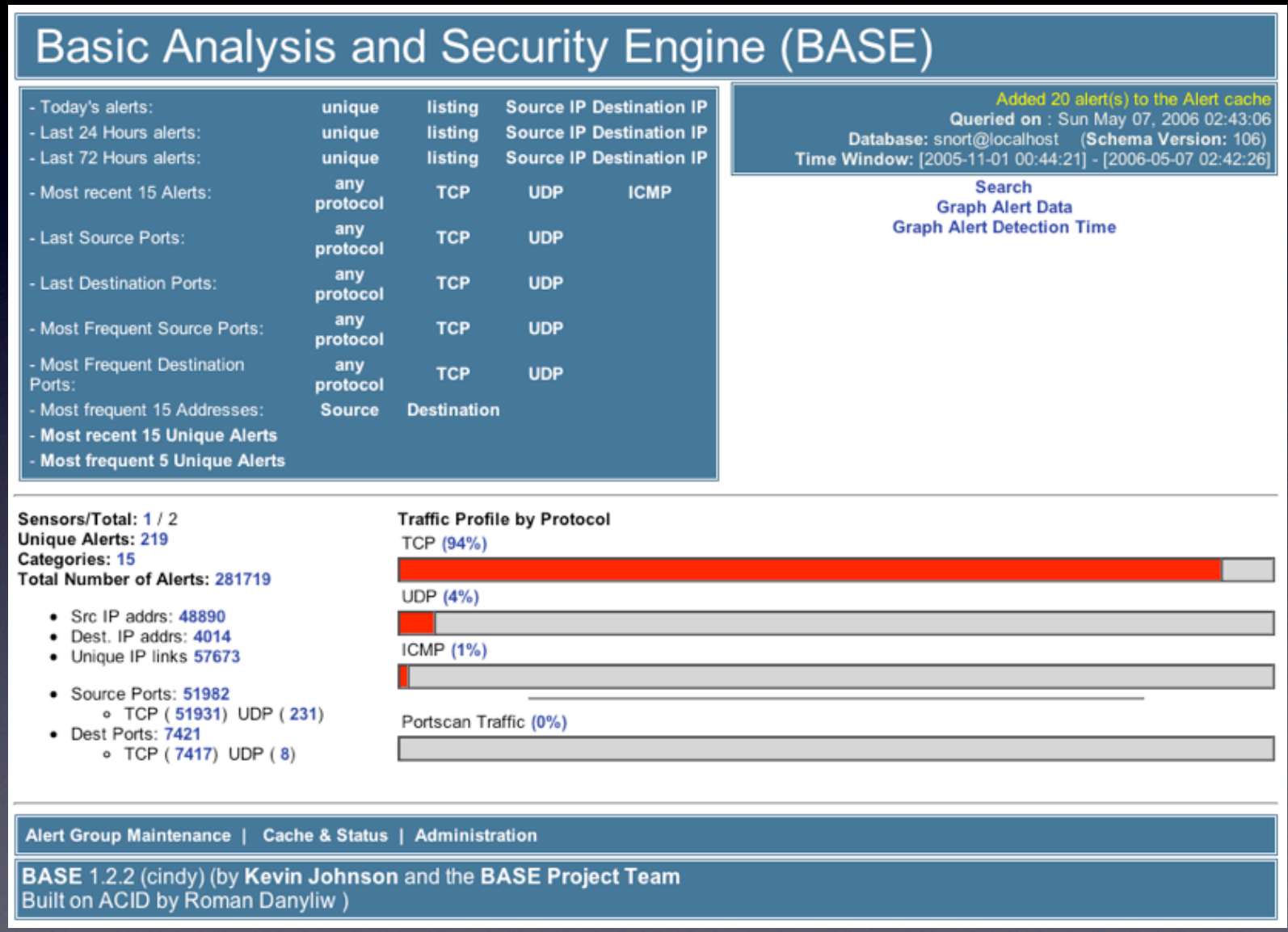
Website Sicherheit

- Absicherung durch intelligente Programme
  - intelligente Web-Formulare, die Spam erkennen und schwarze Listen selbstständig ergänzen
  - Formulare durch Passwörter oder Captcha schützen
  - bekannte Sicherheitslücken durch Monitor-Programme ersetzen, die dynamisch die Firewall aktualisieren
  - “Hacker-Tools” verwenden um Schwachstellen zu entdecken (z.B. Nessus, nmap)
  - E-Mail-Adressen verschlüsseln (JavaScript, Image...)

