State of the Art in Network-Related Extrusion Prevention Systems

Andreas Hackl, Barbara Hauer

Übersicht

- Extrusion Prevention Systems
- Network-Related Extrusion Prevention Systems
- Schwachstellen
- Zusammenfassung
- Überblick über marktführende Anbieter

Extrusion Prevention Systems

Begriffsdefinition

- Herkömmliche Sicherheitssysteme schützen vor unerlaubtem Zugriff auf Daten von außen
- Extrusion Prevention Systems sind Lösung gegen den Verlust vertraulicher Daten durch „Insider“

Gefahrenquellen

- Unerlaubte Weitergabe von Daten über E-Mail, Instant Messanger, USB-Gerät etc.
- Zerstörung/Löschung von Daten
- Manipulation von Daten

Ziele

- Identifizierung,
- Überwachung,
- Analyse und
- Schutz

von vertraulichen Daten während ihres gesamten Lebenszyklus

Datenarten / -Zustände

- Data in Motion
  - Daten die in einem Netzwerk übertragen werden
- Data at Rest
  - Daten in Datenbanken oder Dokumentenmanagementsystemen
- Data in Use
  - Daten mit denen der Benutzer interagiert

System- /Architekturarten

- Endpoint-Related Systems
  - Fokussiert auf „Data in Use“
  - Überwachung und Kontrolle des Datenzugriffs durch Softwareagenten am Endgerät
- Network-Related Systems
  - Fokussiert auf „Data in Motion“
  - Überwachung des Datentransfers in Netzwerken
  - Store-and-Forward-Prinzip

Network-Related Extrusion Prevention Systems

Komponenten

- Netzwerkmonitor
  - Überwachung des Datentransfers
- E-Mail-Integration
  - Quarantäne, Verschlüsselungsintegration und Filterung durch Mail-Agenten
- Filterung/Blockierung und Proxy Integration
  - Filterung und Blockierung des Datentransfers durch Bridge, Proxy oder TCP-Poisoning

Weitere Ziele

- Überwachung des Netzwerkverkehrs
- Reporting
- Protokollierung
- Archivierung

Konzepte

Analyse basierend auf

- Inhalt
- Kontext
  - IP-Adresse und Port von Quelle und Ziel, Größe, Header-Information, Metadaten, etc.
  - Umgebung und Nutzung zur Analysezeit

Techniken zur Inhaltsanalyse

- Regeln und reguläre Ausdrücke
- “Fingerabdrücke” aus Datenbank
- Exakte Übereinstimmung von Dateien
- Partielle Übereinstimmung von Dokumenten
- Statische Analyse
- Konzeptionell/Wörterbuch
- Kategorien

Vor- und Nachteile

- Vorteile
  - Keine Installation am Endgerät
- Nachteile
  - Kein Schutz bei Übertragung von Daten auf physische Geräte
  - Kein Schutz bei verschlüsselten Daten
  - Suchmuster müssen hohe Qualität haben, um Fehlalarme zu vermeiden

Vergleich mit anderen Konzepten

- Network Layer Firewall
  - Keine Inhaltsanalyse
- Application Layer Firewall (ALF)
  - Analysiert nur Teile des Netzwerkverkehrs
- Proxy
  - Nutzbar für Teilbereich
- IDS und IPS
  - Keine Inhaltsanalyse

Schwachstellen

Unübliche Transportkanäle

- Abhängig von Konfiguration der Firewall oder des Proxy
- Bsp.: HTTP und SSH über ICMP
  - ICMP-Tunnel
  - Daten in Payload des ICMP-Pakets
  - meist Request- und Reply-Pakete

Datenschutzgesetz

- Art. 1 § 1 DSG: Grundrecht auf Datenschutz
- Art. 8 ECHR: Recht auf Achtung des Privat- und Familienlebens
- Kontrolle darf Privatsphäre nicht verletzen
  - auf Nichteinhaltung aufmerksam machen
  - ohne Inhalt der privaten Nachrichten zu lesen
- Schutz von Daten ohne Personenzuordnung

Zusammenfassung

- Größte Herausforderung:
  - Definition, Adaption und Anpassung von technischen und organisatorischen Maßnahmen
- Aktuell keine Standards und Normen
- Eingeschränkt auf elektronische Kommunikation
- 1. Schritt bei Extrusion Prevention
- Technology/Konzept im Anfangsstadium

Marktführende Anbieter

- Websense
  - Websense Data Security Suite
  - http://www.websense.com/content/DataSecurity.aspx
- Reconnex
  - iGuard Appliance und inSight Console
  - http://www.reconnex.net/products/index.php
- Verdasys
  - Digital Guardian
  - http://www.verdasys.com/data_loss_prevention.php

Offene Fragen / Diskussion