

Get Secured.

DATAGROUP Hausmesse in Bremen

Matthias Jessen
Territory Sales Manager

WatchGuard XTM 11.4 und XCS



Security Vorhersagen für 2011

- Cyberwar
- Advanced Persistent Threat “APT”
- VoIP
- Netzwerk weitet sich aus
- Fahrzeuge als Zielscheibe
- Facebook
- Eingebaute Malware
- Datenverlust
- Erkennung vs. Verhinderung
- Malware as a Service

Cyberwar

- Bereits 2010 haben wir vor Cyberwar gewarnt
- Unternehmen sind schon länger Zielscheibe gezielter Angriffe
- Staatliche Organe oder Unternehmen treten in den Fokus
- Was ist der Unterschied zu dem was wir kennen?
 - Größere Teams
 - Mehr Spezialisten
 - Staatliche Organe im Hintergrund
 - Methoden werden komplexer



Advanced Persistent Threat ,APT‘

- Keine einheitliche Definition
- Drei Themen übereinstimmend
 - Neue Angriffsmuster und Technologien werden über APT in den Markt eingeführt
 - Unbemerkt auch über einen längeren Zeitraum im Netzwerk
 - Gezielter Schaden
- Erst Denken dann Handeln



Voice over IP

- VoIP ist starker Wachstumsmarkt
- Technologien weit verbreitet
- Baukasten für Angriffswerkzeuge wächst schneller



Netzwerk weitet sich aus

- Perimeter Security weniger stark im Fokus
- Unternehmen sichern einzelne Bereiche besonders ab
 - Abteilungen
 - Funktionale Bereiche
- Mobiles Arbeiten mit 50% Wachstum pro Jahr



Fahrzeuge als Zielscheibe

- Hacker suchen sich immer Bereiche die möglicherweise weniger geschützt sind
- Mehr IP in neuen Fahrzeugen
 - Bluetooth
 - UMTS
 - Onboard Computer
 - Mehr Schnittstellen



Eingebaute Malware

- Mehr und unterschiedlichere Geräte mit Netzwerkanbindung oder anderen Schnittstellen
 - Bilderrahmen
 - Fahrzeuge
 - Kühlschrank
 - TV
- Zufällige oder absichtliche Implementierung?



Datenverlust

- Wandel zur Dienstleistungsgesellschaft
- Mehr Unternehmen stellen „Wissen“ her anstelle von physikalischen Produkten
- Unternehmen und Staaten müssen Wege finden dieses Wissen zu schützen
- Kundendaten sind überall und fast immer einfach zu erhalten



Erkennung vs. Verhinderung

- Fast alle Unternehmen konzentrieren sich auf das Erkennen von Malware oder Eindringlingen
- Wege ins Unternehmen oder an Daten werden vielfältiger
- Anwendungen werden komplexer
- Gesamtes Netzwerk muss ständig beobachtet werden
 - Logging und Reporting muss vorhanden sein und optimiert werden
- Verbindungen zwischen Angriffswegen müssen identifiziert werden



Malware as a Service

- Software, Anwendungen und Medien sind immer und überall verfügbar
- Sofortige Verfügbarkeit verlockend
- Verbreitung von Malware sehr einfach
- Baukästen für Malware nehmen zu
- Es wird einfacher Anwendungen mit weniger Nutzen als schadhaften Inhalten zu erstellen



Schlussfolgerung

- Firewall war gestern
- Flexible Technologien sind notwendig
- Integration von Top Technologien
- Extensible Threat Management
 - XTM Definition von IDC in 2008
- Ausweitung von IT Sicherheit in alle Unternehmensbereiche
- Schnelle Reaktion auf Bedrohung ist wichtiger denn je
- Gesellschaftliche Veränderung im Unternehmen zulassen
- Gesamtes Netzwerk muss überwacht werden
- Datenverlust verhindern
- Kontrolle vs. Vertrauen

Lösungen von WatchGuard



Lösungen von WatchGuard



XTM



XCS



SSL




Extensible Threat Management

- Betriebssystem Fireware XTM
 - Proxy Technology seit mehr als 14 Jahren
 - Netzwerkfunktionen implementiert
- Gateway AV
 - Kooperationspartner AVG
- Intrusion Prevention
 - Kooperationspartner Broadweb
- WebBlocker
 - Kooperationspartner Websense
- spamBlocker
 - Kooperationspartner commtouch



Extensible Threat Management

- Reputation Enabled Defense RED
 - URL basierte Reputation
 - Beschleunigt den Datenverkehr
 - Erhöht die Sicherheit

Reputation		Action
Bad		Blocked No Anti-Virus Scan
Unknown		Anti-Virus Scan
Good		Bypass Scanning Performance Gain

Extensible Threat Management

- Application Control
 - Kooperation mit Broadweb
 - 1500 Anwendungen
 - 2500 Signanturen

 - Web 2.0 : Facebook, Twitter
 - P2P : Gnutella
 - VoIP : skype
 - Streaming : YouTube
 - IM : MSN, ICQ
 - RA : TeamViewer



SocNet Apps und APIs

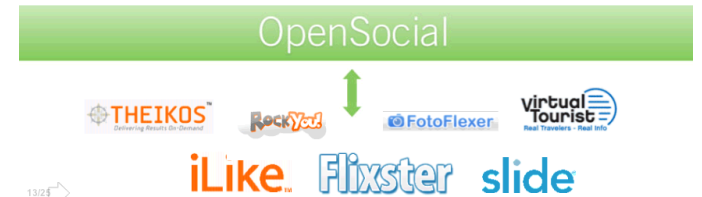
OpenSocial



Facebook Apps



Twitter API



• Facebook – Facts Germany

Allgemein:

- Über 500 Millionen aktive Nutzer
- Über 15 Millionen aktive Nutzer in Deutschland
- 50% der aktiven Nutzer besuchen Facebook täglich
- 1 Nutzer hat 130 Freunde im Durchschnitt
- Nutzer verbringen 700 Milliarden Minuten pro Monat auf Facebook
- Über 3 Milliarden Photos werden monatlich hochgeladen
- Über 5 Milliarden Inhalte werden wöchentlich geshard (Links, News, Blogs, Notes, Photo Alben etc.)



• Facebook – Facts Germany

Aktivitäten auf Facebook

- Es existieren 900 Millionen Objekte (Pages, Gruppen, Events und Community Pages) auf Facebook
- Der durchschnittliche Nutzer ist mit 80 Pages, Gruppen und Events verbunden
- Jeder Nutzer erstellt 90 Inhalte pro Monate
- Über 30 Milliarden Inhalte (Links, News, Blog posts, Notes, Photos usw.) werden jeden Monat geshared

• Facebook – Facts Germany

Plattform Statistiken

- Es existieren über 1 Million Entwickler in über 180 Ländern
- Über 70% der User nutzen Plattform Applikationen jeden Monat
- Es gibt über 550.000 aktive Applikationen
- Über 1 Millionen Webseiten haben Facebook Funktionen integriert
- Über 150 Millionen Menschen interagieren mit Facebook auf externen Webseiten jeden Monat

• FaceBook – Facts Germany

Der durchschnittliche Nutzer...



- ... hat 130 Freunde auf Facebook
- ... sendet 8 Freundschaftsanfragen pro Monat
- ... verbringt 55 Minuten pro Tag auf Facebook
- ... klickt 9x im Monat den Like-Button
- ... schreibt 25 Kommentare pro Monat
- ... wird Fan von 4 Fanpages pro Monat
- ... wird zu 3 Events pro Monat eingeladen
- ... ist Mitglied in 13 Gruppen

Apps können gefährlich sein

- Social Networks erlauben jedem das erstellen von Apps
- Einige Apps sind oder können zu Malware werden
- Vor kurzem ist Farm Town gehacked worden



Web Spy Shield Warning [X]

WARNING!
Windows has been infected

Name	Type	Alert level
✘ SillyDI Spyware high	Spyware	High
✘ Matcash BG Trojan high	Trojan	High
✘ QQPass I Password Capture	PassCapture	Critical
✘ New.Net.Domain.Plugin Spyware	Spyware	High

✘ **Warning found infected data: 4**

Click the "Erase infected" button to erase all spyware and viruses from Windows

WatchGuard System Manager

- Komplette Anwendung
 - Server, Client, Standalone
 - ab XTM5 inklusive
- Zentrales Management
 - Verteilen von Regeln
- Rollenbasiertes Management
- Gruppierung von Appliances mit unterschiedlichen Freigaben
- Logging und Reporting
 - Automatisiert und angepasste Berichte
 - Integrierter Bestandteil der WatchGuard Lösung
- Managed Security Services von klein bis groß

Extensible Content Security

- Email und Web Security in einer Appliance
- Ein- und ausgehender Verkehr wird untersucht
- Benutzer- und zeitabhängiges Verhalten
- Regelbasiertes Verhalten
 - Analyse von Inhalten
- Lösungen von kleinen Kunden bis zur Großindustrie



Extensible Content Security

- Antivirus für email und Web
 - Kooperation mit Kaspersky
- Data Loss Prevention für email und Web
- Reputation Authority für email und Web
 - www.reputationauthority.org
 - Über 98% des unerwünschten Datenverkehrs wird bereits am Perimeter gestoppt
- Email Verschlüsselung
 - Kooperationspartner voltage
 - Keyless
 - Automatisiert oder wenn gewollt
- Keine email geht verloren!
- Einfachste Implementierung von Cluster



XCS Management

- Zentrales Management
 - Rollenbasiert
 - Geeignet für Endanwender und xSPs
- Multi Domain
- Multi Administrator
- Grafische Auswertung



Zusammenfassung

- Die Sicherheitsthemen werden vielfältiger und komplexer
- Anpassungsfähigkeit der Security Lösung ist immer mehr notwendig
- Lösungen müssen für Endanwender einfach zu verstehen sein ohne an Komplexität zu verlieren
- Lösungen müssen für Dienstleister jeder Größenordnung einsetzbar
- Management muss einfach sein
- Auswertungen müssen schnell und automatisiert zu erstellen sein
- Auswertungen müssen für unterschiedliches Know How verfügbar sein

Unser Dank gilt Ihnen!

- Q4 2010 war für WatchGuard das stärkste Quartal seit bestehen der Firma
- Das WatchGuard Team Deutschland wurde ausgezeichnet – von Ihnen!



CeBIT 2011



CeBIT
HANNOVER
1-5 MARCH 2011

Get red. Get secured.
Stand A20, Hall 11



Fragen & Antworten

Matthias Jessen

Territory Sales Manager

Tel +49 170 4760109

Matthias.Jessen@watchguard.com