Pedro Quintanilha

Perimeter Security

EDS do Brasil

Av. Goiás, 3353

09550-051 - São Caetano do Sul - SP - Brasil

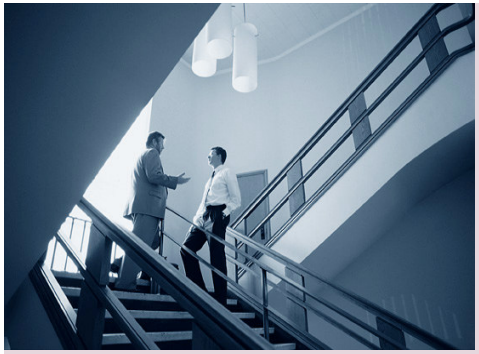
pedro.quintanilha_eds@abril.com.br

RESUMO

A quebra da confidencialidade de informações críticas, gerada por iniciativa interna ou externa, é um risco com o qual muitas instituições convivem, sem porém utilizar estratégias específicas para mitigá-lo.
Esta apresentação visa identificar os riscos mais comuns associados à Evasão de Informações, e descrever técnicas de dissuasão, detecção, bloqueio, e rastreio, esclarecendo aquelas hoje utilizadas, e sugerindo conceitos para futuras implementações.

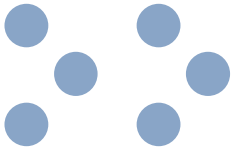
Evasão de Informações

Pedro Quintanilha

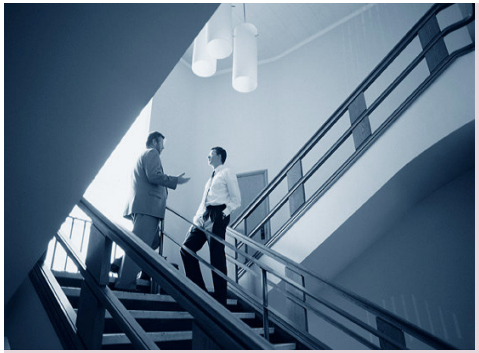


Evasão de Informações

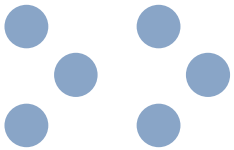
- Meios
- Aspectos Econômicos
- Aspectos Legais
- Dissuasão
- Detecção, Bloqueio e Rastreio
- Problemas
- Conceitos Propostos



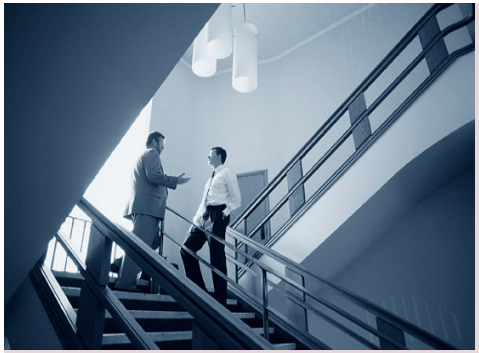
Meios



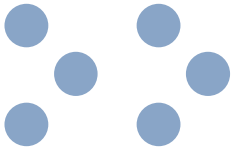
- Por ação pessoal
- Por falha humana
- Por falha no controle de acesso
- Vírus/Worms/Trojans



