Segurança e auditoria de sistemas

Professor Emiliano S. Monteiro

Engenharia Social

- É uma forma de ataque (levantamento de informações, pré-ataque).
- Ela depende muito da interação humana.
- Envolve a manipulação de pessoas para que burlar procedimentos normais ou dispositivos de segurança.
- Os atacantes usam técnicas para esconder suas identidades e motivos .
- Sempre se apresentam como um indivíduo confiável.
- O objetivo é influenciar, manipular ou enganar legítimos usuários.
- Os usuários uma vez enganados são levados a fornecer informações que posteriormente serão usadas para um ataque.
- A engenharia social é uma prática popular entre atacantes.
- É mais fácil explorar o lado “bom” e “solícito” das pessoas que ficar batendo em um firewall.
- É uma das primeiras etapas para se montar um ataque.
- Umas das formas de proteção é a conscientização e treinamento sobre segurança.

namp 127.0.0.1

Engenharia social!

Vuln → exploit
Leak test Firewall

Engenharia Social

Como funciona a engenharia social

1º passo, pesquisas de reconhecimento e levantamento de dados sobre o alvo. Estrutura, filial, telefones, setores, nomes de funcionários listas de emails, parceiros de negócio, ocorrências em jornais públicos e mídia privada, detalhes de operações internas, revirar o lixo da empresa, etc.

2º passo detectar comportamento padrão de funcionários de baixo escalão.

3º passo scanear perfils em mídias sociais.

4º passo planejar o ataque.

Tipo de abordagem, discurso aplicado, lista de pessoas com quem vai falar e citar como referência, etc.

Engenharia Social

- Baiting: o atacante deixa um pendrive (por exemplo) para ser localizado pela vítima em local de fácil acesso (sob uma mesa).
- Phishing: o atacante envia emails fraudulentos se passando pro algum email de fonte segura, geralmente contendo um malware ou link para um site de terceiro.
- Pretexting: o atacante se passa por um funcionário para coletar informações de funcionários desavisados confirmando dados para futuros acesso.
- Furto/Roubo de redirecionamento: Os atacantes alteram endereços de entregas para que as empresas de logísticas enviem os pacotes para o local errado.
- Entrada em prédios seguindo carona em usuários autorizados.
- Espiar usuários digitar senhas de acesso.
- Etc...

Engenharia Social

PS/2

DB9

Engenharia Social

Uma forma de combate a engenharia social é pelo uso de treinamento regular e campanhas de conscientização.

Os funcionários devem saber como se portar ao telefone ou em atendimento com terceiros (público externo e interno).

Gateways de email e firewalls de conteúdo combinados com vacinas ajudam a capturar os “ajudantes virtuais” dos hackers (malwares que são enviados via email).

Estações de trabalho devem ter vacinas configuradas para scanear mídias removíveis assim que estas são conectadas.

Estação de trabalho com porta usb desabilitada.

Desktop virtual.

