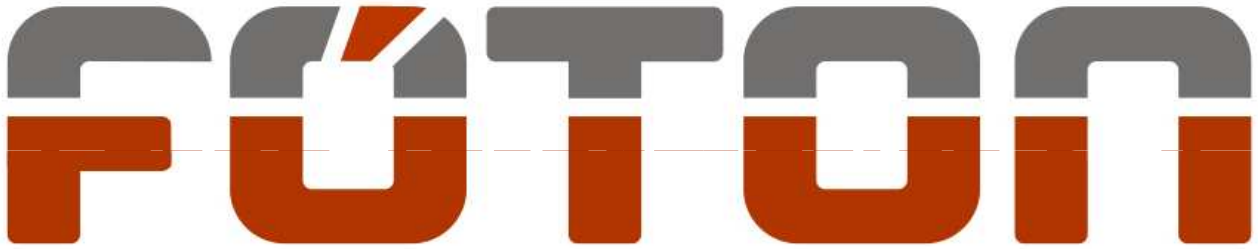


Agenda

- Problemas de Segurança em aplicações Web
- Onde estão as vulnerabilidades
- Principais Ataques
- Solução IBM – Rational Appscan

IBM Rational Appscan

23/01/2006 - 08h16

Ataques virtuais dão prejuízo de US$ 67 bi aos EUA

da **Folha Online**

Os Estados Unidos perderam, no ano passado, cerca de US$ 67,2 bilhões como conseqüência de crimes virtuais. A informação foi divulgada na última semana pelo FBI (polícia federal norte-americana) e tem como base uma pesquisa realizada com 2.066 empresas norte-americanas.

Cerca de 90% destas organizações disseram ter sofrido problemas de segurança com seus computadores nos últimos 12 meses --um quinto delas afirmaram ter sido atacadas 20 ou mais vezes durante o período.

IBM Rational Appscan

Foco no Roubo de Informações

Invasão de sistema expõe dados de 310 mil

Classificação: OOOOO / 0

Fraco ◯ ◯ ◯ ◯ ◉ Bom Avaliar

14-Abr-2005

Uma investigação interna na divisão LexisNexis da editora e provedora de informações Reed Elsevier descobriu evidências de que cerca de 310 mil pessoas podem ter seus dados pessoais expostos. Segundo a empresa, autorizados tiveram acesso ao banco de dados com informações social e os números das carteiras de habilitações de seus client Em um comunicado, a empresa afirmou que foram 59 incidentes ocorridos em seus sistemas. Inicialmente, 30 mil clientes tiveram roubados, e desta vez, outros 280 mil nomes também podem es

No golpe, os invasores utilizaram senhas e nomes de clientes leg ganhar acesso aos dados pessoais.

A LexisNexis é proprietária da Seisint, empresa que mantém em de informações com dados pessoais de cidadãos norte-american segurança social, históricos de crédito e registros criminais.

A empresa divulgou nos últimos anos os dados que mantém no s Terrorism Information Exchange), programa que compartilha os autoridades norte-americanas.

Depois do incidente, a LexisNexis informou que vai reforçar seus News Service, EUA

07/01/2006 - 16h01

Piratas concentram foco no roubo de informações

JULIANA CARPANEZ
da **Folha Online**

PUBLICIDADE

Anúncios UOL

Pen Drive 4GB
USB 2.0. Clique aqui e compre!

Nada de apagar arquivos, travar programas ou alterar dados. Um estudo global da empresa britânica de segurança Sophos mostra que o foco dos piratas virtuais está cada vez mais voltado para o roubo de informações --o objetivo final destas ações são os ganhos financeiros. Em 2005, os programas que repassam dados de micros infectados a pessoas mal-intencionadas (pragas conhecidas como cavalos de tróia) responderam por 62% das infecções.

No Brasil, o padrão se mantém, segundo dados do Cert.br (Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil), um dos braços do Comitê Gestor da Internet no Brasil.

Em 2005, as tentativas de fraudes virtuais no país aumentaram 579% em relação ao ano anterior. No ano passado, quando o centro recebeu 68 mil notificações sobre incidentes, 27.292 (ou 40%) referiam-se a tentativas de fraudes virtuais. Já em 2004, elas responderam por apenas 4.015 dos 75.722 problemas reportados (5,3% do total).

