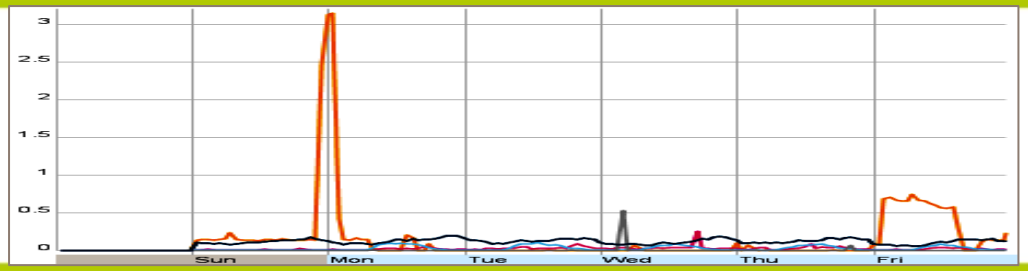
Westfälische Wilhelms-Universität Münster

IT-Sicherheitsmaßnahmen in der Praxis an einer Hochschule

Do 20.03.2014



wissen.leben
WWU Münster

Markus Speer / speer@wwu.de

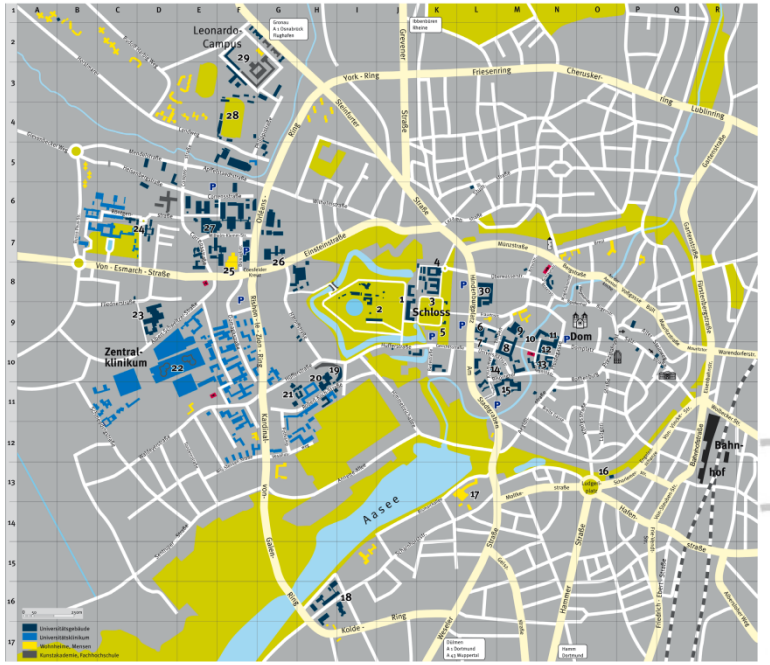
Zentrum für Informationsverarbeitung

Agenda

- Ausgangsituation an der Universität Münster
- Tatsächliche Bedrohungen, Herausforderungen und technische Maßnahmen
  - E-Mail
  - Hackerangriffe
  - Mobilty
- Organisatorische Maßnahmen
- Abschlussbemerkungen

Ausgangssituation / Kennzahlen

Kennzahl	WWU	UKM
Studierende	40.800	-
Mitarbeiter	6.650	8.400
Netzanschlüsse	36.300	26.700
WLAN-Access Points	1.130	720
Erschlossene Gebäude	183	98
Registrierte Endsysteme	37.400	
Nicht registrierte Endsysteme	46.400+ (WLAN)	
Nutzerkennungen	73.600	?
E-Mail-Accounts	66.900	?
Zentrale Server	570	?



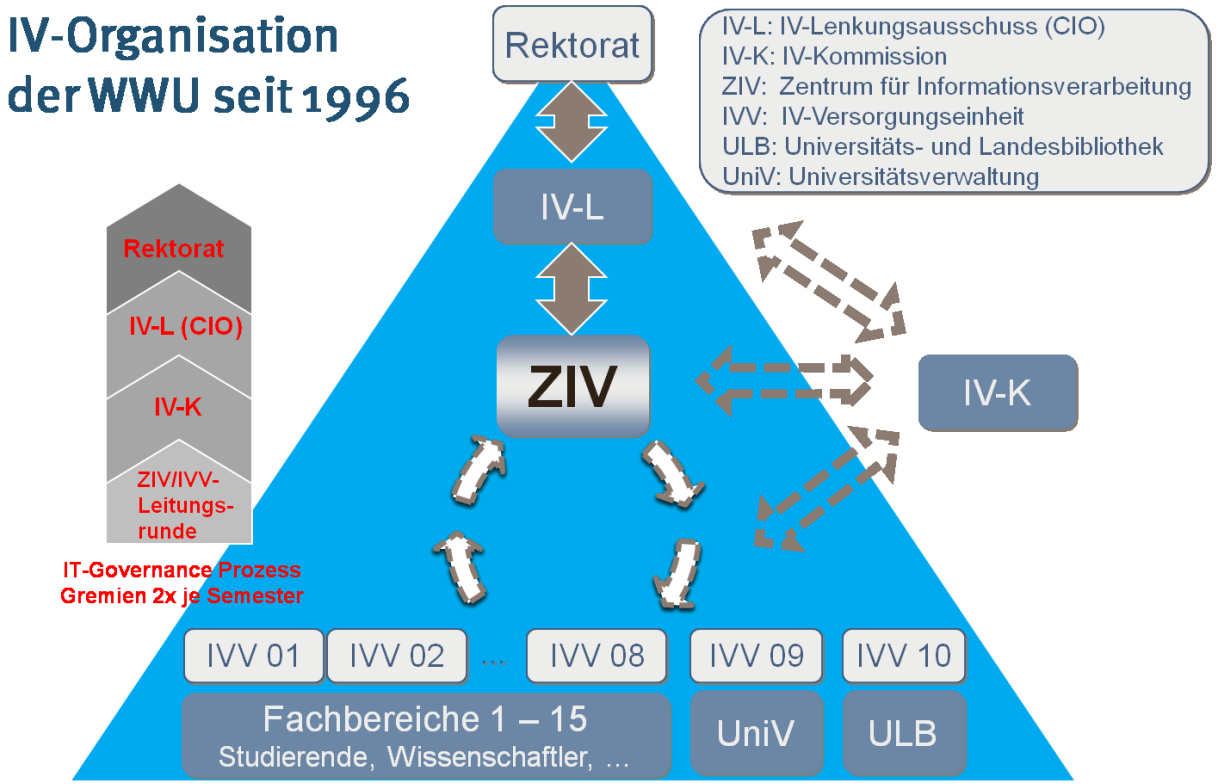
WWU: Westfälische Wilhelms Universität
UKM: Universitätsklinikum Münster

