CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand

IDS, IPS, Date Loss Prevention

CloudCommand GmbH chr.schumacher@gmx.tm

AGENDA

01 IDS/IPS

02 Date Loss Prevention

01 IDS / IPS

Intrusion Detection and Prevention (IDS/IPS)

IDS überwacht den Netzwerkverkehr und analysiert ihn auf mögliche Eindringungsversuche, wie Exploits oder Bedrohungen.

IPS geht einen Schritt weiter, indem es erkannte Angriffe aktiv verhindert, etwa durch das Verwerfen von Paketen oder das Beenden von Sitzungen.

Beide Systeme sind wesentliche Bestandteile der Netzwerksicherheit und oft in Next-Generation Firewalls (NGFW) integriert.

Vorteile von IDS/IPS

Früherkennung von Angriffen: IDS/IPS identifizieren schädliches Verhalten und Exploit-Versuche, bevor sie Schaden anrichten.

Schutz vor Sicherheitslücken: Angriffe auf Schwachstellen in Geräten oder Software werden erkannt und blockiert.

Automatische Bedrohungsabwehr: IPS kann Angriffe aktiv verhindern, indem es Pakete verwirft oder Sitzungen beendet.

Erhöhte Netzwerksicherheit: Schutz sowohl am Netzwerk-Edge als auch im Datencenter, um Angreifer frühzeitig zu stoppen.

Überwachung und Protokollierung: IDS/IPS sammeln wertvolle Informationen über potenzielle Bedrohungen, die für weitere Sicherheitsanalysen genutzt werden können.

Funktionsweise von IDS

Ein Intrusion Detection System (IDS) erkennt verdächtige Aktivitäten im Netzwerk mithilfe drei grundlegender Erkennungsmethoden:

1. Signaturbasierte Erkennung
    - Vergleicht beobachtete Ereignisse mit bekannten Angriffssignaturen.
    - Effektiv gegen bekannte Bedrohungen, jedoch anfällig für neue, unbekannte Angriffe.
2. Anomaliebasierte Erkennung
    - Analysiert den Netzwerkverkehr auf Abweichungen von einem als normal definierten Verhalten.
    - Besonders nützlich zur Erkennung neuer oder Zero-Day-Angriffe.
3. Stateful-Protokollanalyse
    - Überprüft Protokollaktivitäten anhand vordefinierter Regeln für normales Verhalten.
    - Erkennt Unregelmäßigkeiten in der Kommunikation zwischen Geräten.

Diese Methoden ermöglichen es IDS, Bedrohungen frühzeitig zu identifizieren und Sicherheitsmaßnahmen einzuleiten.

Was kann mit IDS/IPS erreicht werden?

Kontinuierliche Netzwerküberwachung

- IDS/IPS überwachen den gesamten Netzwerkverkehr in Echtzeit.

Erkennung und Protokollierung von Sicherheitsvorfällen

- Sie identifizieren potenzielle Angriffe und dokumentieren relevante Informationen für spätere Analysen.

Aktive Bedrohungsabwehr

- IPS kann Angriffe sofort blockieren, indem es verdächtige Pakete verwirft oder Sitzungen beendet.

Was kann mit IDS/IPS erreicht werden?

Sicherstellung der Einhaltung von Sicherheitsrichtlinien

IDS/IPS helfen, Verstöße gegen Unternehmensrichtlinien zu erkennen und zu verhindern.

Schutz vor Angreifern während der Netzwerküberwachung

Sie verhindern, dass Angreifer Informationen über das Netzwerk sammeln und gezielte Angriffe vorbereiten.

Erhöhung der Gesamtsicherheit der IT-Infrastruktur

IDS/IPS sind eine essenzielle Ergänzung moderner Sicherheitskonzepte, insbesondere in Unternehmen.

Diese Funktionen machen IDS/IPS zu einem unverzichtbaren Bestandteil der Netzwerksicherheit.

