Empresa FIREWALLS

Desafios e Soluções em Detecção de Intrusão

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)

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

SOURCEfire

Applied Watch Technologies

ScannerX vulnerability assessment services

Objetivos

- Explicar o que e Detecção de Intrusos;
- Explicar o porquê e onde se deve utilizar detecção de intrusão;
- Demonstrar as falhas e dificuldades existentes em sistemas de detecção de intrusos;
- Fornecer panoramos e idéias concretas para escolha de um bom sistema de detecção de intrusão;
- Demonstrar como e com o que um sistema de detecção de intrusos pode interagir;
- Demonstrar a capacidade de sistemas de detecção de Intrusão e seus tipos;
- Apresentar uma estrutura lógica e coerente de detecção de Intrusão.

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.

Anatomia de um Ataque

- Anatomia de um Ataque:

*** Detectando informações do alvo;**
*** Buscando vulnerabilidades;**
*** Explorando vulnerabilidades encontradas.**

Tipos de Ataque

- **DoS/DDoS**

  * **LinkFlood**
  * **Smurf**
  * **SynFlood**
  * **Vulnerabilidade**
  * **Land**
  * **Teardrop**
  * **Exploração**
  * **BufferOverflow**
  * **FormatString**
  * **SQL Injection**
  * **Cookie Poisoning**
  * **Cookie Tampering**
  * **...**

IDS – Porque utilizar?

- Firewalls podem agir somente sob ataques, IDS detectam as varreduras.

- Firewalls agem segundo regras pré-estabelecidas que geralmente não enchergam a camada de aplicação.

Tipos de IDS

Constitui-se de 4 grandes tipos, a saber:

*** HIDS**
*** NIDS**
*** IDS Ativo**
*** IDS Passivo**

Fornecedores de IDS

* **NFR;**
* **SourceFire;**
* **Snort;**
* **Microsoft;**
* **CheckPoint;**
* **SecurePoint;**
* **Cisco;**
* **Symantec;**
* **CA;**
* **ISS.**

Problemas com Detecção de Intrusão

* **Fragmentação;**
* **Criptografia (VPN);**
* **UUEncode;**
* **Velocidade dos Links;**
* **Falsos Positivos x Falsos Negativos.**

Soluções

Como diminuir falsos positivos Integrando com análise de vulnerabilidades

VANTAGENS x DESVANTAGENS

*** Automatizando o processo;**
*** Inteligência em Detecção de Intrusos;**
*** Gerenciamento integrado de detectores;**
*** Correlação de eventos em Detecção de Intrusão e sua importância;**
*** Integrando com Firewalls.**

IDS + Traffic Shaping

- **Controle de DoS, Worms e Virus;**

- **Controle de Spams, e uso de Links por aplicativos indevidos;**

- **Garantia de disponibilidade dos serviços essenciais;**

LEGALIDADE

- **Direito a Privacidade;**

- **Informações Particulares podem ser capturadas?;**

- **Convencendo os Diretores/Funcionários;**

- **Termo aditivo ao contrato de trabalho.**

Outras considerações

- **Detecção de Intrusos em Máquinas Virtuais;**

- **Firewalls Rapid ResponseTeam no Brasil (FRRT);**

- **Garantia de disponibilidade dos serviços essenciais;**

- **Terceirização de Detecção de Intrusos.**

NFR

(nfr)(security)

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

- **Distribuidor Exclusivo no Brasil: Firewalls;**
- **Firewalls Rapid ResponseTeam no Brasil (FRRT);**
- **Robustez, performance, gerenciamento, inteligência;**
- **Certificação OSEC e OPSEC.**

Certificação OSEC

- Certificação para sistemas de IDS;
- Mantido por uma parte neutra (Neohapsis);
- Testes de Fragmentação e Segmentação a altas larguras de banda e números de sessões;
- Testes de Injeção de Delay e Ofuscação HTTP (codificação hexa, codificacao hexa dupla, unicode, parâmetros incorretos,reuso de conexões, strings manipuladas, etc);
- Injeção de strings;
- Testes de estado;
- Testes de integridade do dispositivo;
- Testes de base de assinaturas;
- Testes de descarte de pacotes forjados/manipulados.

FIM! Será mesmo?

DÚVIDAS?!?

Rodrigo Rubira Branco
rodrigo@firewalls.com.br