IT-Sicherheit an Hochschulen - Wunschdenken oder Realität

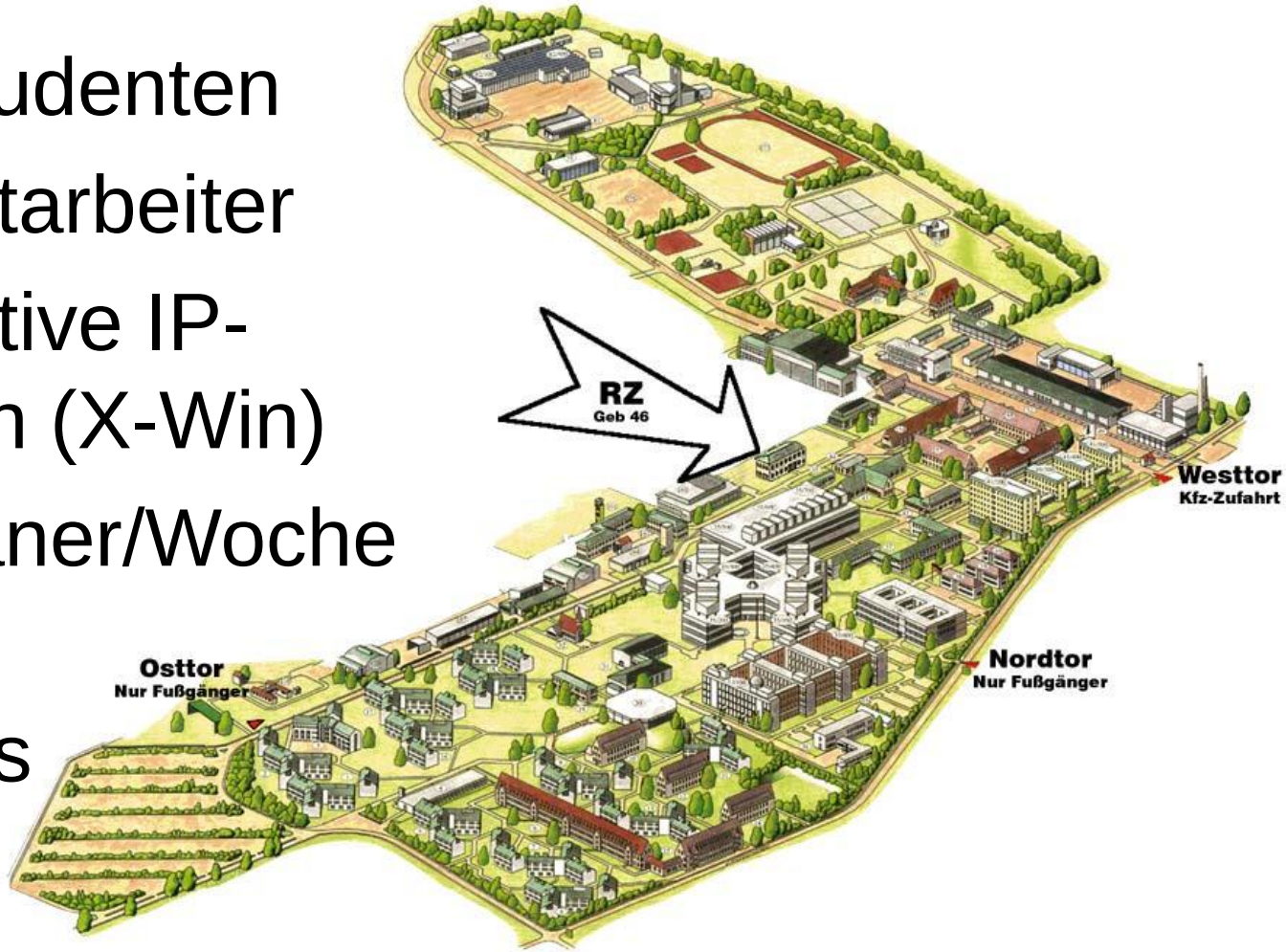
Prof. Stefan Schwarz, Universität der Bundeswehr München

