IDS x IPS

Matriz: Bauru/SP
Filial 1: Florianopolis/SC

O que é a Firewalls?

- **Empresa Especializada em Segurança;**
- **Profissionais Certificados;**
- **Atenta a Padrões Internacionais;**
- **Parceira das maiores empresas de Segurança do Mundo;**
- **Visão de Negócios e Ética Empresarial;**
- **Soluções Personalizadas para a Realidade das Empresas;**
- **Independente de Fornecedores e Tecnologias proporcionando a melhor solução para o cliente específico.**

O que a Firewalls tem?

- **Treinamentos em Segurança;**
- **Implementação de Infra-Estrutura de Redes;**
- **Implementação de Análises de Risco e Vulnerabilidades;**
- **Implementação de Detectores de Intrusão e Politicas de Segurança;**
- **Consultoria em E-commerce e Desenvolvimento;**
- **Divisão de Alta Disponibilidade e Disponibilidade Continua;**
- **Homologação de Firewall.**

Parcerias

SOPHOS anti-virus and anti-spam for business

ISPA CYCLADES

DATASAFE DATA SECURITY

CYCLADES

iAnywhere SOLUTIONS A SYBASE COMPANY

3M Worldwide

SPI DYNAMICS secure. protect. inspect.

SERASA

SCUA Segurança e Gestão de TI

CLM

thawte it's a trust thing

(nfr)(security)

SOURCEfire™

"If you want steel doors and shutters on your network, NFR is the one for you."
- SC Magazine

Applied Watch Technologies

ScannerX vulnerability assessment services

Objetivos

- **Explicar o que é Detecção de Intrusos;**

- **Explicar o que é Prevenção de Intrusão;**

- **Justificar o relatório do Gartner a respeito do fim da Detecção de Intrusos, através da resposta da Enterasys.**

O que é Segurança?

CIDAL =

Confidencialidade
Integridade
Disponibilidade
Autenticidade
Legalidade

LEMBRAR-SE SEMPRE DISTO NO DECORRER DA PALESTRA!

Ambiente em Questão

Trabalhamos em um mundo real de sistemas mal configurados:

* **Bugs de Software**
* **Empregados Insatisfeitos**
* **Administradores de Sistemas Sobrecarregados**
* **Acomodação de necessidades empresariais**
* **Falta de Educação em Segurança**
* **B2B,B2C,B2E,C2C,X2X?**

Defense In-Depth

- Um Firewall apenas aumenta o nível de segurança;
- O conceito de segurança em camadas garante que as falhas existentes em um Firewall sejam supridas por outros tipos de defesa e segurança;
- Através de diversas camadas cria-se um modelo de segurança robusto e capaz de suportar falhas.

Quando pensar em Segurança pense em uma CEBOLA.

Gartner

- Responsável pelas afirmações (foram traduzidas)
GaryGolomb
Engenheiro Senior de Pesquisas
Dragon Intrusion Detection Group
Enterasys Networks

- Gartner, Inc. Recentemente lançou um documento de autoria do Sr. Richard Stiennon entitulado "Intrusion Detection Is Dead - Long Live Intrusion Prevention".

- Gartner se descreve como "Por 20 anos, o Gartner Research & Adivisory services tem sido reconhecido como fonte definitiva pelos líderes de tecnologia"

Comentários

- Todos cometem erros e infortunadamente este não é o primeiro erro do Gartner. Um outro artigo já de algum tempo do próprio Gartner menciona:

" Prevenção de Intrusão irá substituir a Detecção de Intrusão. Empresas investiram muito dinheiro em sistemas para detectar intrusos – estes falharam em prover segurança adicional – enquanto os sistemas de prevenção de intrusão emergem para prover uma forte defesa contra cyber-ataques"

- Não, está não é a primeira vez que o Gartner mostrou uma grotesca falta de entendimento entre detecção e prevenção quanto a tarefas reais, porém este sem dúvidas foi o mais horrivel.

Comentários

- Então, como todas estas afirmações são sérias, vamos primeiro definir COMO as pessoas utilizam tecnologias de Detecção de Intrusos.

- Sistemas de Detecção de Intrusos são utilizados por uma única razão. São a última chance de ser notificados a respeito de uma falha em sistemas. Enquanto as organizações investem muito tempo e dinheiro em sistemas protecionistas (...) os IDS tem o propósito de avisar caso estes falhem. Apesar de todos os investimentos em tecnologias para proteção, os invasores conseguem passá-los (automaticmamente ou não). Isso devido a falhas no design da rede, vulnerabilidades em aplicações ou dispositivos mal-configurados. Por isso os detectores de intrusos foram inventados.

Comentários

- A maior diferença entre sistemas de IDS e outros dispositivos de segurança é o fato deste ser out-of-band, ou passivos por natureza. Ele passivamente verifica o tráfego que passa procurando por assinaturas de ataques, comprometimentos ou outros usos incorretos. O benefício chave deste gerenciamento out-of-band é que você tem a habilidade de marcar os tráfegos que são suspeitos. Se seu IDS lhe dá muitos tráfegos suspeitos, então, configure-o! O que é suspeito em um ambiente pode não ser em outro. Os fabricantes tentam compensar o melhor possivel, mas somente você sabe o que é melhor para seu ambiente! (...)

Comentários

- Vejamos agora algumas razões que o Gartner definiu para sua afirmativa insensata:

--- Razao #1 " Contrariamente a filosofia, é impossivel proteger as redes contra todos os ataques que elas venham a sofrer." ---

Ok, esta é a razão mais cômica de todas. Começando falando que a intenção de um IDS é a de proteger a rede de todos os ataques contra estas, tenho que rir. Isto demonstra o posicionamento do resto do documento.

Comentários

--- Afirmativa #2 "As zonas desmilitarizadas (DMZ) demonstram diversas exceções em políticas de segurança. Esta possui as tarefas de serviços de missão crítica ---

Enquanto as DMZs (aparentemente) possui tarefas de missão crítica, Richard propõe (o que dúvido) uma nova nomenclatura, uma arquitetura para substituir as DMZ. O novo nome seria The Transition Zone (TTZ?). A idéia seria colocar um Firewall entre a internet e seus servidores públicos e um outro entre seus servidores públicos e sua intranet.

Interessantemente, isto realmente é o que o resto do mundo chama de DMZ. Não se foi demonstrado diferenças entre TTZ e o que as organizações vêem como sua DMZ.

Comentários

--- Afirmativa #3 A respeito de outros problemas com hosts na DMZ: "Devido a constante exposição desses ao mundo, eles precisam ser protegidos e exigem investimentos em dispositivos de segurança, como hosts de sacrifício." ---

Tenho perguntado a muitas empresas Fortune 50 e alguns consumidores pequenos, sobre a existência, em suas DMZ, de hosts para sacrificio. Eles dizem NÃO.

Comentários

--- Afirmativa #4 "Em 2005, 90% dos 200 gateways globais vão estar com 100% de inspeção de pacotes, habilitando o bloqueio de ataques de aplicação." ---

Voltaremos a esta afirmação em um minuto.

---Afirmativa #5 "IDS propõe o modelo 'belt-and-suspenders' a defesa do perímetro" ---

Nesta curta afirmação existem dois erros.

UM- IDS não impõe "belt-and-suspenders" a defesa de perímetro (...) apesar do contraste, ele não "suporta" proteção, ele "detecta" quando outros mecanismos falham. Ele ajuda na auditoria, fazendo parte do último ciclo da segurança - "reação".

Comentários

DOIS - IDS não foram desenvolvidos apenas para o perímetro. Muitas organizações os tem em outras partes da rede, grupos de servidores, grupos com grandes caches de IP ou outros dados, e também em locações de parceiros (...).

--- Afirmativa #6 "As tecnologias de estado irão exigir dos agentes de rede escalarem até velocidades multigigabit." ---

Esta afirmação demonstra o óbvio e grosso desentendimento da implementação e design do desenvolvimento de IDS. Uma robusta implementação de estado leva em consideração overhead devido a um bom reconhecimento de string, decodificação de protocolo ou detecção de anomalias. Os firewalls são prova disto.

Comentários

Detectores de intrusos precisam encontrar um balanço entre estas metodologias, sem retirar a performance do sensor. Não existe uma simples solução (como checagem de estado) que seja boa para ser utilizada como único método de detecção, ou para o estado suportar velocidades multigigabit.

--- Afirmativa #7 IPS precisa fazer isto: "Ele requer uma detecção eficiente de ataques maliciosos. Agentes de rede utilizam combinações de assinaturas, detecção de anomalias em protocolos e análises de tráfego para minimizar os falsos positivos. Tecnologia de estados permitirá os agentes de rede escalarem até velocidades multigigabit se necessário. Isto permitirá que eles decidam transparentemente se devem permitir ou bloquear seções." ---

Comentários

Esta afirmação aparentemente demonstra como o Gartner sucumbiu ao marketing. Você pensa que eles basearam o seu paper em análises de novas vulnerabilidades, ou mantendo um time de desenvolvimento de exploits todo o tempo, ou verificando o desenvolvimento geopolítico e os impactos sociais dos ataques e do hacking, certo? Baseado no dito, requerimentos de design, isso soa como um documento escrito para ser um glossário de marketing para um IPS.

(Omitimos alguns exemplos de afirmações de outros revendedores de IPS por questões de PROFISSIONALISMO).

Resumo da Firewalls

Diversos itens como colocar um IPS transparentemente garantindo inspeção em tempo real para aplicações multigigabit demonstram total falta de profundidade demonstrada pelo artigo do Gartner, já que as profundas inspeções realizadas por sensores IDS não poderiam ser desenvolvidas conjuntamente com o roteamento/bloqueio de tráfego exigido por um IPS.

Outros itens como falsos positivos, que gerariam bloqueios instantâneos e falsos negativos que não seriam vistos por ninguém, geram mais questões a serem levadas em consideração.

Esperamos com isto termos definido de uma vez que o artigo é insensato e portanto não pode ser tomado por base para uma real medida e escolha de uma solução de segurança.

Utilizamos as afirmativas demonstradas por pessoas do Dragon, para demonstrarmos que este não é apenas o posicionamento da Firewalls, representante exclusiva da NFR no Brasil, como também de todos os grandes players do mercado.

FIM! Será mesmo?

DÚVIDAS?!?

Rodrigo Rubira Branco
rodrigo@firewalls.com.br