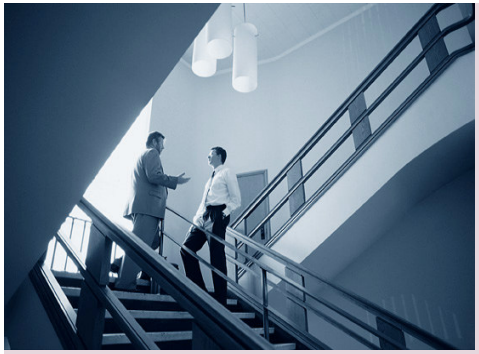
Aspectos Econômicos



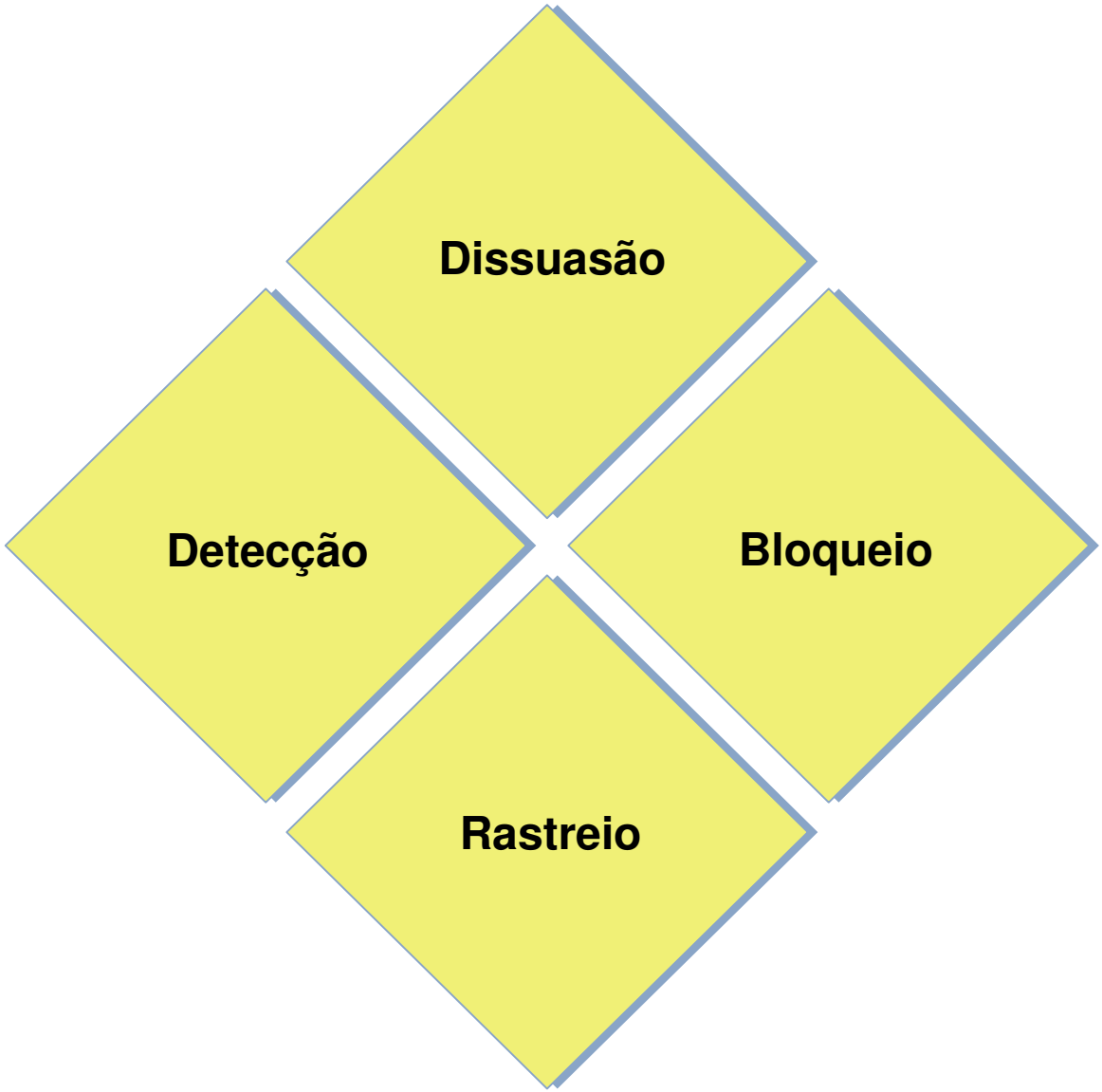
- Prejuízo Imediato
- Desvantagem Estratégica
- Segurança Estrutural
- Imagem