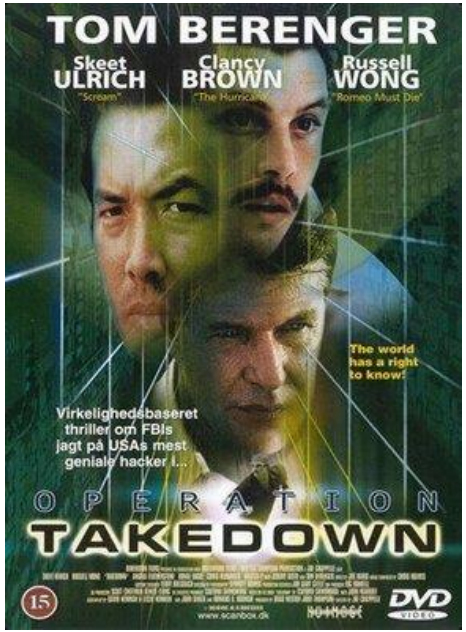
Engenharia Social

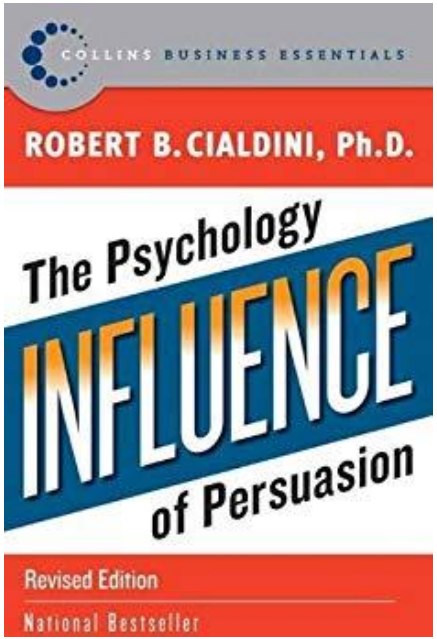
Motivadores para as pessoas (o Dr. Robert Cialdini publicou “Influência: A Psicologia da Persuasão” em 1984), segue alguns:

1. Reciprocidade.
2. Agir como os outros.
3. Compromisso com os demais.
4. Autoridade.

Entre outros...