wissen.leben WWU Münster

Besondere Herausforderungen

- Grundsatz der Freiheit von Forschung und Lehre
- Vermeidung „unnötiger“ Nutzerbeeinträchtigung
  - Begrenzte Reglementierungsmöglichkeiten
  - Eine Vielfalt von Betriebssystemen, Anwendungen, …
  - Freizügige Internet-Nutzung
- Massiver Einsatz von nicht verwalteten (unbekannten) Geräten:
  - Mobile Geräte (WLAN)
  - Private Geräten (BYOD)
  - Studierende
  - Gäste / Externe
- Nutzung von externen (Cloud-)Services durch die Nutzer
- Anbindung von Studierendenwohnheimen

IV-Organisation



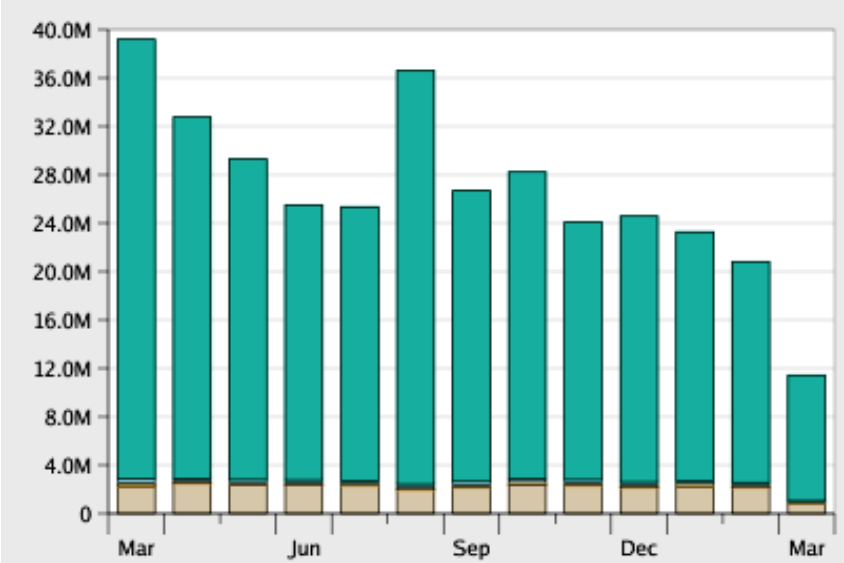
IV: Informationsverarbeitung (=IT)

Zentrale Verantwortlichkeit für das Kommunikationssystem im ZIV: LAN, TK/VoIP, ...

Wo ist hier die IT-Security?

Bedrohungen im Bereich E-Mail

Overview > Incoming Mail Graph



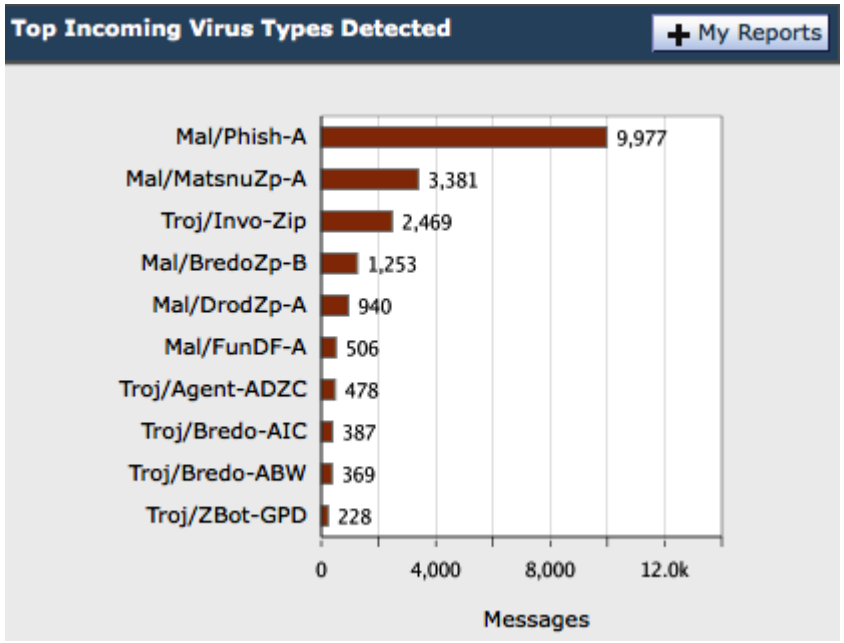
Overview > Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	90.3%	313.9M
Stopped as Invalid Recipients	0.8%	2.9M
Spam Detected	0.8%	2.7M
Virus Detected	0.0%	15.1k
Stopped by Content Filter	0.0%	0
Total Threat Messages:	**91.9%**	**319.6M**
Clean Messages	8.1%	28.1M
Total Attempted Messages:		**347.7M**

