FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT-Sicherheit

Next Generation Firewall / Intrusion Prevention System

B.Sc. Benedikt Paffen

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Inhaltsverzeichnis

Was sind die neuen Trends / Gefahren der IT-Sicherheit?

- Gefahren sind nicht mehr klar sichtbar
- Anzahl der mobilen Arbeiter steigt
- Defense in Depth
- BYOD
- Verschlüsselungen werden beliebter
- Verbreitung von Malware immer schwerer zu entdecken

Was sind Legacy-Firewalls*

- Filtern Verkehr basierend auf Ports (Layer 4)
- Speichern Verbindungen und ordnen sie zu (stateful inspection)
- N(etwork) A(ddress) T(ranslation)
- Grundlegende Inspection von Programmbefehlen
- Erlauben die Anbindung via VPN

*Herstellerlösungen

Vergleich Legacy Firewall zu NGFW

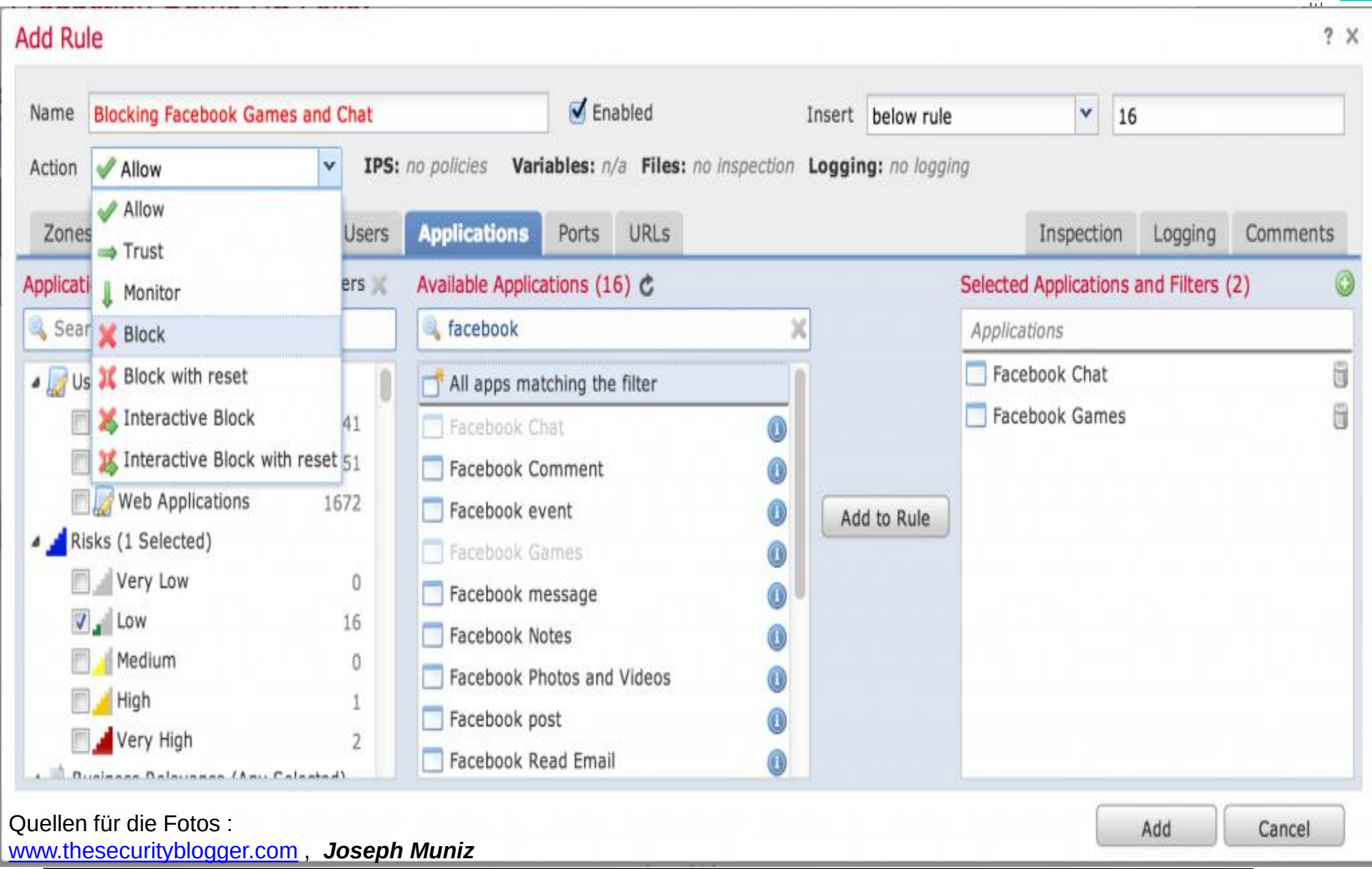
Legacy:

1. Einblick in Verbindungen nicht möglich
2. Keine Erfassung von Kontexten
3. Erkennen keine Malware im Verkehr
4. Zusammenarbeit ist limitiert
5. Keine All-in-One Lösung

NGFW:

1. Eine Mischung zwischen Firewall, IPS und Proxy
2. Kontextsensitive Firewalls
3. Benutzerzuordnung
4. Malware im Verkehr erkennen und unterbinden

Vergleich Inspection Legacy <-> NG



Quellen für die Fotos :
www.thesecurityblogger.com , ***Joseph Muniz***

Was können NG-Devices (noch) ?

- Schnell
- Selbstlernend
- Erkennen Benutzer, Anwendungen, Verkehr etc.
- Können verschlüsselten Verkehr entschlüsseln
- Zusammenarbeit mit anderen Geräten
- Zero-Day-Schutz durch „Call-Home“
- Weitere Features können einfach hinzugekauft werden

Infrastruktur für NG-Devices

- Legacy-Devices meist nur einmal konfiguriert
- Sie waren als Stand-Alone gedacht

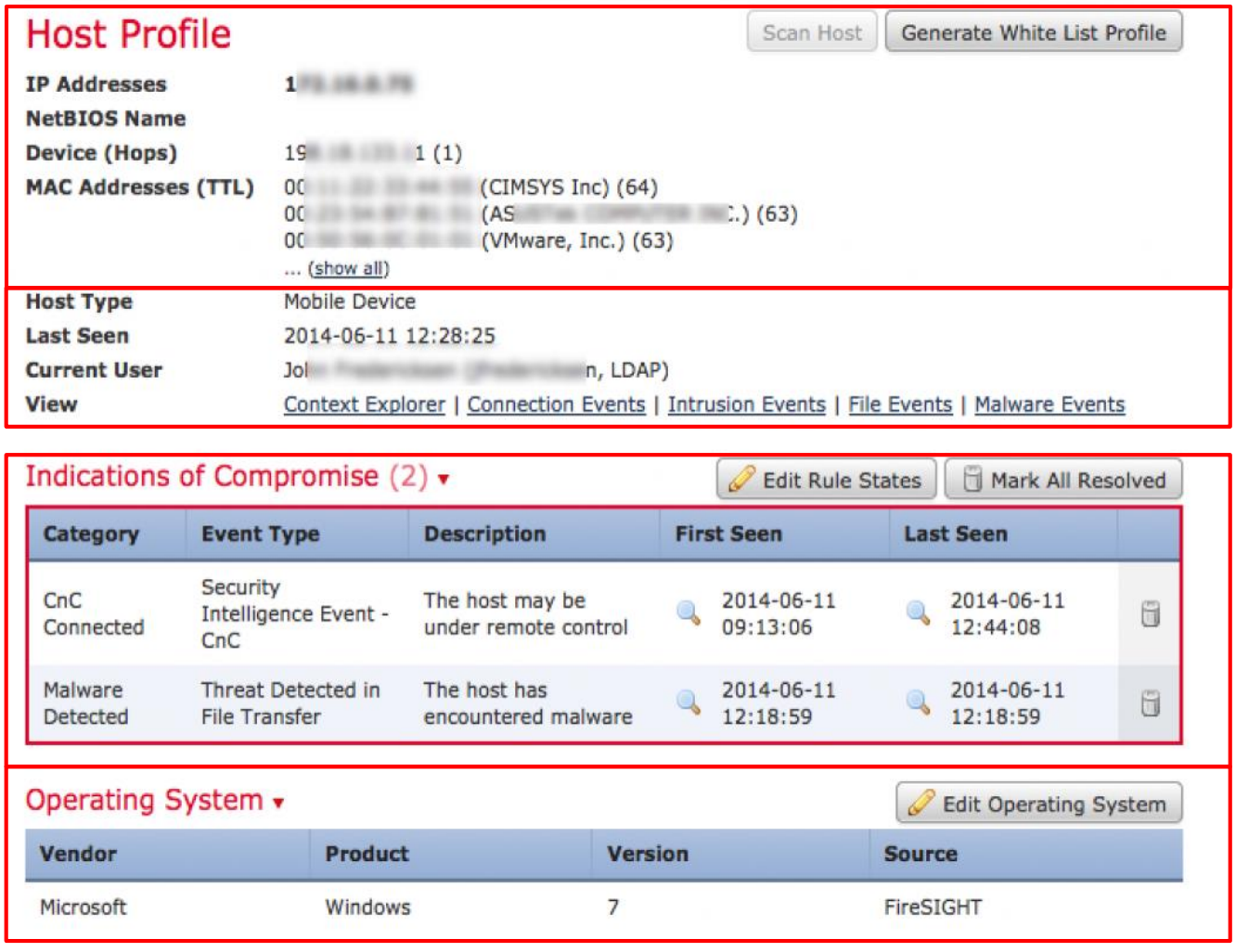
- NG-Devices sind das komplette Gegenteil
- Sie erfordern eine Anbindung an:
  - Identity-Management
  - Zentralisierte Management-Appliances
  - Internet