ZKI-Frühjahrstagung
07.-09. März 2016

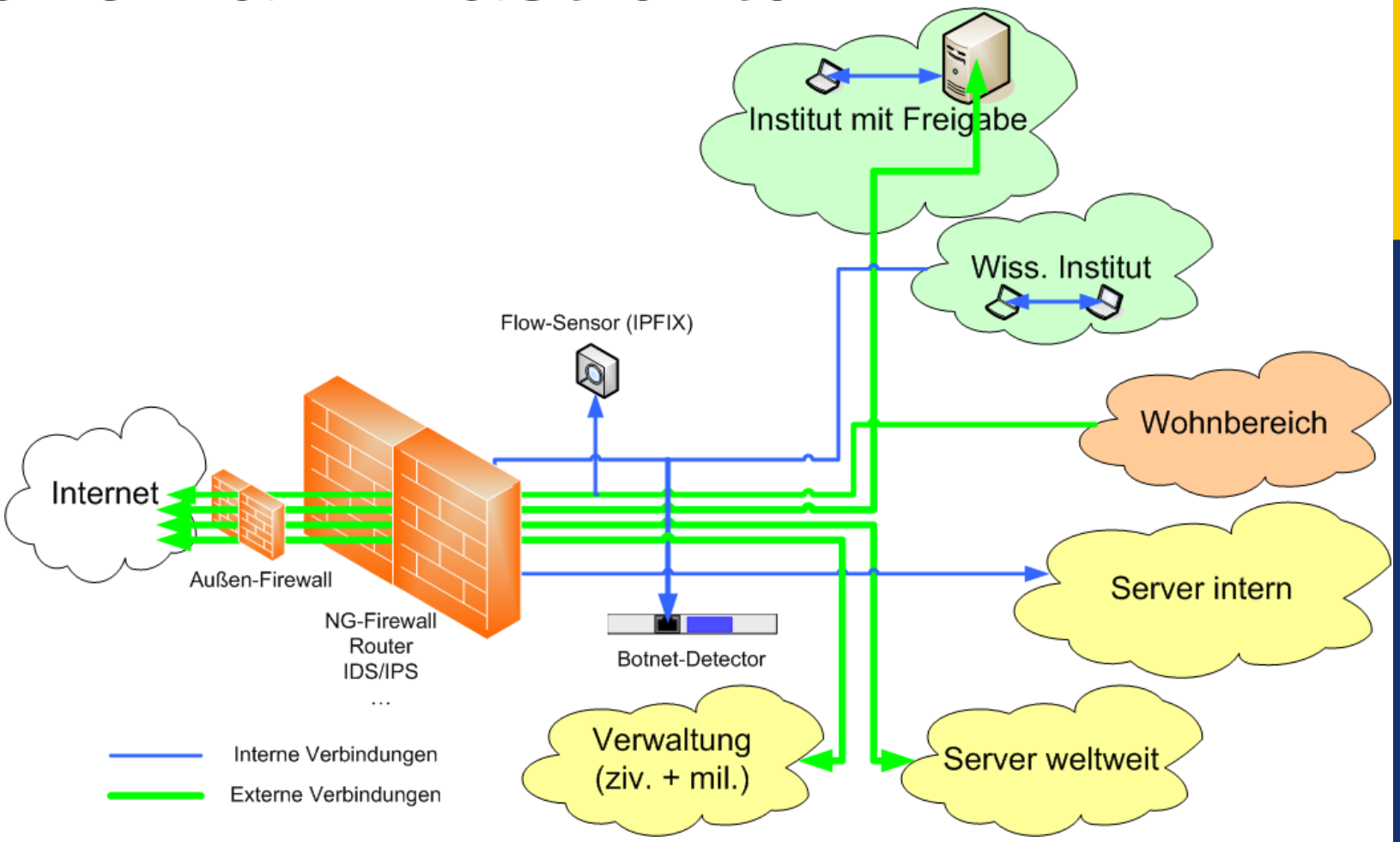
Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Ausgangslage

- Campus-Uni
- 3.000 Studenten
- 1.500 Mitarbeiter
- 9.000 aktive IP-Adressen (X-Win)
- 3-5 Trojaner/Woche
- X-Win
  3,5 Gbit/s



Schema Infrastruktur



Problematik IT-Sicherheit an Universitäten

- Alle nur denkbaren Programme und Protokolle im Netz inkl. Eigenentwicklungen
- Insbesondere Verbindungen in das Internet werden kaum blockiert
- Keine durchgängige zentrale Administration aller Arbeitsplätze (viele lokale Admins)
- Keine klaren Nutzungsszenarien
  Prinzipiell ist alles erlaubt bzw. begründbar
- Schutzbedarf der eigenen (Forschungs-)Daten noch wenig ausgeprägt.
- Zentrale Kontrollmechanismen eher unbeliebt

Bedrohungsszenarien

- DoS
  Bislang kaum beobachtet
- Abnehmende Bedeutung für klassischen Virenschutz
  - Abnehmende Erkennungsraten (80%)
  - Kein zeitnaher Schutz vor neuer Malware („Locky“)
- Flächendeckende und weltweite Zugänge
  - VPN und WLAN mit zentralen Zugangsdaten
  - Rogue WLAN-APs (Labor, Wohnbereiche)
- Mangelnder Pflegezustand von Systemen
  - Projektbezogene (Web-)Server
  - Virtuelle Webserver
  - Fehlende Zeit/Qualifikation der Admins/Studenten

Beobachte Angriffsszenarien

1. Malware-Download aus Internet
   Software aus nicht vertrauenswürdigen Quellen
2. E-Mail
   - Malware im Anhang (Rechnung.*, Mahnung.*,…)
   - (Spear-)Phishing
     auch schlecht gemachte Mails haben
     Erfolgsquoten von 1-2%
     Hohe Gefährdung durch „gut gemachten“ Angriff
   - Begünstigt durch Mobilgeräte
     Nur noch formatierte Ansichten und verschleierte Links
3. Angriffe auf Server zur Hinterlegung von Schadcode oder Abgreifen interner Informationen (XSS, SQLi)