Betrachteter Zeitraum: 01.03.2013 – 13.03.2014

wissen.leben WWU Münster

Bedrohungen im Bereich E-Mail



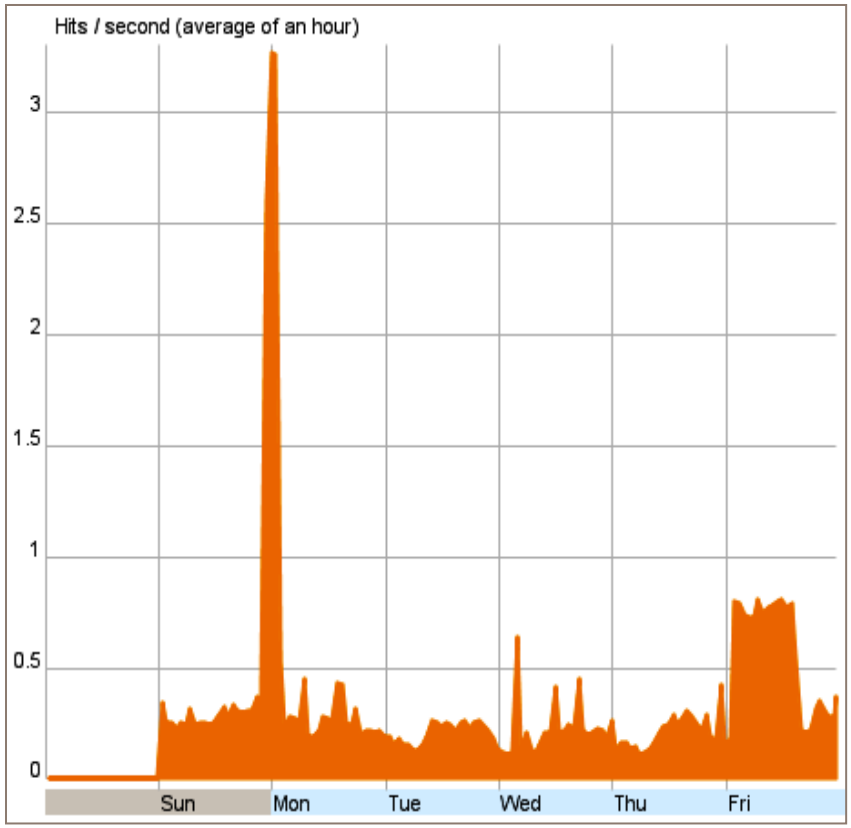
- Ca. 15.100 nicht durch den Reputationsfilter abgeblockte virenverseuchte Mails
- D.h. ca. 45 pro Tag

Maßnahmen im Bereich E-Mail
E-Mail Security Appliance

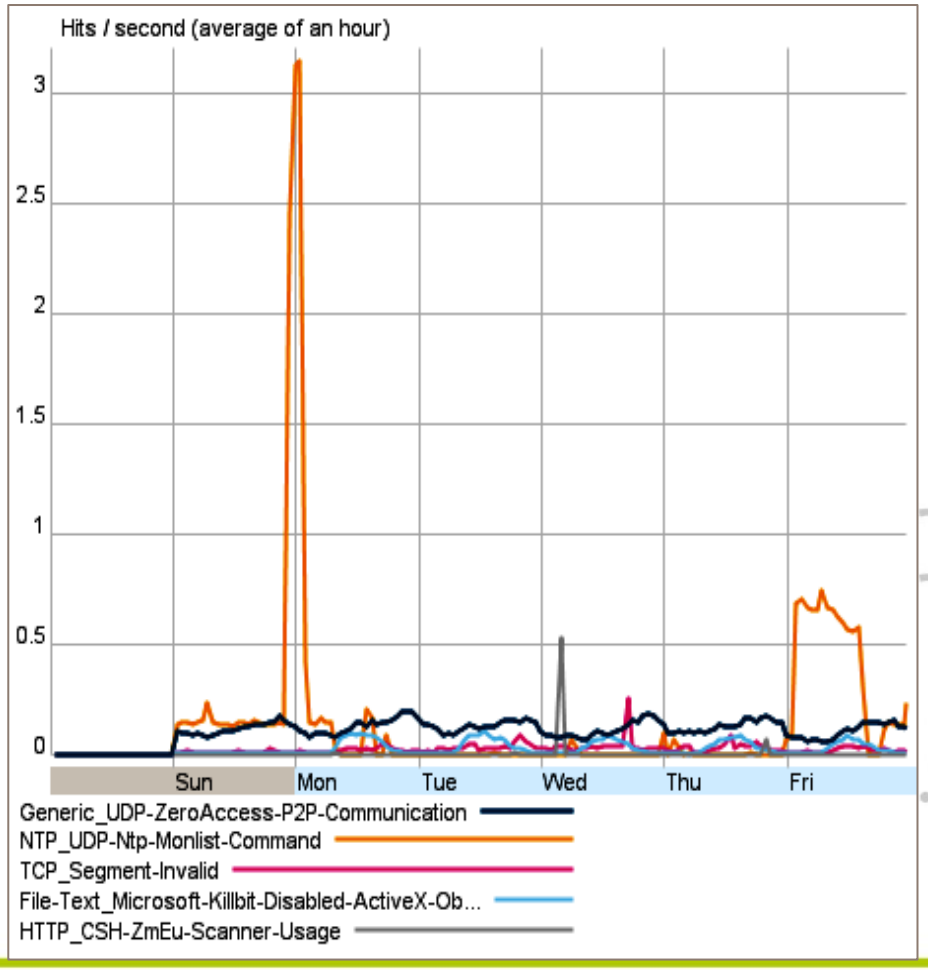
- Annahme von E-Mails nach Reputations-Filtering
- Wert für die Einstufung der IP-Absender-Adresse einer E-Mail
  1. Ablehnung einer E-Mail
  2. Drosselung des E-Mail-Empfangs
  3. Annahme der E-Mail
- 2.+3. Analyse und ggf. Markierung als Malware (Virenverseucht, Phishing-Mail, ...)
- Opt-In-Möglichkeit des Nutzer: automatisches Löschen einer markierten Mail
- Erfahrungen
  - Praktische keine False-Positives
    - meist „saubere“ Mail über E-Mail-Server mit schlechter Reputation
  - Gelegentlich kommt es zu „False-Negatives“.