Website Sicherheit

- Analyse und Verfolgung von Angriffen
  - Analyse von Web-Logs um Schwachstellen zu entdecken
  - Netzwerk-Protokoll-Scanner einsetzen
  - Netzwerk-Tools zur Identifizierung der Angreifer einsetzen
  - Meldung von Angriffen bei der FCCU (Federale Abteilung gegen Computer Kriminalität)
  - Überwachung von WebSite-Inhalten und ggf. Alarm per E-Mail oder SMS

Website Sicherheit



Website Sicherheit

- Beispiel aus der Praxis:

  Euregio.Net setzt auf folgende Lösungen:

  - geschütztes Rechenzentrum in Brüssel, abgesichert durch Zugangskontrolle, Video-Überwachung, Klima-Kontrolle...
  - verschiedene Dienste auf separaten Server mit Hardware RAID, 2-4 GB RAM
  - gehärtetes MacOS X Server Betriebssystem (UNIX-basierend)
  - Apache Firewalls (mod_security), NetBarrier X, snort, nessus, eigene Kontroll-Systeme mit Alarm per SMS/Mail

Firewalls

- Schutz des eigenen Computers gegen Angriffe von aussen
- Schutz des Netzwerks
  - Zugriff auf Firmen-Daten von ausserhalb
  - Überwachung des internen und externen Datenverkehrs
  - DMZ und Bastion Hosts
  - Absicherung eines Funk-Netzwerks

Firewalls

- Schutz des eigenen Computers gegen Angriffe von aussen
  - unbedingt eine Firewall auf dem eigenen PC/Laptop installieren und entsprechend konfigurieren
  - alle unnötigen Programme entfernen oder sichern
  - Anti-Viren Software installieren und regelmässig nach Adware-Programmen suchen.

Firewalls

- Schutz des Netzwerks: Zugriff auf Firmen-Daten von ausserhalb
  - Virtual Private Networks (VPN) erlauben eine sichere Verbindung von externen PC's oder Netzwerken ins interne Firmen-Netzwerk - Protokolle wie IPSec benötigen spezielle Client-Programme und Netzwerk-Konfiguration.
  - Spezielle Software erlaubt den Austausch von Daten oder das Arbeiten auf internen Rechnern, z.B. Timbuktu Pro, pcAnywhere, VNC, Remote Desktop Connection, Apple Remote Desktop, GoToMyPC, LogMeIn,...