Ziele der Angreifer

1. Abgreifen von Nutzeridentitäten
   Angreifer wird zum Innentäter

2. Akquise von Botnet-Clients
   Die eigentlichen Angriffsziele liegen außerhalb der HS

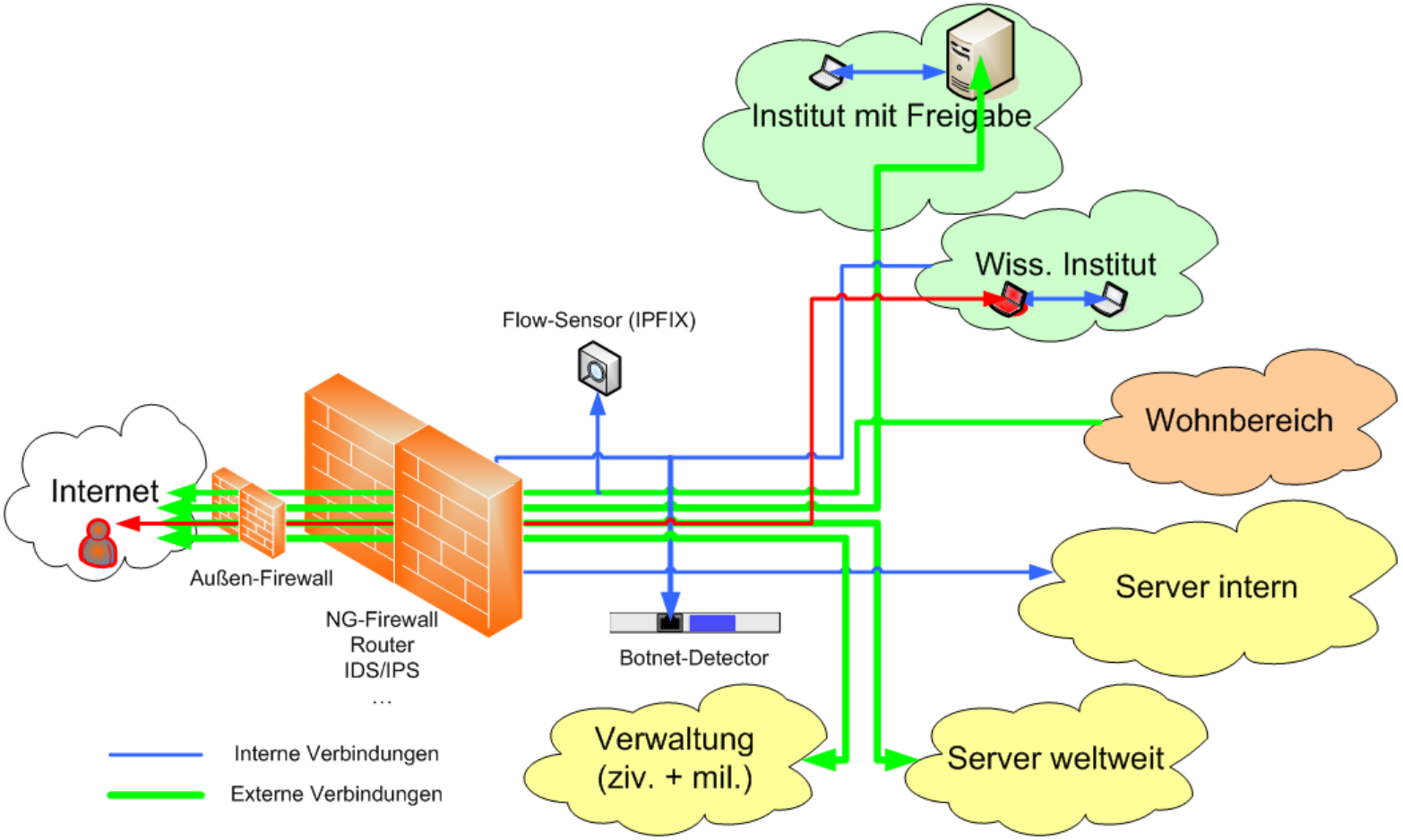
3. Abgreifen oder Manipulation von Daten

4. Überwachungs-/Spionagetools (RAT)

Inzwischen für fast alle Angriffsarten typisch:
Der eigentliche Angriff beginnt mit einer Infektion gefolgt von externer Kommunikation wie Nachladen von Schadcode (→Schwerpunkt auf Szenario „Innentäter“)

Szenario „Innentäter

Die klassische Firewall ist weitgehend wirkungslos



Maßnahmen

1. Organisation
   Ziel: Verankerung der IT-Sicherheit in Hochschule
   - Unterstützung der Hochschulleitung
   - Festlegung der erforderlichen Rollen
   - Begleitende Awareness-Maßnahmen
   - Regularien für alle Beteiligten (auch Datenschutz)
2. Technik
   Ziel: Verhinderung bzw. Erkennung von Infektionen
   - Filtermechanismen bis zum Endgerät
   - Etablierung von Überwachungsmaßnahmen
   - Detektion von auffälligen Verhaltensmustern
3. Beratung und Kontrolle
   - Unterstützung der Betroffenen im Schadensfall
   - Kontrolle der Wirksamkeit von Maßnahmen