Bedrohung durch Hackerangriffe: Reports des Intrusion Prevention Systems (IPS)

Top 5 Angriffe im zeitl. Verlauf

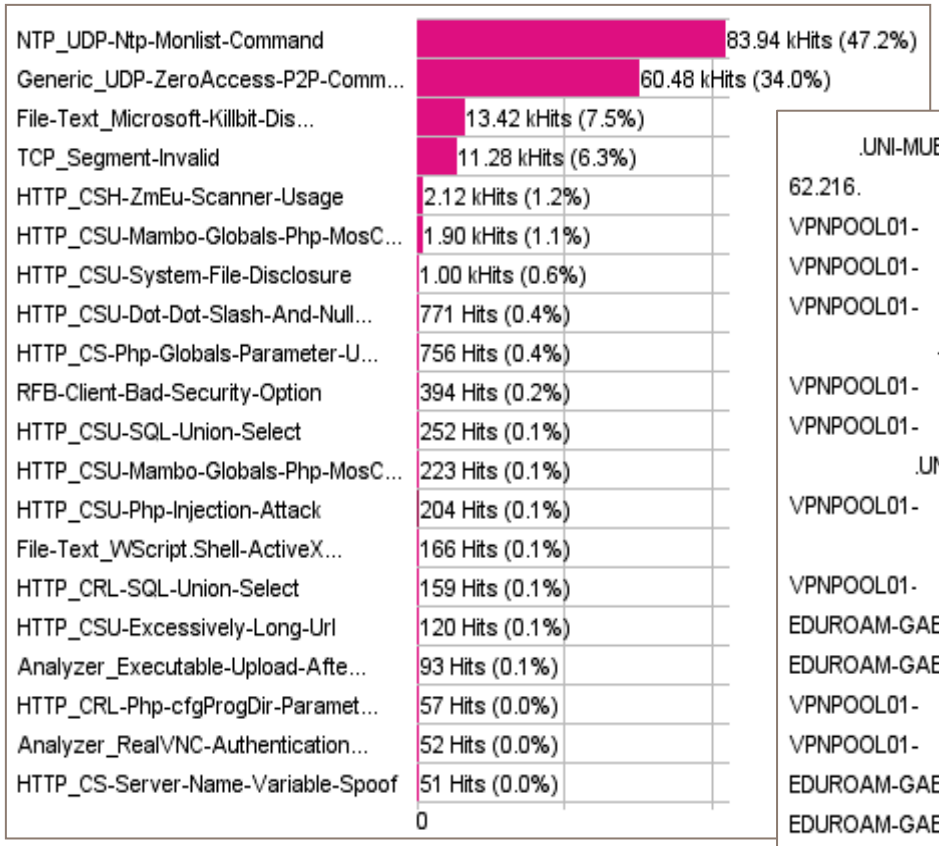


Angriffe insgesamt: So 09. – Fr 14.03.2014



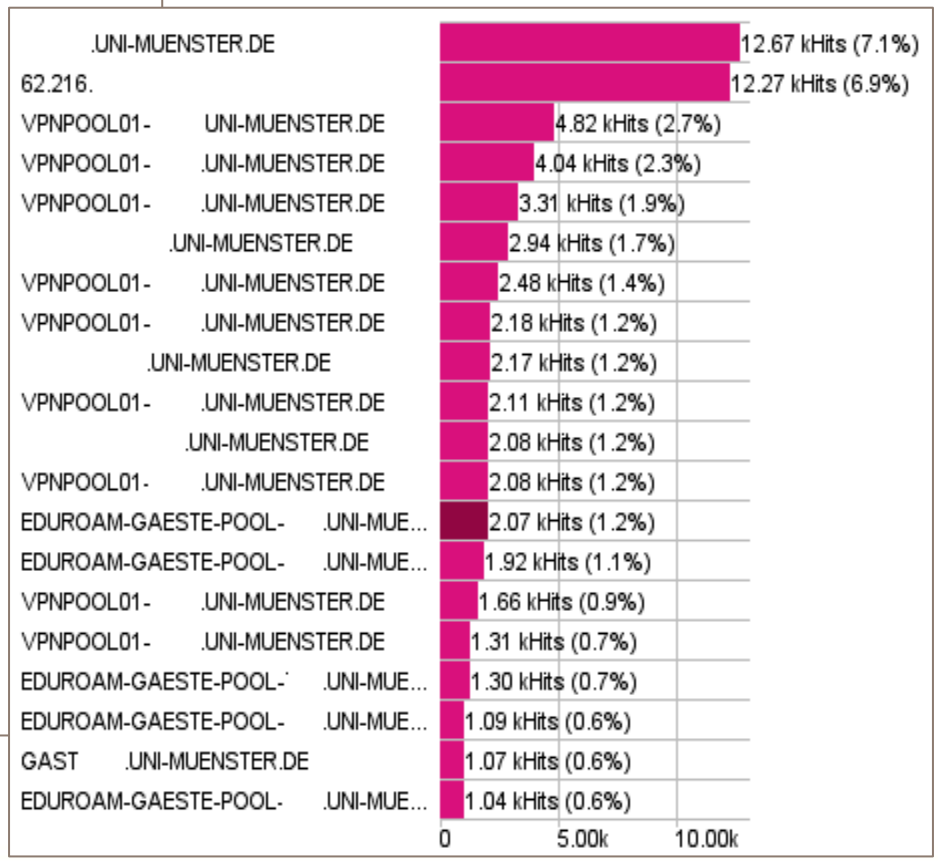
wissen.leben WWU Münster

Bedrohung durch Hackerangriffe



Top 20 Angriffe: So 09. – Fr 14.03.2014

Top 20 Angriffsziele



wissen.leben WWU Münster

Erfahrungen im Einsatz von Intrusion Prevention Systemen

- **Insgesamt seit 2005 mit guten Erfahrungen im Einsatz**
- Schutz gegen schadhafte Datenströme
  - Hackerangriffe
  - Malware
  - Fehlerhafte Pakete
- Automatische Erkennung der Anwendung: „Application Awareness“
  - YouTube
  - DropBox
  - …
- Erarbeitung einer Security-Policy in einer Einführungsphase