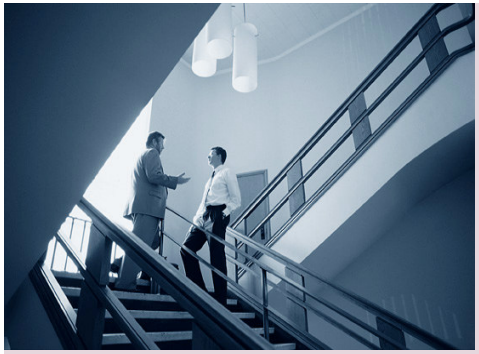


Aspectos Legais



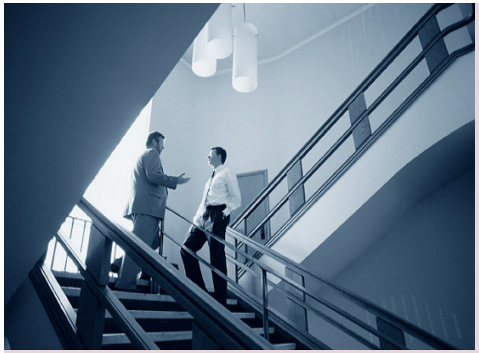
- # Direitos e Deveres Legais Relativos ao Sigilo
- # Artigo 8 da Instrução CVM Nº 358
  - "**Cumpre aos** acionistas controladores, diretores, membros do conselho de administração, do conselho fiscal e de quaisquer órgãos com funções técnicas ou consultivas, criados por disposição estatutária, e **empregados da companhia, guardar sigilo das informações** relativas a ato ou fato relevante às quais tenham acesso privilegiado em razão do cargo ou posição que ocupam, até sua divulgação ao mercado, **bem como zelar para que subordinados e terceiros de sua confiança também o façam**, respondendo solidariamente com estes na hipótese de descumprimento."
- # Artigo 482 da CLT
  - "Constituem justa causa para rescisão do contrato de trabalho pelo empregador:
    - g) violação de segredo da empresa"
- # Artigo 154 do Código Penal
  - "Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem"





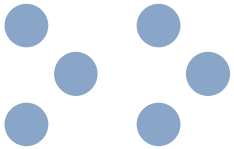
Dissuasão

- Termo de Confidencialidade
- Código de Conduta
- Percepção de Segurança
  - Política de Segurança
  - Classificação de Informações
  - Controle de Acesso
  - Ações de Conscientização
- Ações Administrativas (*post factum*)
- Evasão Consentida
  - Descrédito
  - Identificação do Autor

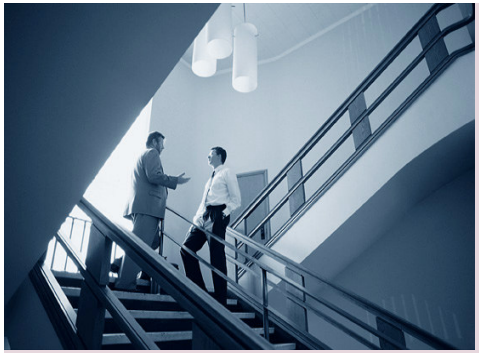


Detecção, Bloqueio e Rastreio

- *Honeytokens*
  - Inconsistências Propositais
- *Watermarks*
  - Inserção de Identificadores



Exemplos



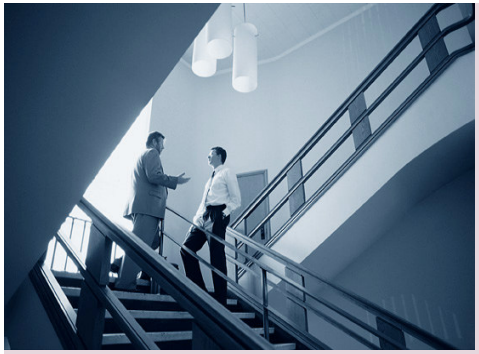
Falhas Personalizadas em Textos

Ata enviada para o Diretor 1

...e assim, por decisão unânime do Comitê, dá-se por aprovada a aquisição da empresa INGA CALAFETAGEM LTDA e suas subsidiárias em todo território nacional, de acordo com...

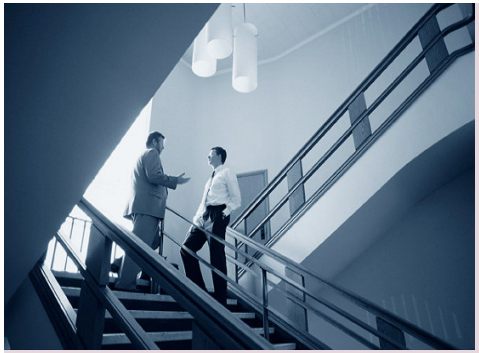
Ata enviada para o Diretor 2

...e assim, por decisão unânime do Comitê, da-se por aprovada a aquisição da empresa INGA CALAFETAGEM LTDA. e suas subsidiárias em todo território nacional, de acordo com...



