NTT Security

Solution Overview

Managed Security Device Service IDS/IPS

24/7 Managed Intrusion Detection und Prevention

Angreifer finden immer öfter einen Weg an Firewall und Virenscanner vorbei und bedrohen das Firmennetz. Dagegen helfen Intrusion Prevention Systeme (IPS), die nach Angriffsmustern oder Anomalien im Netzwerk suchen und Schadsoftware abwehren. Doch der Einsatz von Intrusion Prevention Systemen muss gut konzipiert, richtig umgesetzt und die Daten vor allem richtig interpretiert werden.

Die Produkte haben sich mittlerweile zu vielseitigen Schutzwerkzeugen entwickelt, die dem Administrator wichtige Einblicke ins Netzwerk geben und, wenn richtig konfiguriert, sogar Compliance-Anforderungen wie und Standards wie ISO 27001, PCI DSS und Empfehlungen der FINMA erfüllen. IPS reagieren nicht nur auf bekannte Verhaltensmuster, sondern erkennen auch verdächtige Anomalien und sind in der Lage, selbständig gefährliche oder verdächtige Netzverbindungen zu unterbrechen.

Sie können Gefahren im Netzwerkverkehr erkennen, klassifizieren und stoppen. Dies bezieht sich z.B. auf die Erkennung und Prävention von:

- Bekannte Zero-Day-, Denial-of-Service (DoS)- und verschlüsselte Angriffe
- Bedrohungen wie Spyware, VoIP-Sicherheitslücken, Botnets, Netzwerkwürmer, Malware, Phishing, Trojanern und Peer-to-Peer-Applikationen
- Protokoll-Anomalien und Tunneling-Versuche

Herausforderungen

Die regelmässige Aktualisierung und die permanente Überwachung der Systeme können schnell zu einer grossen Belastung für Ihre begrenzten Sicherheitsressourcen werden.

IDS-/IPS-Geräte generieren zudem täglich Tausende von Warnmeldungen, deren Untersuchung für Ihr Security-Team sehr zeitaufwändig ist. Hinzu kommt der stetige Bedarf an erfahrenen Security-Analysten und Threat Huntern zur Sicherung einer hohen Analyse-Qualität – und das in Zeiten akuten Fachkräftemangels.

Bei der Planung und dem Betrieb von IDS/IPS gilt es also einiges zu beachten. Seinen vollen Nutzen kann ein IDS/IPS nur entfalten, wenn es richtig platziert und entsprechend der individuellen Unternehmensanforderungen konfiguriert, immer up-to-date und rund um die Uhr gemanagt, überwacht und gewartet wird.

NTT Security unterstützt Sie mit zertifizierten Sicherheitsexperten, Ihre IDS-/IPS-Effizienz zu steigern:

- Bereitstellung/Installation eines State-of-the-Art ISD/IPS (alternativ: MSS-kompatible Basiskonfiguration eines bestehenden IDS/IPS)
- Health Incident Monitoring und Management (oder Leistungs- und Verfügbarkeitsverwaltung)
- Life-Cycle- und Release-Management (oder Regelmässige Updates/Upgrades und Patchverwaltung)
- Policy- und Signaturverwaltung (oder Richtlinien- und Policy-konforme Signaturkonfiguration und -aktualisierung)

Maximale Rendite Ihrer IDS/IPS-Investitionen

- Optimierte Sicherheitsleistung Ihres IDS/IPS durch fachkundige Signaturabstimmung und Geräteverwaltung
- Zugang zu NTT Security eigenen Spezial-Signaturen, Entwicklung individueller Signaturen
- Bessere Analyse-Ergebnisse und Entscheidungsgrundlage für richtige Abwehrmassnahmen
- Schnellere Bedrohungserkennung und Reaktion in Echtzeit durch 24/7 Überwachung der IDS/IPS-Alarme
- Erfüllung von Compliance-Vorgaben und Gesetzen sowie richtlinienkonforme Berichterstattung
- Geringerer Bedarf an spezialisierten internen IT-Fachkräften (oder Lösung des Fachkräftemangel-Problems)
- Informationen zum Traffic-Verhalten im Unternehmen
- Zusätzliche Sicherheit durch IDS/IPS-Datenkorrelation mit hochentwickelter Threat Intelligence
- Fix kalkulierbare IDS/IPS-Kosten für 24/7 IDS/IPS-Management, -Monitoring und -Support

- 24/7 Security Device Support mit integriertem, rund um die Uhr erreichbaren SOC
- Datensicherung und -wiederherstellung (oder Back-Up)
- Vulnerability Management bei Veröffentlichung einer kritischen Schwachstelle des Managed Devices
- Change-Management
- Standalone Sensor für spezielle Punkte im Netzwerk

NTT Security unterstützt Sie mit erfahrenen Security-Analysten und Threat Huntern, die Sicherheitsleistung Ihres IDS/IPS zu optimieren:

- 24/7 Event-Analyse und Echtzeitreaktion (oder Bedrohungsüberwachung und Echtzeitreaktion)
- NTT Security eigene Spezial-Signaturen und Entwicklung individueller Signaturen
- Zusätzliche Threat Intelligence- und Human Expert-Analysen von Störungen
- Fachkundige Massnahmen-Empfehlungen im Fall von Sicherheitsverletzungen
- IDS/IPS-Strategieberatung, z.B. für das Blocken von Bedrohungen
- Sicherheits- und Compliance-Reporting
- Regelmässiger Service-Clean-Up nach ausführlichen Log- und Signaturen-Analysen
- Periodischer Review der Managed Security Service-Qualität

Erste Schritte zum Managed IPS

KICK-OFF WORKSHOP

Analyse der eingesetzten IT-Systeme und Applikationen

Identifikation der zu schützenden Daten und Netzwerksegmente

Überprüfung von Performance und Hardware-Sizing

Bestimmung der unternehmensspezifischen Sicherheitsanforderungen

Festlegen des individuelles IPS-Schutzprofil

Definition der Verantwortlichkeiten und Ansprechpartner

IDS-SET-UP PHASE

Aufbau und Installation des IPS als IDS

Konfiguration der IPS-Schutzprofile

Klassifizierung der Signaturen nach Risikograd

Klassifizierung der Signaturen nach Erkennungsrate

Klassifizierung der Signaturen nach Performance-Impact

Definition und Implementierung des Signatur-Sets

IPS-SET-UP PHASE

Optimierung der IDS/IPS-Konfiguration

Optimierung der Confidence-Level

Abstimmung der Signaturen auf die Kundenumgebung

Eliminierung Netzwerk oder IPS-spezifischen Fehlverhaltens

Bandbreitenregulierung und anwendungsorientierte Priorisierung

Finale Umstellung von IDS auf IPS

BETRIEBSPHASE

24/7 IPS-Management, -Monitoring und -Support

IPS-Systemadministration, -Kalibrierung und -Fine-Tuning

IPS-Anpassungen bei veränderter Einsatzumgebung und Rechtslage

Echtzeitanalyse des Netzwerkverkehrs entsprechend festgelegter Policies

Threat Intelligence- und Human Intelligence-Analyse im Störungsfall

Incident Handling

Über NTT Security

NTT Security ist das auf Informationssicherheit und Risikomanagement spezialisierte Unternehmen der NTT Group (Nippon Telegraph and Telephone Corporation), einem der grössten IKT-Unternehmen weltweit. Der Experte für IT-Security steht für ein ganzheitliches Sicherheitskonzept und die Bereitstellung ausfallsicherer Lösungen, die den Anforderungen der Kunden vor dem Hintergrund des digitalen Wandels gerecht werden. Mit zehn globalen SOCs, sieben Zentren für Forschung und Entwicklung sowie mehr als 1.500 Sicherheitsexperten unterstützt NTT Security Unternehmen auf sechs Kontinenten bei der Reaktion auf Hunderttausende Sicherheitsvorfälle pro Jahr.

NTT Security bietet Kunden die richtige Mischung aus Beratung, Managed Services und Technologien, indem lokales Know-how optimal mit globalen Ressourcen kombiniert wird. Weitere Informationen finden sich unter **nttsecurity.com/ch**.