- Anschließend praktisch kein Pflegeaufwand
  - automatische Signatur-Updates
- Evtl. Single Point of Failure
  - Fehlfunktionen des IPS können gravierende Auswirkungen haben.
  - Fehlerhafte Signatur-Updates können Probleme verursachen.
- **Wichtig: Platzierung in der Netzstruktur: Wer soll vor wem geschützt werden?**
  - Grundsatz: alle unbekannten Geräte müssen durch das IPS!

Netzseitige Sicherheitsmaßnahmen

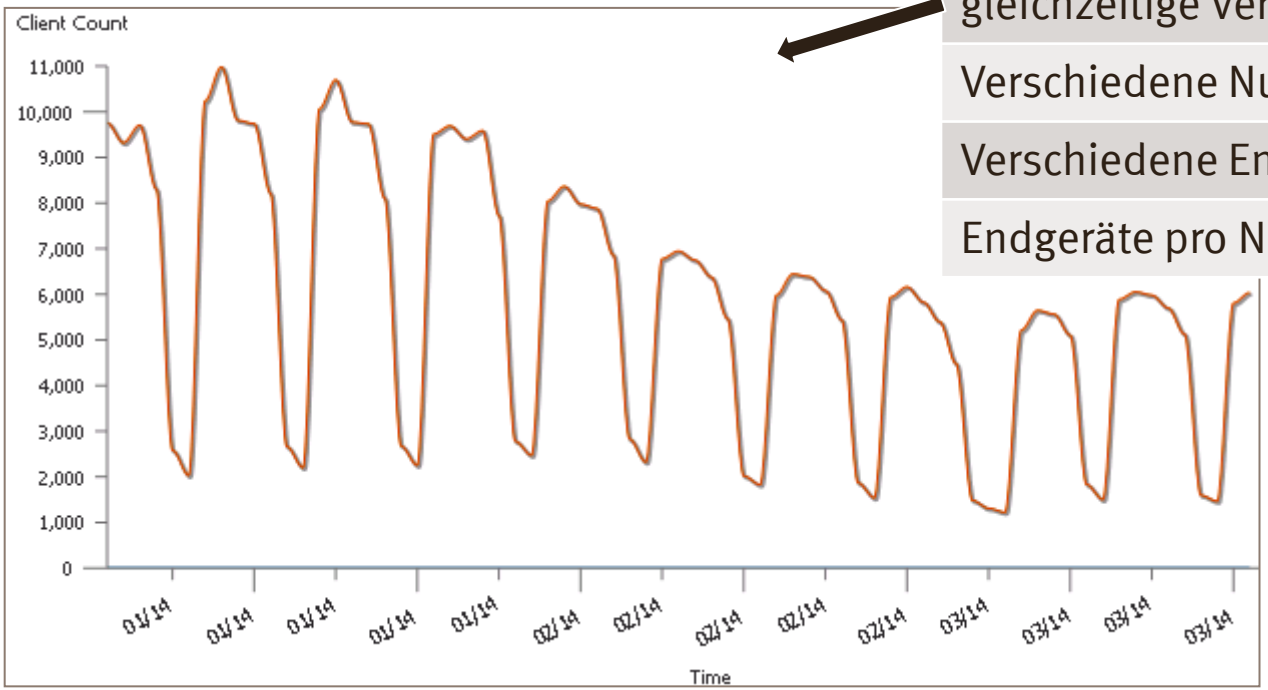
Altbekannter Werkzeugkasten	
Netzstrukturierung	Unterteilung in Netzbereiche
Firewall, Access Control Lists	Beschränkung der Kommunikation
IPS (Intrusion Prevention System)	Schutz gegen Hackerangriffe, Malware
VPN-Zugänge	gesicherter Netzzugang

Unabhängig von Endgeräten vorgenommenen oder organisatorischen Maßnahmen!