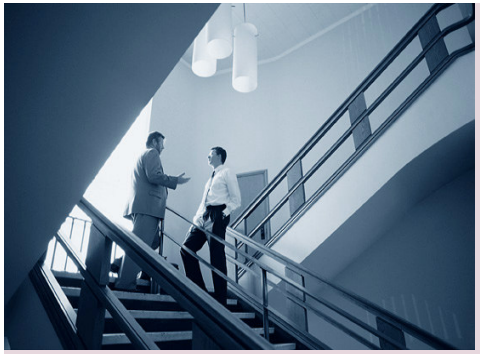
Entradas em *Data-Bases*

NOME	ENDEREÇO	COMPL	BAIRRO	CEP	SALARIOBASE
JOSE FERREIRA DOS SANTOS	RUA SANTA JOSEFINA	1433 AP 18	VILA MAICA	04828001	1433,23
MARIA APARECIDA ANDRADE	RUA DAS AMPOLAS	428 CASA 5	JESUS MENINO	<NULL>	438,95
NIVEA MARIA PEREIRA ROCHA	RUA VIRGULINO FERREIRA	234	SAPOPEMBA	05383000	2348,45



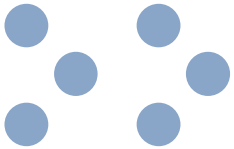
Marcas Esteganográficas

Processo 4228
ENV KXV TRAT DIG IMG
20041402

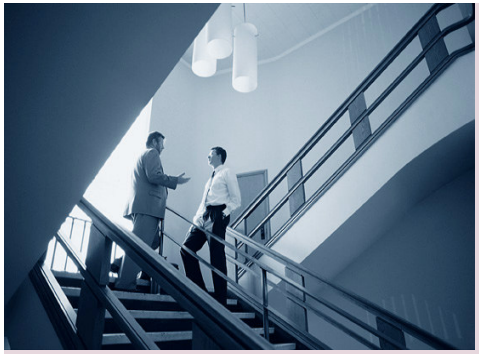


Detecção, Bloqueio e Rastreio

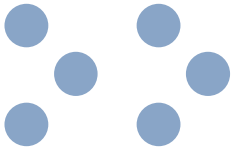
- Utilização de *IDS* (*ID²S - Information Disclosure Detection System*)
- Detecção dos *Honeytokens* ou de suas Características
- Bloqueio Parcial
  - Terminação de Sessões
  - Interação com Instrumentos de Bloqueio
- Alarme e Registro
  - Resposta a Incidente
  - *Trace-Back*



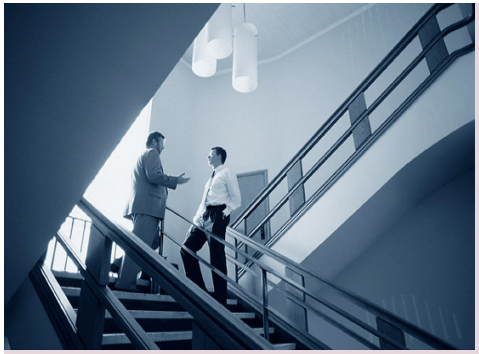
Problemas



- Detecção quando:
  - Encriptado
  - Comprimido
  - Alterado
  - Fragmentado
- Recuperação para *Trace-Back*
- Mídias Não-Digitais

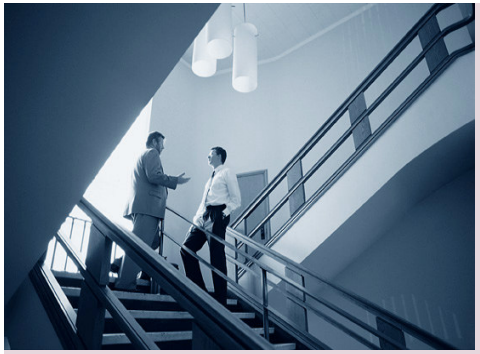


Conceitos Propostos



Assinaturas Digitais

- Agentes Especialistas Distribuídos
- *CRC*/*Checksum*
- Data-Base Dinâmico de Assinaturas e Agentes de Detecção em *Gateways* (*HTTP*/*FTP*/*SMTP*)



Classificação Bayesiana

- Detecção de Fragmentos (*ad similio*)
- Palavras-Chave
  - 5 a 8 caracteres
  - Valores Numéricos
- ID²S
  - Tráfego
  - Gateways
  - Agentes (mais invasivo)

Perguntas

Leitura Recomendada

- http://www.temporeal.com.br/downloads/honeypots_e_honeytokens.ppt
- http://www.securityfocus.com/infocus/1713
- http://www.cs.ucsb.edu/~wkr/publications/acsac03bayes.pdf
- http://www.paesdebarros.com.br/2003_02_23_arqartigos.html