

IT-Sicherheit

Next Generation Firewall / Intrusion Prevention System

B.Sc. Benedikt Paffen

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik



1. Einführung
2. Was sind Firewalls
3. Vergleich Legacy <-> NGFW
4. Was können NG-Devices
5. Infrastruktur
6. Forensik
7. Gefahren

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

- 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

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

Add Rule

Name **Blocking Facebook Games and Chat** Enabled Insert **below rule** 16

Action **Allow** **IPS: no policies Variables: n/a Files: no inspection Logging: no logging**

Zones Users **Applications** Ports URLs Inspection Logging Comments

Available Applications (16)

Search: facebook

- All apps matching the filter
- Facebook Chat
- Facebook Comment
- Facebook event
- Facebook Games
- Facebook message
- Facebook Notes
- Facebook Photos and Videos
- Facebook post
- Facebook Read Email

Selected Applications and Filters (2)

- Facebook Chat
- Facebook Games

Add to Rule

Add Cancel

Quellen für die Fotos :

www.thesecurityblogger.com , **Joseph Muniz**

- 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

- 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

- 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



Host Profile

Scan Host Generate White List Profile

IP Addresses 172.16.0.79

NetBIOS Name

Device (Hops) 19 (1)

MAC Addresses (TTL)

- 00:0C:29:3E:4E:00 (CIMSYS Inc) (64)
- 00:0C:29:3E:4E:00 (AS) (63)
- 00:0C:29:3E:4E:00 (VMware, Inc.) (63)
- ... (show all)

Host Type Mobile Device

Last Seen 2014-06-11 12:28:25

Current User Job: Frederic (Frederic, LDAP)

View [Context Explorer](#) | [Connection Events](#) | [Intrusion Events](#) | [File Events](#) | [Malware Events](#)

Allgemeine Informationen zum Hostcomputer

Indications of Compromise (2) ▾

Edit Rule States Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2014-06-11 09:13:06	2014-06-11 12:44:08
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	2014-06-11 12:18:59	2014-06-11 12:18:59

Informationen aus dem Identity-MGNT & NMAP

Operating System ▾

Edit Operating System

Vendor	Product	Version	Source
Microsoft	Windows	7	FireSIGHT

Informationen über die gefundene Malware

Servers (1) ▾

IP Address	Host Name	OS	Vendor	Product	Version	Source
172.16.0.79

Durch die NG-Devices gelernte Infos über das Gerät

Connection Events	Intrusion Events	FireAMP Events	Hosts	Applications
<input type="checkbox"/>	Message			
↓	<input checked="" type="checkbox"/>	<u>SERVER-WEBAPP /cgi-bin/ access (1:1668)</u>		
↓	<input type="checkbox"/>	<u>SERVER-IIS Directory transversal attempt (1:974)</u>		
↓	<input checked="" type="checkbox"/>	<u>SERVER-IIS iissamples access (1:1402)</u>		

- 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

- 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?