Netzstrukturierung

- Netzstrukturierung: wichtigste und schwierigste Maßnahme
- Strukturierungskriterien (Beispiele)
  - externer oder interner Nutzer
  - verwaltetes oder unbekanntes Endgerät
    - Netzzugang für unbekannte Endgeräte nur nach Authentifizierung
  - hoher Schutzbedarf (Personaldaten, Prüfungsergebnisse, Betriebsgeheimnisse)
  - Geräte ohne eigene Schutzfunktionen:
    - Gebäudeleittechnik, allg. Steuerungssysteme
    - **Demnächst Windows XP-Systeme!**

Herausforderung Mobility



WLAN-Kennzahl	Wert
gleichzeitige Verbindungen	bis zu 11.000
Verschiedene Nutzer	29.300
Verschiedene Endgeräte	46.200
Endgeräte pro Nutzer	1,6

Probleme /Herausforderungen im Bereich WLAN:

- keine Verwaltung der Endgeräte
- Einsatz von Privatgeräten (BYOD)
- Nutzung von externen Cloud-Services: Dropbox, …
- WLAN-Zugang für Gäste, Konferenzteilnehmer

Herausforderung Mobility - Maßnahmen

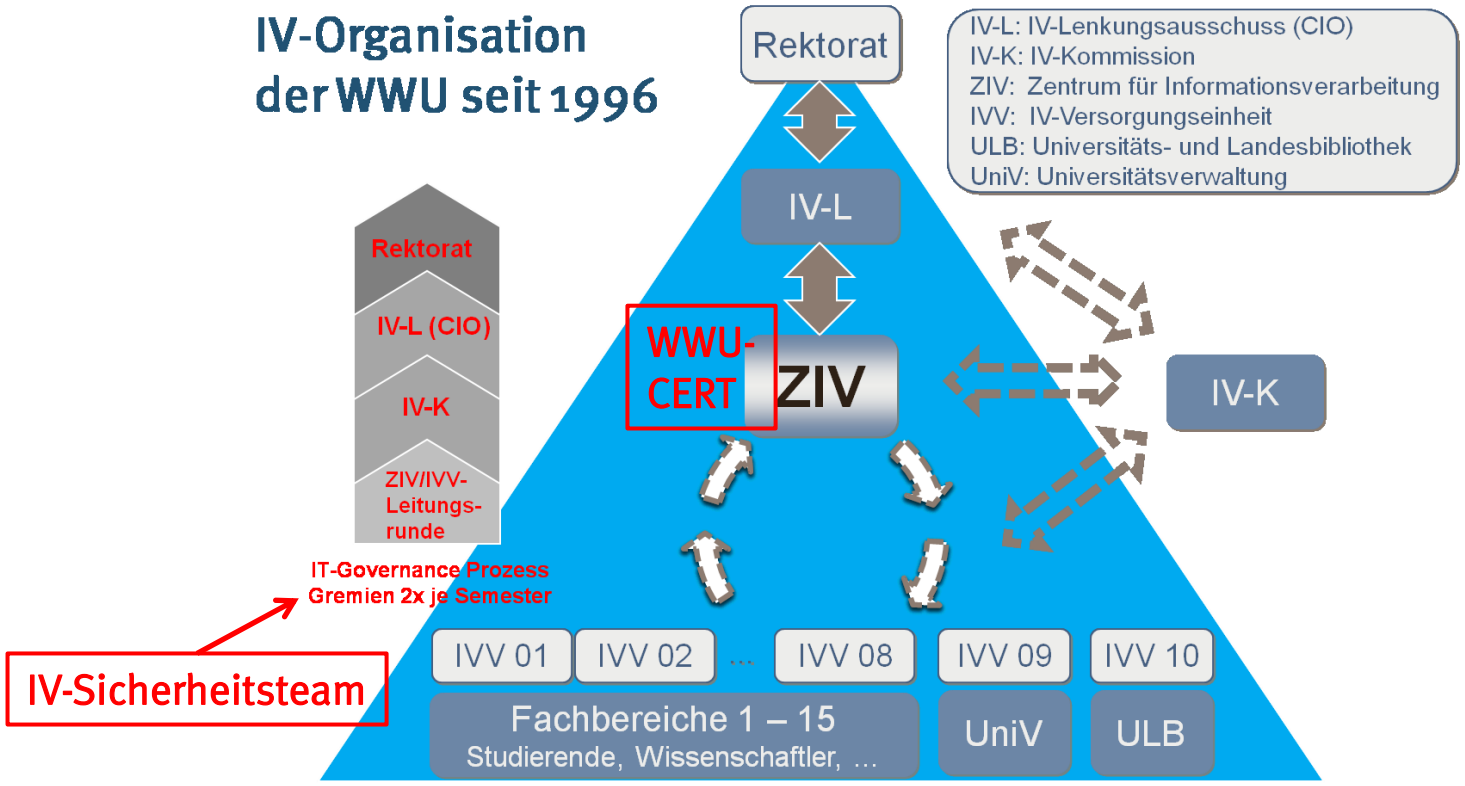
- mehrere SSIDs im WLAN (Netzstrukturierung!)
  - „eduroam“ für Gäste
  - „uni-ms“ und „wwu“ für interne Nutzer
- Netzzugang nur nach Authentifizierung
- Netztechnische Behandlung in jedem Fall wie Externe
  - da unbekanntes Endgerät
  - D.h. Durchlaufen von Sicherheitsfunktionen: IPS
- Cloud-Richtlinie für den Umgang mit Daten im Rahmen dienstlicher Tätigkeit
- Verabschiedung einer MDM-Policy in Vorbereitung
  - Rudimentäres MDM mit Microsoft Exchange; d.h. bei Active-Sync-Nutzung
    - Gerätesperre durch Kennwortschutz zwingend
    - Fernlösch-Funktion
- Projekt „Sync&Share NRW“ – Cloud-Speicher für Hochschulen
  - Daten verbleiben innerhalb der Hochschulen.