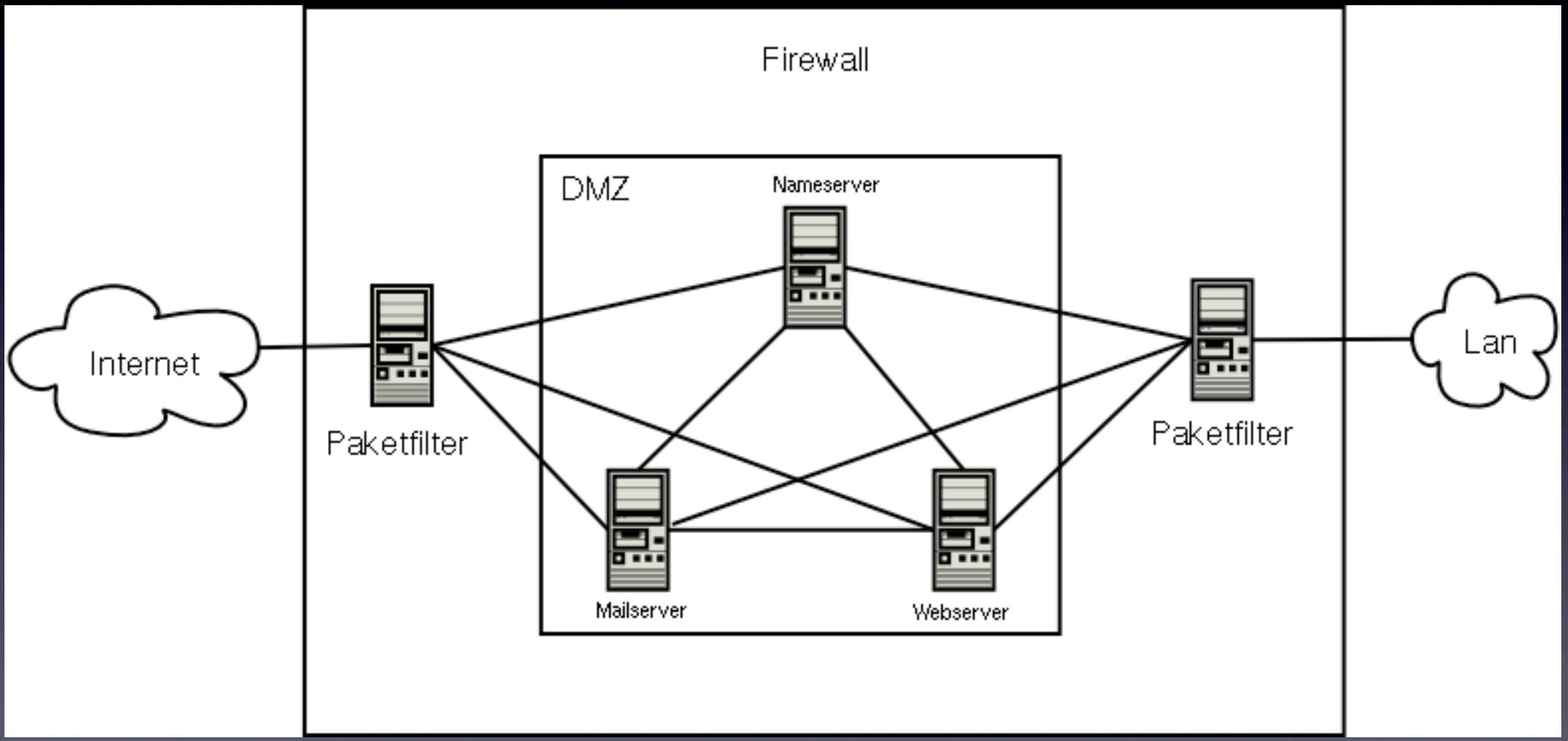
Firewalls

- Überwachung des internen und externen Datenverkehrs
  - Installation einer Perimeter-Firewall, die die offenen Pforten nach innen und aussen auf das Notwendigste begrenzt
  - Analyse der Firewall Log-Dateien
  - Kontrolle des Netzwerk-Verkehrs durch einen Paket-Analyzer

Firewalls

- DMZ und Bastion Hosts
  - Trennung von öffentlichen Diensten (Web/Mail/DNS) vom internen Netzwerk
  - Absicherung durch getrennte Netzwerke
  - optimierung der Geschwindigkeit für verschiedene Dienste

Firewalls



http://de.wikipedia.org/wiki/Demilitarized_Zone

Firewalls

- Absicherung eines Funk-Netzwerks
  - Standart-Passwort des WLAN-Routers ändern
  - Die SSID (Netzwerk-Name) ändern und das Aussenden abschalten
  - Passwort für das Netzwerk setzen
  - WLAN-Verschlüsselung aktivieren (mindestens WEP - besser WPA2)
  - Zugang durch MAC-Adressen limitieren
  - Antennen Reichweite auf das Nötigste begrenzen
  - Verhindern, dass eigene (private) Access-Points

Firewalls

- Beispiel aus der Praxis:

  Euregio.Net setzt auf folgende Lösungen:

  - Fortigate Firewall sowie separater snort Paketfilter
  - Host-Firewalls auf allen Servern und Computer
  - getrennte Netzwerke für Administration und Server
  - getrennte Administratoren- und Benutzer-Passwörter
  - Überwachung und Analyse der Firewall-Logs
  - Fernwartung und Datenzugriff mit Timbuktu Pro, ssh, SFTP

Firewalls

- http://de.wikipedia.org/wiki/Kategorie:IT-Sicherheit
- http://www.fortinet.com
- http://www.sonicwall.com
- http://www.zyxel.com
- http://www.watchguard.com
- http://www.snort.org
- http://www.netopia.com
- http://www.apple.com/server

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Links zu diesem Vortrag unter:
http://support.euregio.net/ihk-vortrag/

Quellen:

- Wikipedia
- Microsoft Small Business Team
- Internet Security Alliance
- European Commission
- Howstuffworks.com
- News.com
- Heise.de