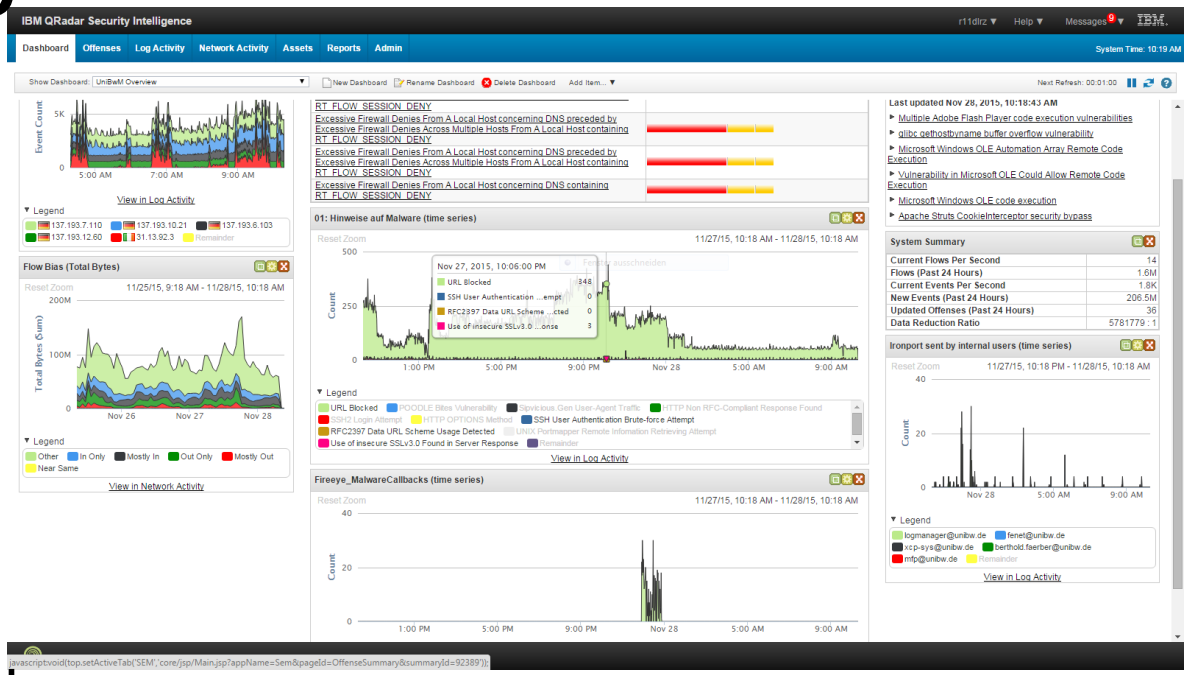
Technische Maßnahmen

1. Logmanagement
   - Vielzahl beteiligter Systeme erfordert zwingend ein zentrales Logmanagement
2. Regelmäßige Überprüfung sensibler Systeme
   - Definition „sensible Systeme“
     Extern erreichbare Server, Server mit DFN-PKI-Zertifikat, …
   - (Gezielte) Schwachstellenscans
3. Next-Generation-Firewalling
   - Zusammenfassung verschiedener Technologien
   - Zentrale Stelle zur Überwachung und Filterung
4. Dedizierte Systeme zur Malwareerkennung
   - Erkennung jenseits von Punkten 1.-3.

3 Grundregeln beachten

1. Blockieren von Malwaretraffic beseitigt nicht die Ursache
   - Information für Betroffene bereit stellen
   - Beratungsleistungen einplanen
   - Durchführung der Maßnahmen überwachen
2. Vermeidung von False Positives
   - FPs kosten viel Zeit
   - FPs kosten langfristig aufgebaute Reputation
   - Beurteilung erfordert Erfahrung
3. IT-Sicherheit bindet Personal
   - Personal ist auch durch Technik nicht zu ersetzen
   - Personal benötigt Zeit/Mittel für Weiterbildung

Logmanagement

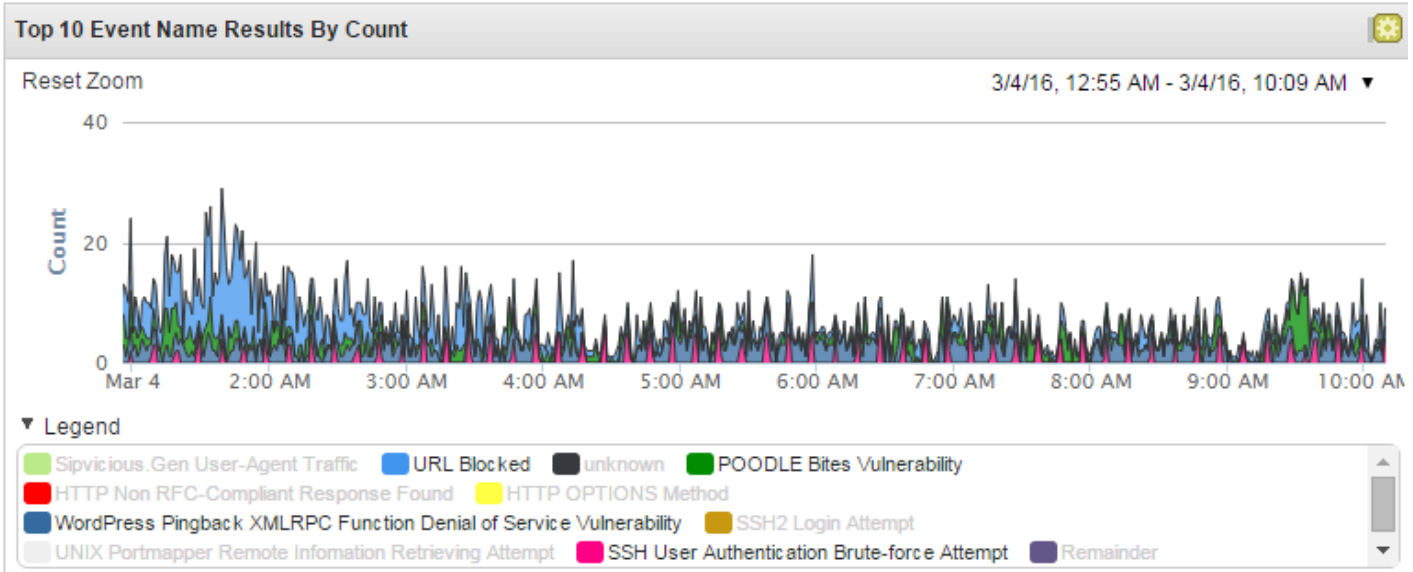


- IBM QRadar
- Kosten: 15T€/Jahr
- Betriebsaufwand: 0,25 VZÄ
- Regelbasiertes SIEM-Tool
- Schnittstelle zum Ticketsystem für Vorfallsbearbeitung
- Ermittlung von Nutzern zur IP
- Datenschutz beachten (Regelungen zu Vorratsdaten!)

Überprüfung sensibler Systeme

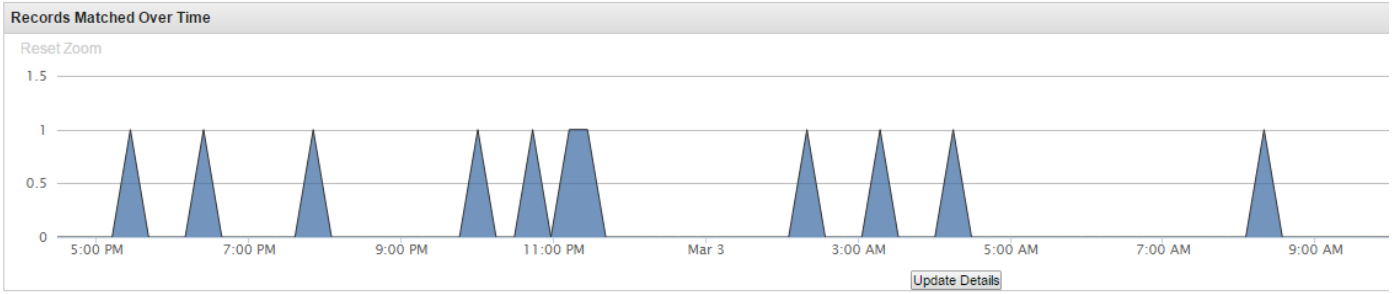
- OpenVAS/Greenbone
- Kosten: 5T€/Jahr
- Betriebsaufwand: 0,25 VZÄ
- Automatisierte Aufgaben
- Anbindung an Logmanagement→Vorfallsgenerierung
- Definition der Scankonfiguration ggf. aufwändig
- Siehe auch ZKI AK SMS

Next-Generation Firewall



- PaloAlto
- Kosten: 200T€/Jahr
- Betriebsaufwand: 1 VZÄ
- Detaillierte Einblicke in alle Protokollebenen
- Wirksame (URL-)Filter zur Verhinderung von Infektionen
- Aufbau von Applikations-Policies wo möglich
- Anbindung an Logmanagement→Vorfallsgenerierung

Malwareerkennung



	Event Name	Eve Cou	Start Time	Low Level Category	Source IP	Destination IP	
	malware-callback	1	Mar 3, 2016, 8:27:55 AM	Virus Detected	137.193.	184.168.147.153	80
	malware-callback	1	Mar 3, 2016, 4:27:56 AM	Virus Detected	137.193.	184.168.147.153	80
	malware-callback	1	Mar 3, 2016, 3:26:15 AM	Virus Detected	137.193.	184.168.147.153	80
	malware-callback	1	Mar 3, 2016, 2:27:55 AM	Virus Detected	137.193.	184.168.147.153	80
	malware-callback	1	Mar 2, 2016, 11:31:57 PM	Virus Detected	137.193.	92.243.68.138	80
	malware-callback	1	Mar 2, 2016, 11:23:50 PM	Virus Detected	137.193.	92.243.68.138	80
	malware-callback	1	Mar 2, 2016, 10:49:27 PM	Virus Detected	137.193.	92.243.68.138	80
	malware-object	1	Mar 2, 2016, 10:12:41 PM	Misc Malware	137.193.	104.25.127.10	0
	Information - Event CRE	1	Mar 2, 2016, 8:01:12 PM	Misc Malware	137.193.	192.230.80.145	0
	malware-callback	1	Mar 2, 2016, 6:34:46 PM	Virus Detected	137.193.	184.168.147.153	80
	malware-callback	1	Mar 2, 2016, 5:35:49 PM	Virus Detected	137.193.	184.168.147.153	80

- FireEye
- Kosten: 80T€/Jahr
- Betriebsaufwand: 0,5 VZÄ
- Erkennung von infektiösem Inhalt und Callbacks nach Infektion sowie deren Zusammenwirken
- Nutzt Sandboxing in verschiedenen Instanzen
- Anbindung an Logmanagement→Vorfallsgenerierung
- Hoher Grad an zuverlässiger Erkennung

Praxisbeispiel „Infektion“

Historie eines Vorfalls in besonders sensiblem Bereich

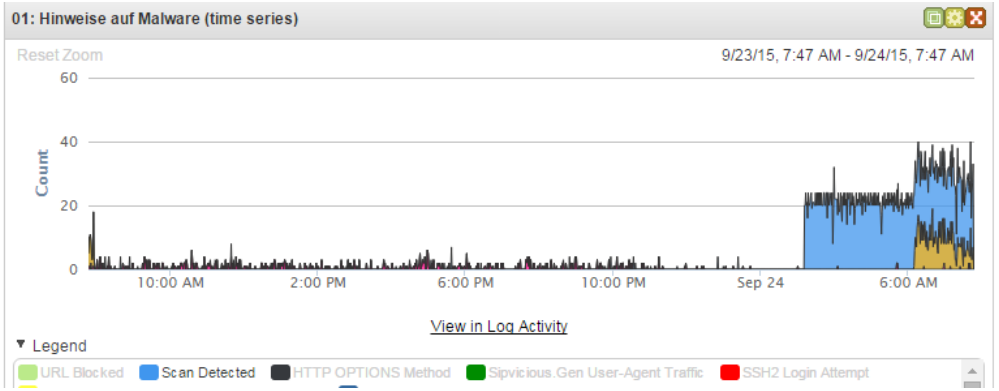
- 18:08: FireEye meldet „Malware Callback“
  `Host=blame-sleep-chart.com;name=Trojan.Matsnu`
- +1 08:16: initiierter Sophos-Scan findet Verdächtiges
  `AppData\Local\Temp\B771.tmp.exe" gehört zu Virus/Spyware 'Mal/Generic-S +weitere 3 Dateien`
- +1 11:09: Nutzer meldet sich, da er am Vortag gegen 18 Uhr eine Mail zu „Mahnung“ erhalten und den Anhang
  `„Forderung 01.11.2015-Stellvertretender Rechtsanwalt Online24 Pay GmbH.zip“` geöffnet hat
- +1 bis 15:15 Abschließende Maßnahmen Bereinigung + Neue Zugangsdaten