Organisatorische Maßnahmen

IV-Sicherheitsteam: Einbeziehung in den IT-Governanceprozess
Mitglieder aus den IVVen und dem ZIV
Ansprechpartner für alle sicherheitsrelevanten Fragen
Erarbeitung von umzusetzenden IT-Sicherheitsmaßnahmen
Durchführung von bereichsweisen IT-Sicherheitsüberprüfungen
Formulierung von Sicherheitsregelungen
Herausgabe des IV-Sicherheitshandbuchs

WWU-CERT: Computer Emergency Response Team im ZIV
Bearbeitung von Sicherheitsvorfällen
Ggf. Sperrung von Rechnern und Nutzerkennungen
Urheberrechtsverletzungen
Bearbeitung von staatsanwaltlichen und polizeilichen Anfragen

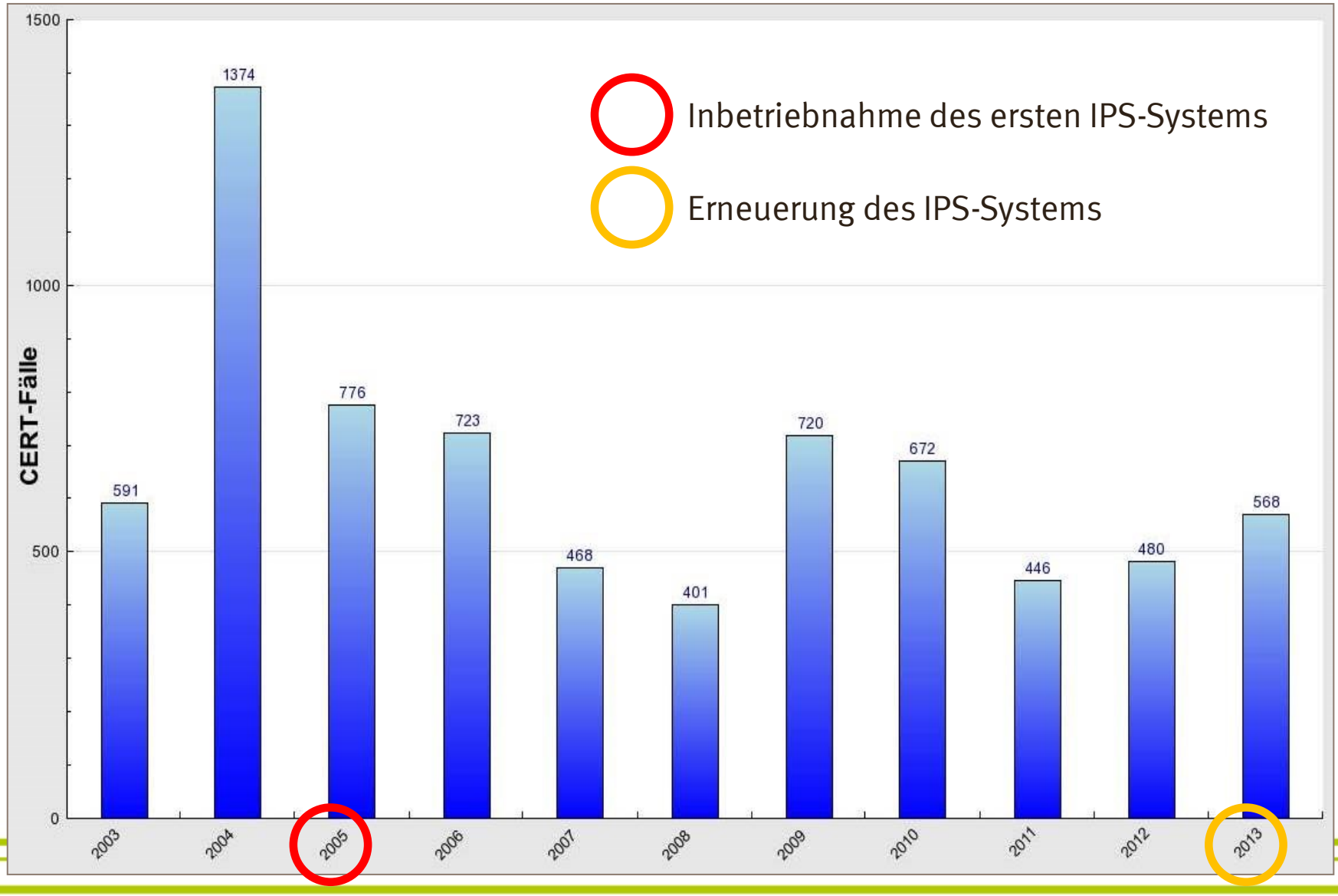
IV-Organisation: IV-Sicherheitsteam und WWU-CERT