Was sollte ich auf jeden Fall behalten

- Ein im Internet und Firmennetzwerken häufig genutztes Modell ist das Client Servermodell
- Ein zentraler Serverdienst verwaltet eine oder mehrere Ressourcen, die den Clients zur Verfügung gestellt werden können
- Das Peer-to-Peer-Netzwerk besteht aus gleichberechtigten Arbeitsplatzrechnern.

02 Data Loss Prevention (DLP)

Was ist DLP (Data Loss Prevention)?

Data Loss Prevention (DLP) ist eine Sicherheitsstrategie zur **Erkennung**, **Überwachung und Verhinderung** von **Datenverlust**, **Datenlecks oder unerlaubter Datenexfiltration** in einem Unternehmen.

Wie funktioniert DLP zur Erkennung sensibler Daten?

DLP-Lösungen verwenden verschiedene Techniken, um **sensible Daten zu identifizieren, zu überwachen und zu schützen**.

Diese Methoden ermöglichen es, Datenverluste und unbefugte Übertragungen zu verhindern.

Techniken zur Erkennung sensibler Daten:

Data Fingerprinting

- Erstellt einen **einzigartigen digitalen Fingerabdruck** einer Datei.
- Alle Kopien derselben Datei haben denselben Fingerprint.
- Die DLP-Software scannt ausgehende Daten und vergleicht sie mit bekannten Fingerprints.

Schlüsselwortabgleich

- DLP sucht in Nachrichten oder Dokumenten nach **vordefinierten Schlüsselwörtern oder Phrasen**.
- Beispiel: Eine E-Mail mit dem Wort „vierteljährlicher Finanzbericht“ wird blockiert, wenn das Unternehmen dessen vorzeitige Veröffentlichung verhindern möchte.

Techniken zur Erkennung sensibler Daten:

Pattern Matching (Mustererkennung)

- Analysiert Daten anhand typischer **Muster und Strukturen**.
- Beispiel: Eine 16-stellige Zahlenfolge könnte als **Kreditkartennummer** erkannt und geschützt werden.

Dateiabgleich (File Hashing)

- Vergleicht **Hashes von Dateien**, um sie eindeutig zu identifizieren.
- Ein Hash ist eine einzigartige Zeichenkette, die aus einer Datei generiert wird.
- Bewegt sich eine Datei aus dem Netzwerk, wird ihr Hash mit geschützten Dateien abgeglichen.

Exakter Datenabgleich

- Vergleich mit vollständigen **Datensätzen, die unter organisatorischer Kontrolle stehen**.
- Beispiel: Listen mit Sozialversicherungsnummern oder Kundenlisten werden geschützt, sodass keine unautorisierte Weitergabe erfolgt.

Was ist Datenexfiltration?

Datenexfiltration bezeichnet die **unerlaubte Übertragung oder den Diebstahl von Daten** aus einem Unternehmen oder einer Organisation.

Dies kann durch interne oder externe Akteure erfolgen und stellt eine große Sicherheitsbedrohung dar.

Methoden der Datenexfiltration:

- **E-Mail oder Instant Messaging** → Vertrauliche Daten werden per E-Mail oder Chat weitergeleitet.
- **Externe Speichermedien** → Daten werden auf USB-Sticks oder externe Festplatten kopiert.
- **Cloud-Speicher** → Mitarbeiter laden Daten in eine nicht genehmigte Cloud (z. B. Google Drive, Dropbox).
- **Externe Angriffe** → Hacker erhalten unbefugten Zugriff und stehlen Daten.
- **KI-Tools & LLMs** → Sensible Daten werden in KI-Tools hochgeladen, was Risiken für Datenschutz und Sicherheit birgt.

Wie verhindert DLP Datenexfiltration?

✅ **Überwachung des Datenflusses** → DLP verfolgt Daten in Bewegung, auf Endgeräten und bei der Speicherung.

✅ **Warnmeldungen & Zugriffskontrolle** → Falls sensible Daten das Netzwerk verlassen könnten, warnt DLP Administratoren.