FÓTON

Foco no Roubo de Informações

Homem teria roubado 130 milhões de nº de cartões de crédito

17 de agosto de 2009 • 18h30 • atualizado às 19h01

NOTÍCIA

AA

Um americano de 28 anos foi acusado de roubar informações relacionadas a 130 milhões de números de cartões de crédito e débito nos EUA. Segundo autoridades judiciárias, o caso pode ser maior tentativa de fraude e roubo de identidades online já registrado no país.

Albert Gonzales foi indiciado por conspiração para invadir redes de computadores de importantes organizações financeiras americanas e por roubar dados relativos a mais de 130 milhões de cartões. Gonzales, do Estado da Flórida, está sendo acusado, junto com dois outros cúmplices de usar uma técnica sofisticada chamada de "SQL injection Attack" que invade as redes via seus dispositivos firewall para roubar informações de cartões de crédito ou débito.

A promotoria afirma que a partir de outubro de 2006, Gonzales e seus cúmplices estudaram os sistemas de crédito e débito usados por suas vítimas, criando em seguida uma forma de invadi-los. Os dados roubados eram então enviados para servidores nos Estados americanos da Califórnia, Illinois e em outros países como Letônia, Holanda e Ucrânia.

FÓTON

IBM Rational Appscan

Guerra Cibernética?

Tecnologia

Imprimir Enviar Rss Celular

Quinta, 9 de julho de 2009, 18h42

REUTERS

Novos ataques na web são registrados; Coreia do Norte é suspeita

Uma nova onda de ataques cibernéticos que causaram lentidão em websites dos Estados Unidos e Coréia do Sul atingiu novos alvos nesta quinta-feira, informou uma empresa de segurança na Internet.

Segundo a agência de inteligência sul-coreana, o ataque dos hackers pode ter ligação com a Coréia do Norte.

O impacto dos ataques cibernéticos, que até agora tiveram como alvo dezenas de sites, incluindo o da Casa Branca e o da sede do governo da Coréia do Sul, foi considerado insignificante, mas serviu como um lembrete de que o governo norte-coreano tem se planejado para uma guerra cibernética.

"O ataque previsto de fato ocorreu, mas medidas consideráveis de contenção foram tomadas e realmente funcionaram como uma defesa até certo grau", disse um dirigente da empresa de segurança online Ahnlab.

Últimas notícias

19h29 »Serviço gratuito promete "tweets" com até 200 caracteres

18h38 »Lucro e receita da HP superam levemente estimativas

16h59 »Usuários processam Facebook por políticas de proteção de dados

Busque outras notícias no Terra

BUSCAR

FÓTON

IBM Rational Appscan

Web 2.0

IBM Rational Appscan

Web 2.0

Sexta, 14 de agosto de 2009, 20h20

Hacker controlava 200 computadores via Twitter

Jordan Robertson

Um investigador que analisava os ataques que bloquearam o Twitter na semana passada descobriu outro problema de segurança diferente que também afetou a popular rede de microblog. O - ou os - delinquentes por trás dos ataques utilizaram uma conta no Twitter para controlar uma rede com cerca de 200 PCs, a maioria no Brasil, disse José Nazario, da Arbor Networks.

» **Professor de 34 anos foi alvo principal de ataques ao Twitter**
» **Hackers russos tiraram Twitter do ar, diz especialista**

As redes de PCs infectados são conhecidas como "botnets", ou redes de PCs "zumbis", e são usadas para causar grande parte dos ataques como o que paralisou o Twitter, além dos roubos de identidade ou envio de spam.

Nazario disse que encontrou uma conta do Twitter que enviava mensagens que pareciam não ter sentido, mas que na realidade eram ordens para que os computadores infectados visitassem sites de onde baixavam programas desenhados para roubar senhas bancárias.

Últimas notícias

20h20 »**Hacker contr computadore**
18h06 »**Ministério ale falsos sobre**
13h08 »**Professor de principal de a**

Busque outras notíci

BUS

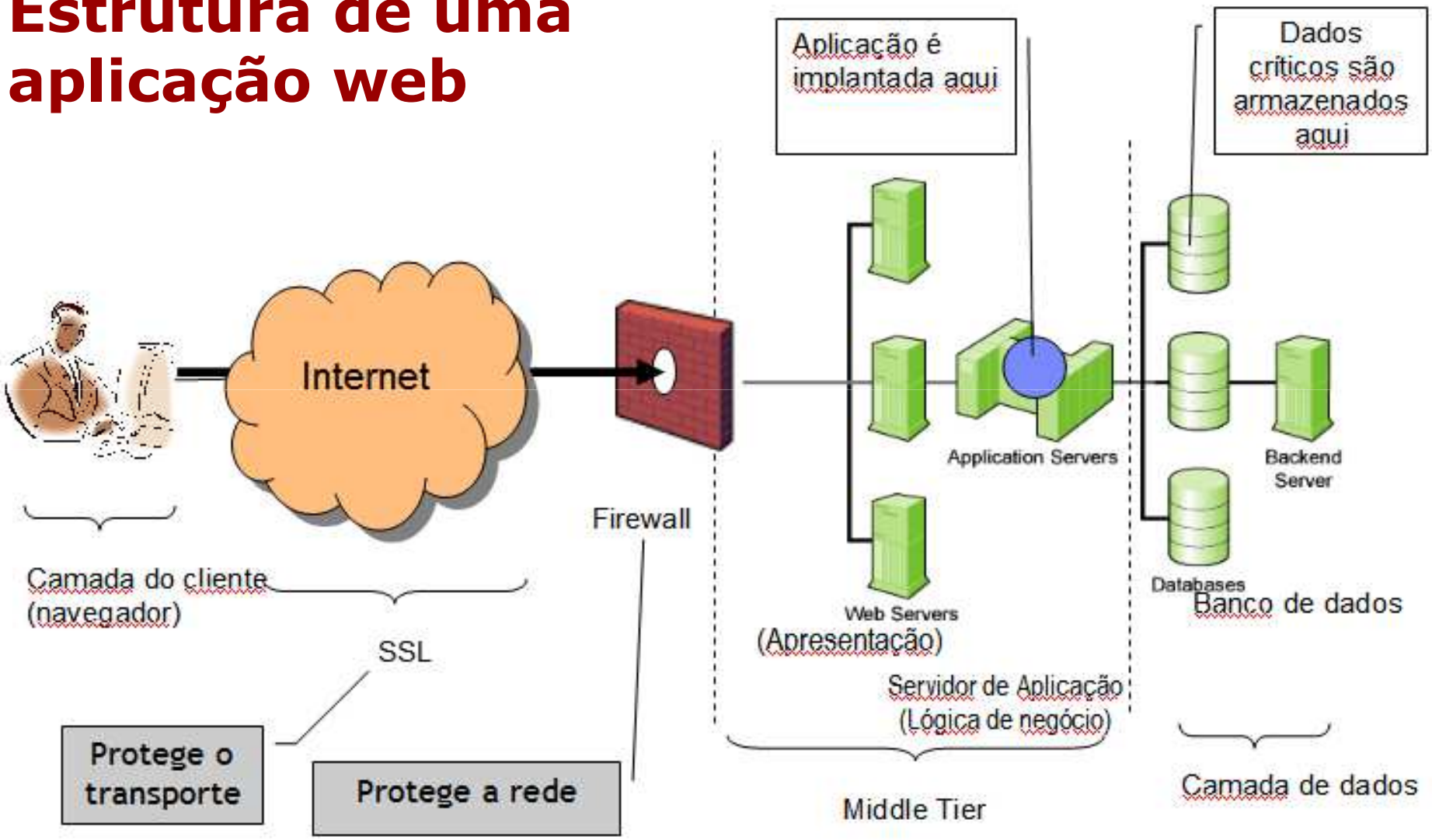
FÓTON

IBM Rational Appscan

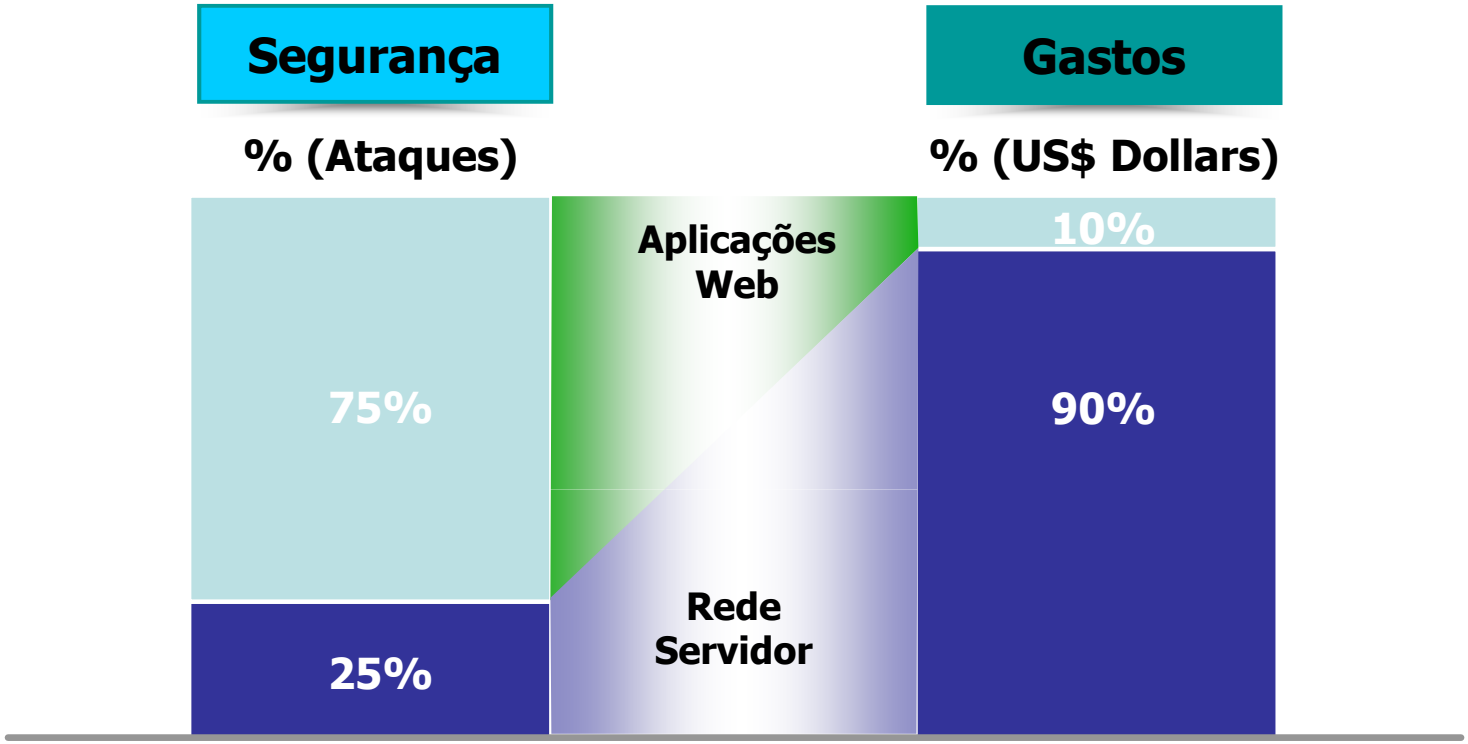
IBM Rational Appscan

Não temos implementado segurança suficiente?

Estrutura de uma aplicação web



IBM Rational Appscan



75% de todos os ataques são direcionados à camada de aplicação web

2/3 de todas as aplicações web estão vulneráveis

Gartner

FÓTON

Rational Appscan

Principais Tipos de Vulnerabilidade

- SQL Injection
- XSS (Cross-Site Scripting)
- Manipulações de URL

Rational Appscan

SQL Injection

- SQL – Linguagem textual – Query – Banco de Dados
- Os comando e parâmetros de uma query podem modificar a estrutura e conteúdo do bando de dados (DDL, DML)
- Aplicações que não validam as entradas dos usuários muitas vezes permitem a um "hacker" inserir trechos de declarações SQL
- Demonstração

Rational Appscan

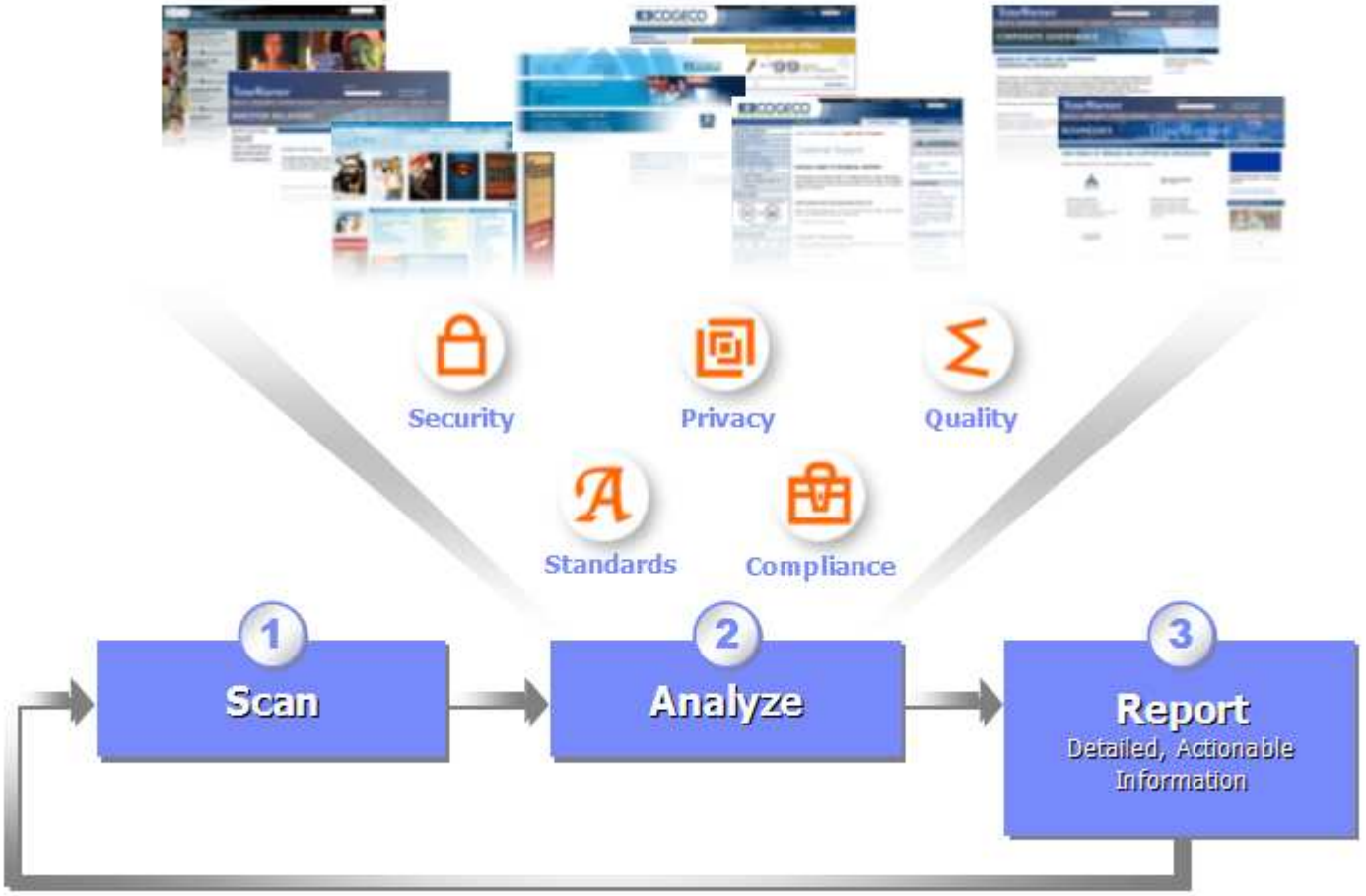
Cross-site Scripting (XSS)

- Ataque que induz o navegador a executar um script malicioso
- A exploração bem sucedida permite ao hacker recuperar informações do usuário ou direcionar suas ações para outros site mal intencionados.
- 68% dos websites possuem alguma vulnerabilidade a ataques XSS
- Demonstração do XSS

Rational Appscan

O que é?

Solução para testes automatizados de vulnerabilidades e conformidade das aplicações Web que ajuda a reduzir riscos e custos associados às falhas de segurança e inconformidades



Rational Appscan

Atuação

- Appscan explora e testa as vulnerabilidades das aplicações web, submentendo-a a ataques diversos.

IBM Rational Appscan

- O que os desenvolvedores e testadores da minha organização sabem sobre segurança da informação?
- Eles têm meios de prevenir vulnerabilidades?
- Apesar de nosso investimento em segurança de rede, será que realmente estamos seguros?
- Ainda que esteja seguro hoje, tenho como garantir que não haverá falhas de segurança no futuro?

Parceria Tecnológica

E-MAIL: elson.oliveira@foton.la

Visite o sítio:

www.foton.la