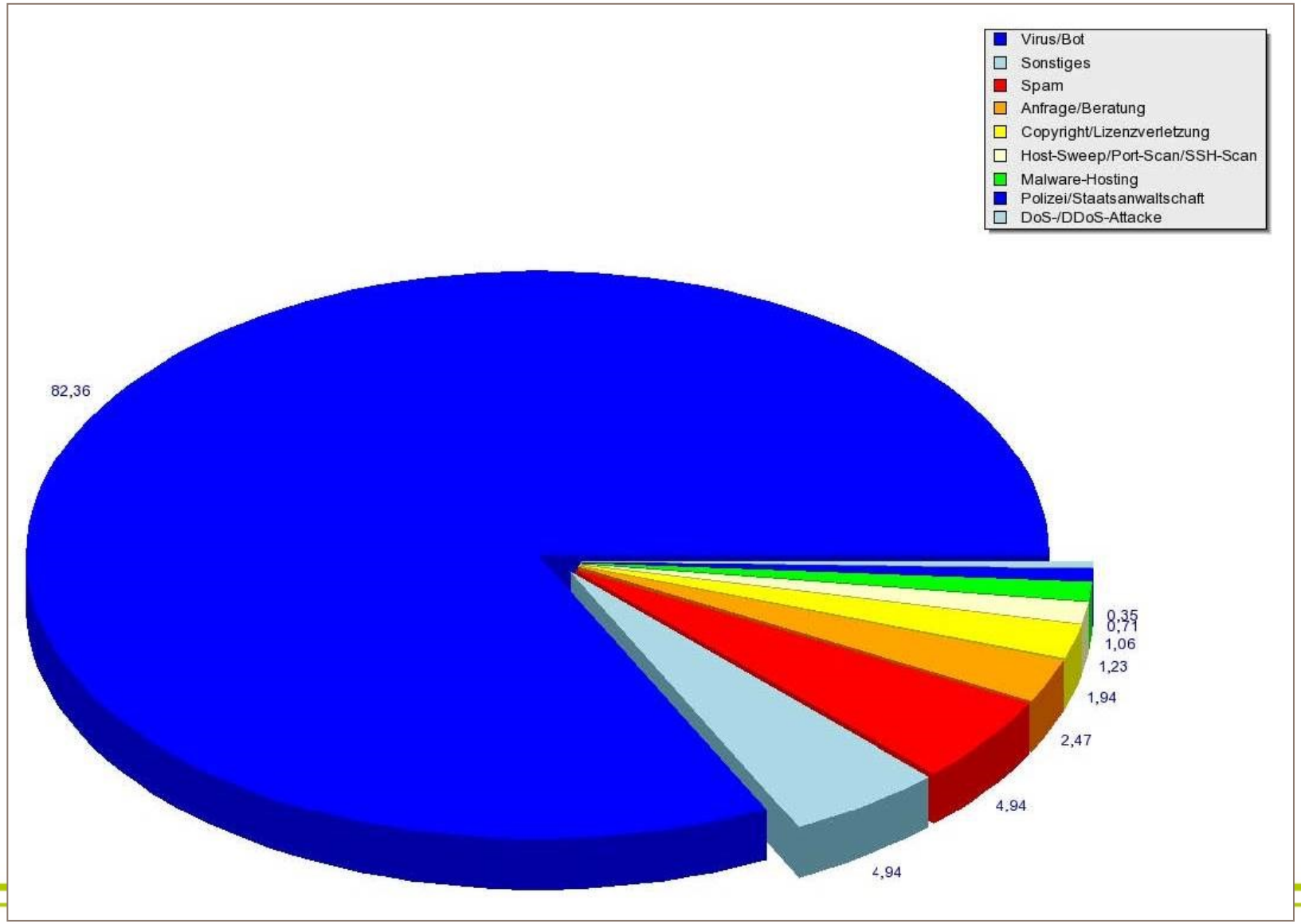
Gesamtdarstellung im IV-Sicherheitshandbuch

wissen.leben WWU Münster

CERT-Fälle pro Jahr



CERT-Fälle nach Typen 2013



Abschlussbemerkungen

- Was unterscheidet IT-Security von anderen IT-Themen?
  - IT-Security ist kein „Hype-Thema“ sondern eine „Daueraufgabe“!
  - IT-Security verursacht dauerhaft einen Sockel an laufenden Kosten / Aufwänden!
- Wirksame Strategie an einer großen Universität
  - Maßnahmen mit einer möglichst großen automatischen Flächenwirkung
    - Netzseitige Sicherheitsmaßnahmen
    - Einfache aber viele Geräte erfassende MDM-Policy
    - Schaffung von attraktiven Angeboten: Sync&Share NRW
- Fragen
  - Was sind aussagekräftige IT-Security-Kennzahlen (keine Selbsteinschätzungen)?
  - Wie sicher sind wir eigentlich?
  - Sind wir zumindest sicherer als vor einem Jahr?

Vielen Dank für Ihre Aufmerksamkeit!

Mitwirkende an der Vortragsvorbereitung

- Damian Bucher (E-Mail-Security)
- Thorsten Küfer (IV-Sicherheitsteam, CERT)
- Guido Wessendorf (Netzseitige Sicherheitsmaßnahmen)

Links

- IV-Sicherheitshandbuch:
  - http://www.uni-muenster.de/IV-Sicherheit/handbuch/
- Cloud-Richtlinie:
  - http://www.uni-muenster.de/imperia/md/content/ziv/pdf/cloud_richtlinie_wwu.pdf
- Online-Zeitschrift Z.I.V. 1/2013 mit Schwerpunktthema „IV-Sicherheit“:
  - http://www.uni-muenster.de/ZIV/Z.I.V.Ausgaben/Z.I.V.2013-01Sicherheit.pdf