Forensische Möglichkeiten

- Tiefer Einblick in Verbindung erlaubt mehr Daten
  - NetFlow
  - Monitoringports
  - PCAP
- Zuordnung von Verkehr und Benutzern
- Korrelation mit anderen Geräten
- Zentrales Management erlaubt Nachverfolgung von Vorfällen

Weg einer Infektion

Genaue Informationen



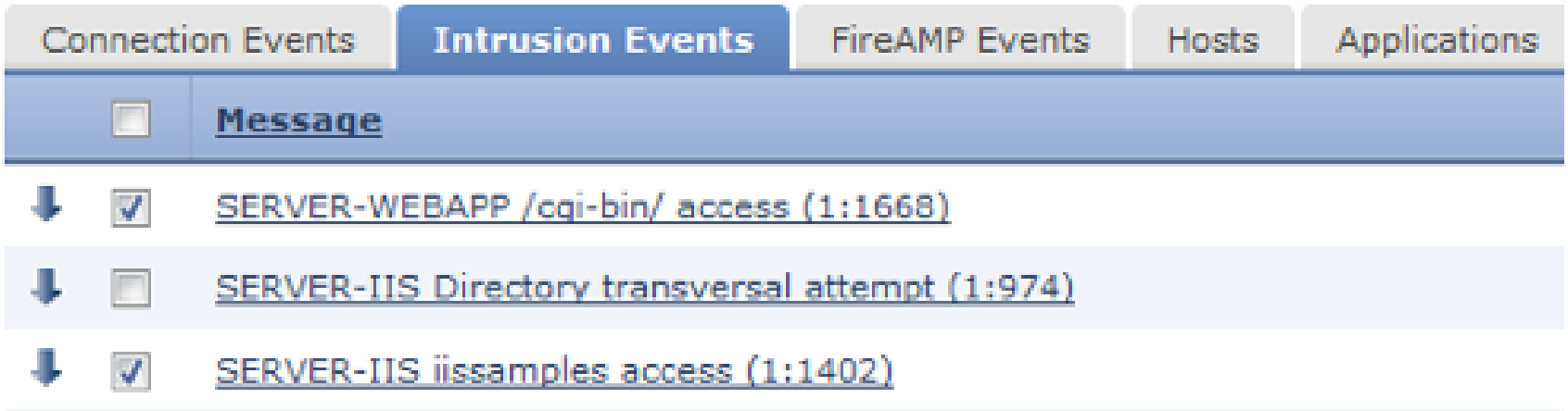
Allgemeine Informationen zum Hostcomputer

Informationen aus dem Identity-MGNT & NMAP

Informationen über die gefundene Malware

Durch die NG-Devices gelernte Infos über das Gerät

Export


Connection Events
Intrusion Events
FireAMP Events
Hosts
Applications
Message
SERVER-WEBAPP /cgi-bin/ access (1:1668)
SERVER-IIS Directory transversal attempt (1:974)
SERVER-IIS iissamples access (1:1402)

Gefahren durch NG-Devices?

- Laut Hersteller zwar „gehärtete Appliance“…….

  ……. Aber meist Hardware mit Standard-Linux
- Codeartefakte der Vorgänger
- Kommunikation zwischen und mit den Systemen
  - Webrequests ☹
  - Eventl. Verwendung von Telnet zur Kommunikation☹ ☹
  - SNMP v2 ist noch Standard ☹ ☹ ☹
  - SSL-Vpn (WEBVPN) -> benötigt WebServer auf der Firewall ☹x4
- Umgang mit Malware
- Analyse erfordert Umgang und „anfassen“
- Inspektion erfordert auch Umgang => oft DOS

Fazit

- NG-Devices gehört die Zukunft
- Sie sind jedoch aufwändig zu
  - Planen
  - Implementieren
  - Betreiben
- Benötigen eine funktionierende Infrastruktur im „Rücken“
- Durchaus auch angreifbar
- Teuer (im Moment)

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?