Praxisbeispiel „Hola-Software“

Identifikation der Software Hola (https://hola.org)

- Freie „VPN“-Software
- Umgehen von Geo-Sperren
- Freigabe des eigenen Rechners als VPN-Endpunkt
- Freigabe des eigenen Rechners für Fremdnutzung

- Erkennung durch Auffälligkeiten eines (evtl. ungeschickt konfigurierten) Systems im Logmanagement
- Identifikation und erweiterte Erkennung durch PaloAlto



Log Source (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Start Time (Maximum)	Low Level Category (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	PA_Application (custom) (Unique Count)	Count
PaSeries @ paola1.rz.unibw-muenchen.de	301	Jan 22, 2016, 10:13:20 AM	Jan 22, 2016, 4:09:40 PM	Firewall Permit	Multiple (301)	Multiple (109)	Multiple (3)	hola-unblocker	301
PaSeries @ paola1.rz.unibw-muenchen.de	18	Jan 22, 2016, 1:45:10 PM	Jan 22, 2016, 4:04:48 PM	Firewall Permit	Multiple (18)	Multiple (3)	Multiple (2)	hola-unblocker	18
PaSeries @ paola1.rz.unibw-muenchen.de	2	Jan 22, 2016, 11:06:46 AM	Jan 22, 2016, 2:52:32 PM	Firewall Permit	Multiple (2)	Multiple (2)	Multiple (2)	hola-unblocker	2
PaSeries @ paola1.rz.unibw-muenchen.de	2	Jan 22, 2016, 3:58:34 PM	Jan 22, 2016, 3:58:44 PM	Firewall Permit	Multiple (2)	Multiple (2)	6861	hola-unblocker	2

Erfahrungen UniBw München

1. Konsequente Verfolgung von Malwarevorfällen reduziert weitere Vorkommnisse (und damit Aufwand) deutlich.

2. Auch nur kurzzeitige Zugangssperren von (wenigen) Wiederholungstätern wirkt besser als jede Sensibilisierungsmaßnahme (Multiplikatoreffekt).

3. Zentral administrierte Systeme sind deutlich weniger anfällig als dezentral administrierte Systeme (nahezu keine Vorfälle in diesem sensiblen Bereich).

4. IT-Sicherheit ist ein Argument in Verhandlungen zum Haushalt.

Künftige Herausforderungen

1. Permanente Anpassung der Sicherheitsmaßnahmen

2. Intensive Beobachtung und Evaluation eines hochdynamischen Marktes, leider teilweise bestimmt durch leere Versprechungen

3. Enge Einbindung des Datenschutzes zu Themen wie Vorratsdatenspeicherung

4. Notwendigkeit des zumindest teilweisen Aufbrechens von Verschlüsselungen (SSL-Decryption) bei zunehmender Nutzung von verschlüsselten Verbindungen durch Malware

Fazit

1. IT-Sicherheit an Hochschulen ist in wohl definiertem Umfang durchaus erreichbar
2. IT-Sicherheit erfordert den Einsatz von personellen und materiellen Ressourcen
3. IT-Sicherheit ist allein mit organisatorischen Regelungen nicht ausreichend erreichbar
4. IT-Sicherheit kann nicht allein mit klassischen Bordmitteln erreicht werden, vor allem nicht bei endlichen personellen Ressourcen
5. IT-Sicherheit ist ein permanenter Prozess auf organisatorischer, vor allem aber auch auf technischer Ebene (Evaluation)
6. IT-Sicherheit wird durch gemeinsamen Informationsaustausch gefördert (→ ZKI AK SMS)

Weitere Fragen

Kontakt Stefan.Schwarz@unibw.de

xmpp:stsc@dfncis.de

Dieser Vortrag