✅ **Blockieren von Datenübertragungen** → DLP kann unautorisierte Dateiübertragungen stoppen.

✅ **Einschränkung von Funktionen** → Das Kopieren/Einfügen innerhalb unsicherer Anwendungen kann verhindert werden.

Anwendungsbereiche von DLP:

Schutz vertraulicher Daten

- Verhindert den Verlust von sensiblen Geschäftsinformationen, z. B. Finanzdaten oder Kundendaten.

Einhaltung von Datenschutzrichtlinien

- Unternehmen können mit DLP **gesetzliche Vorgaben** wie **DSGVO, HIPAA oder PCI-DSS** einhalten.

Anwendungsbereiche von DLP:

Überwachung des Datenverkehrs

- DLP erkennt und blockiert verdächtige Datenübertragungen über E-Mail, Cloud-Dienste oder USB-Geräte.

Schutz vor Insider-Bedrohungen

- DLP kann verhindern, dass Mitarbeiter absichtlich oder versehentlich vertrauliche Daten weitergeben.

Arten von DLP-Lösungen:

Netzwerk-DLP → Überwacht und kontrolliert Datenverkehr über das Unternehmensnetzwerk.

Endpoint-DLP → Überwacht und schützt Daten auf Endgeräten (PCs, Laptops, USBs).

Cloud-DLP → Schützt Daten in Cloud-Anwendungen und Cloud-Speichern.

Best Practices zum Schutz vor Datenverlust (DLP)

Ein wirksamer Schutz vor Datenverlust erfordert mehr als nur eine DLP-Software. Unternehmen sollten eine umfassende Sicherheitsstrategie implementieren, die **technische, organisatorische und menschliche Faktoren** berücksichtigt.

Best Practices zum Schutz vor Datenverlust (DLP)

Mitarbeiteraufklärung & Schulungen

- Sensibilisierung der Nutzer für Sicherheitsrisiken und Best Practices.
- Schulungen zu Phishing, Social Engineering und sicheren Datenpraktiken.

Datenklassifizierung & Transparenz

- Unternehmen müssen wissen, **welche Daten wo gespeichert sind** und wie sensibel sie sind.
- Regelmäßige Audits zur Überwachung der Datenströme.

Zugriffskontrollen implementieren

- Beschränkung des Zugriffs auf sensible Daten nach dem **Prinzip der geringsten Rechte (Least Privilege)**.
- Multi-Faktor-Authentifizierung (MFA) für besonders kritische Daten.

Best Practices zum Schutz vor Datenverlust (DLP)

Datenverschlüsselung

- **Ende-zu-Ende-Verschlüsselung** für Daten während der Übertragung und im Ruhezustand.
- Schutz vertraulicher Dateien mit sicheren Verschlüsselungsalgorithmen.

Zero-Trust-Ansatz einführen

- Kein Benutzer oder Gerät wird standardmäßig als vertrauenswürdig eingestuft.
- **Authentifizierung und Autorisierung** werden kontinuierlich überprüft.

Best Practices zum Schutz vor Datenverlust (DLP)

Einsatz einer DLP-Lösung

- Implementierung einer **Data Loss Prevention (DLP)**-Software zur **Überwachung, Erkennung und Blockierung** sensibler Datenbewegungen.
- Kombination aus **Data Fingerprinting, Pattern Matching und Zugriffskontrollen**.

Regelmäßige Sicherheitsüberprüfungen & Audits

- Proaktive **Schwachstellenanalysen und Penetrationstests** durchführen.
- Anpassung der Sicherheitsrichtlinien an neue Bedrohungen.

Fazit

DLP ist eine Kombination aus **Technologie, Prozessen und Schulungen**.

Durch den Einsatz von **Verschlüsselung, Zugriffskontrollen und Zero-Trust-Sicherheitsmodellen** kann das Risiko von Datenverlusten erheblich reduziert werden.

Gibt es noch Fragen?

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm