Histórias de um Security Officer
Estudos de Caso

Reinaldo de Medeiros

CIO e Office Boy

Agenda – Estudos de Caso

- DLP – Data Loss Prevention e Espionagem Comercial
- Phishing – Análise e Investigação de um Artefato
- Gestão de Risco
- Análise Forense
- e-mail Surveillance
- Políticas e Procedimentos

O Meio Ambiente

- Empresa da Área de Varejo
- Período de 2003 a 2006
- 7.000 empregados (à época)
- > 350 Lojas (Sudeste, Sul, Centro-Oeste)
- 4 Áreas de negócios:
  - Lojas
  - Web
  - 0800
  - Atacado

A Equipe de Segurança

- Eu

O Logo

1º Caso - O Duende Verde

- DLP
- Saci/Curupira
- Homeopatia
- Lendas Urbanas
- Palmeiras se empenhar para dar o campeonato para o Corínthians

Cenário - Controles implementados

- Filtro Web (WebSense)
  - Bloqueio de WebMail
- Poucas portas abertas
- Alguns Dispositivos de I/O Bloqueados
  - USB (Hoje não creio que fosse possível...)
  - CD/DVD

OrangeBox
Monitoramento de e-Mail

- Requisitos
  - Sigilo
  - Política - Auditoria.
  - Ética
- 99,9% sexo, cerveja e *networking*
- Mas nos 0,1%...

Pegando o Duende Verde

- A placa de rede deu defeito...
- A máquina foi espelhada duas vezes
  - Uma foi detalhadamente escrutinada (*Archives* do Lotus Notes)
  - A outra Isolada e lacrada
  - Testemunhas

Chamado na Presidência

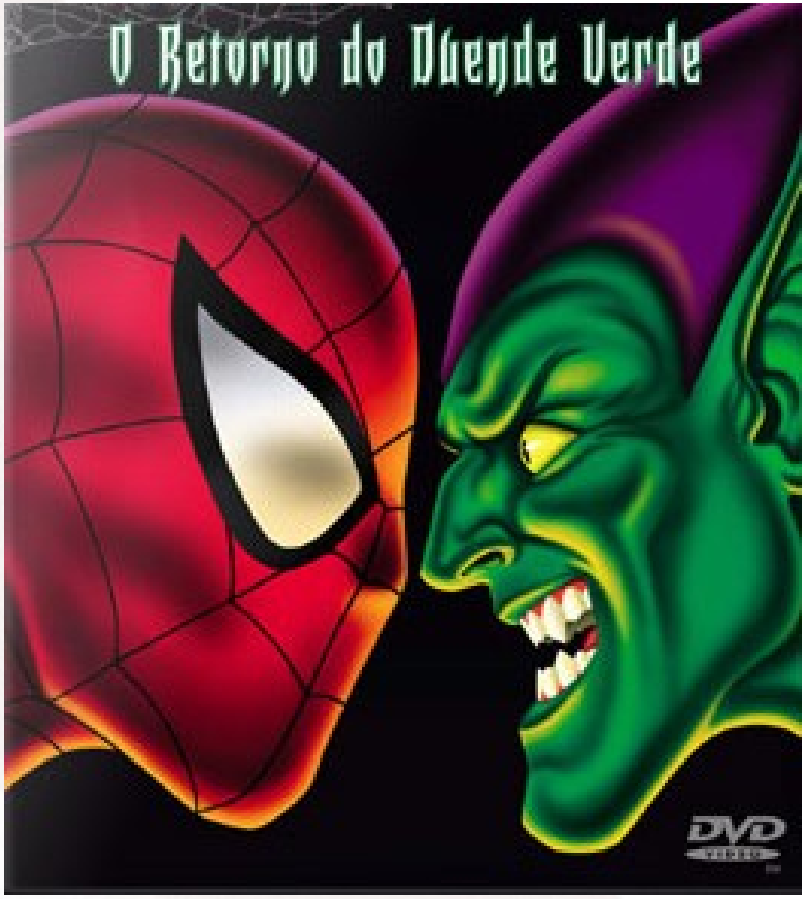
- Questionado, negou e jurou inocência.
- Então foi dado o flagrante na máquina dele.
- Justa Causa

Como o Universo não é Ético...

- O Duende Verde foi trabalhar na concorrência...
- Mas e empresa sofreu uma devassa fiscal e quase faliu...

LinkedIn

- Alguns meses depois o “Duende Verde” tentou contato no LinkedIn.
- Ignorei, claro



Tempos Depois...

- Depois de algum tempo, o diretor de TI me perguntou como andava o monitoramento da OrangeBox, respondi:
  - Só sexo, cerveja e *networking*... Nada relevante.
- No que ele retrucou:
  - Quero um relatório completo e detalhado...

2º Caso - Falha na DLP.

- Como não implementar o conceito de Proprietário da Informação.

Cenário da Implementação

- Sistemas mapeados
- Proprietários definidos
- Proprietários davam a última palavra sobre os sistemas

Resultado Prático

- O Diretor de uma linha de negócio (vendas em atacado) levou toda a base de clientes e produtos embaixo do braço.
- E montou um negócio de vendas para o Atacado concorrendo diretamente.

Reção Imediata

- Liminar
- Foresinc da Base de Dados
  - Dados iguais, inclusive os erros
- Processo

Solução Semântica

- Proprietário da Informação vs Gestor da Informação
- Política de Gestão de Dados
- “Gestor da Informação” segue normas de gestão
- Já o “Dono da Informação”...

Em Tempo:

- Faliram.
- Uma empresa que já nasce sem ética, não sobrevive no mercado atual.

3º Caso Análise de Risco – Maldito Sasser

- Arquitetura monolítica e “estável”
- A guerra entre os *patches* e a estabilidade do ambiente.

Ambiente de Loja - O Caldo de Cultura

- Windows XP Sem Patches
- Comunicação sem controle entre lojas
- Sem Antivírus
- Em tese, isolado do mundo real
- Lojas intercomunicando-se via *Frame Relay*
- *Servidores Linux*

Moral da História

- R$ 5.000.000,00 (aproximado) de prejuízo
- Salvo pelo relatório de risco
- Se você não consegue eliminar o risco, relate
- Seja chato
- Gestão de Risco é a coisa mais importante para a empregabilidade do Security Officer

4º Caso: Anatomia de um Phishing.

- Pena de Morte
- Sou contra.
- Exceto para *phishers* e *spammers*

O Phishing

- *Caro cliente Fulano de Tal, CPF nr xxxyyyy, sua compra foi efetuada com sucesso.*
- *Em breve estaremos debitando da sua conta o valor R$ 3.000,00...*
- *Se você não for o Fulano de Tal clique aqui...*

Reação - Primeira Noite

- SAC
- Site
- A busca pelo artefato

Segundo Dia

- Identificando o Phishing
- Montei o pior ambiente possível:
  - W98+Sem patch+IE4 + Linha discada
- Acesso ao Bradesco – Splash
- O Phishing como cortina de fumaça.

Ethereal (WireShark)

- O melhor canivete suíço para tráfego de rede
- God Save *“Follow TCP Stream”*
- *Bankers* deveriam criptografar a transmissão das senhas
- A captura da senha e IP do servidor ftp
- A curiosidade é difícil de conter!!
- E perdi a segunda noite...

A há!! - Peguei Agora...

A Ida ao Servidor


fotos_inicial.jpg


Imagem 001.jpg


Imagem 002.jpg


Imagem 003.jpg


Imagem 004.jpg


Imagem 005.jpg


Imagem 010.jpg


Imagem 011.jpg


Imagem 013.jpg


Imagem 014.jpg


Imagem 015.jpg


Imagem 018.jpg


Imagem 022.jpg


Imagem 024.jpg


Imagem 025.jpg


Imagem 028.jpg


Imagem 029.jpg


Imagem 030.jpg


Imagem 031.jpg

Imagem 033.jpg


Imagem 034.jpg


Imagem 035.jpg


Imagem 036.jpg


Imagem 037.jpg


Imagem 039.jpg


Imagem 040.jpg


Imagem 041.jpg


Imagem 042.jpg

logo.JPG

logo_war.gif

war_logo.jpg

A Ida ao Servidor


andre e keide.jpg


Bruno.jpg


cebolinha.jpg


Chicaum.jpg


Dragon.jpg


gaucha.jpg


gaucha1.jpg


glaucio.jpg


historia_012.jpg


Jack.jpg


jmmy e dnamiti.jpg


jmmy e namorada.jpg


k palhacinha.jpg


kzada.jpg


kzada e familia.jpg


lamb sal.jpg


Leandro.jpg


mini.jpg


Nilson.jpg


outro lamb.jpg


P5261723.JPG


P5261742.JPG


P5261746.JPG


trio.jpg


Vinicius.jpg

E aí?

- A bronca do amigo
- Coincidência ou não, tinha lá um *user_password.php e login.php*
- Relatório para o Jurídico
- E o que aconteceu?
- Não sei
- Falta um canal centralizado de interlocução direta com a polícia.

Obrigado

- Reinaldo de Medeiros
- reinaldo@entropiasecurity.com
- reinaldo@reinaldo.org
- Skype – ReiMed
- Twitter: ReiMedeiros
- 21 8129-1545

Entropia Security