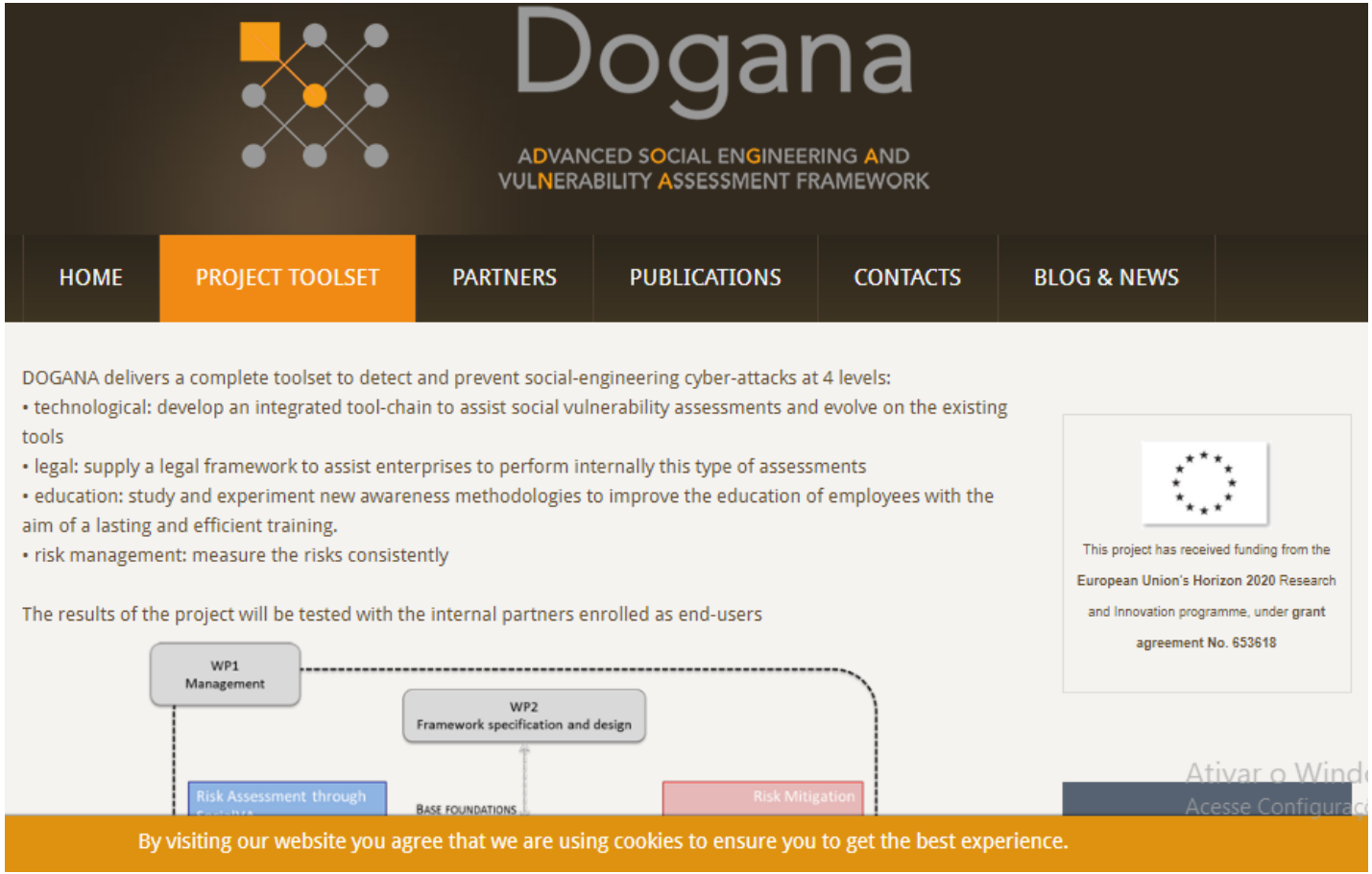
Engenharia Social



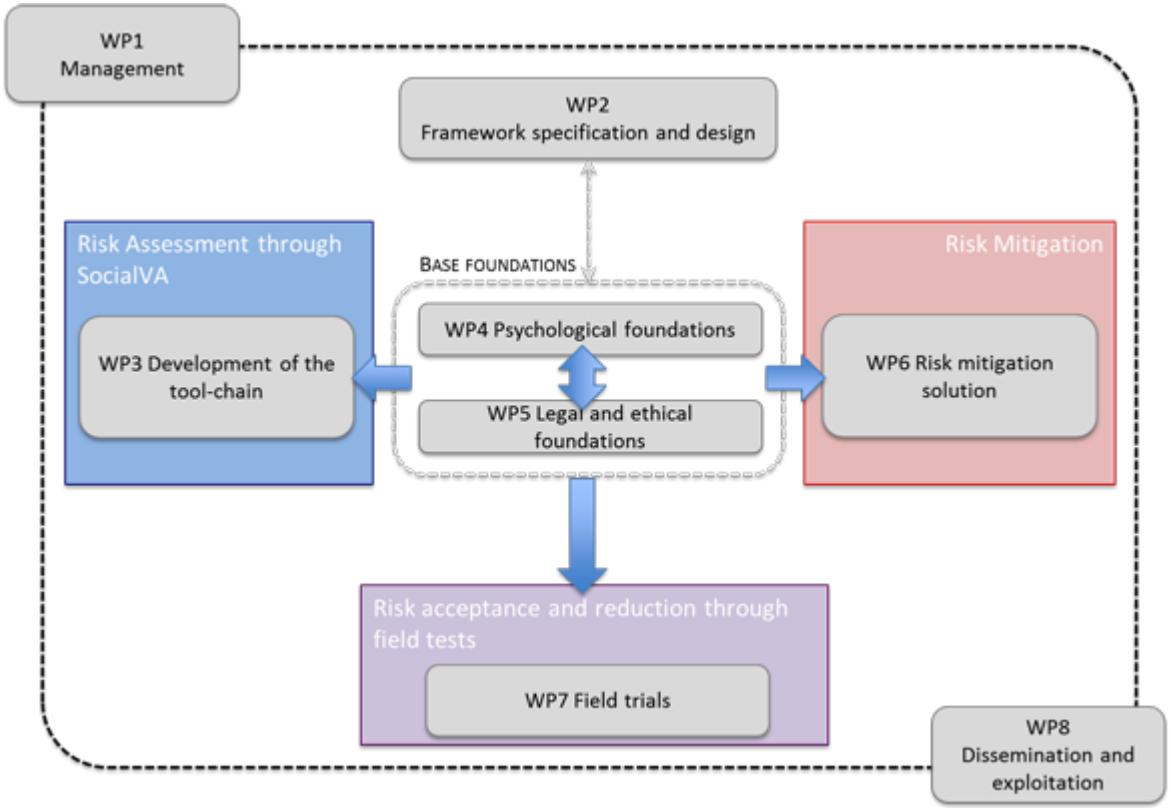


Filme: Caçada virtual

Engenharia Social

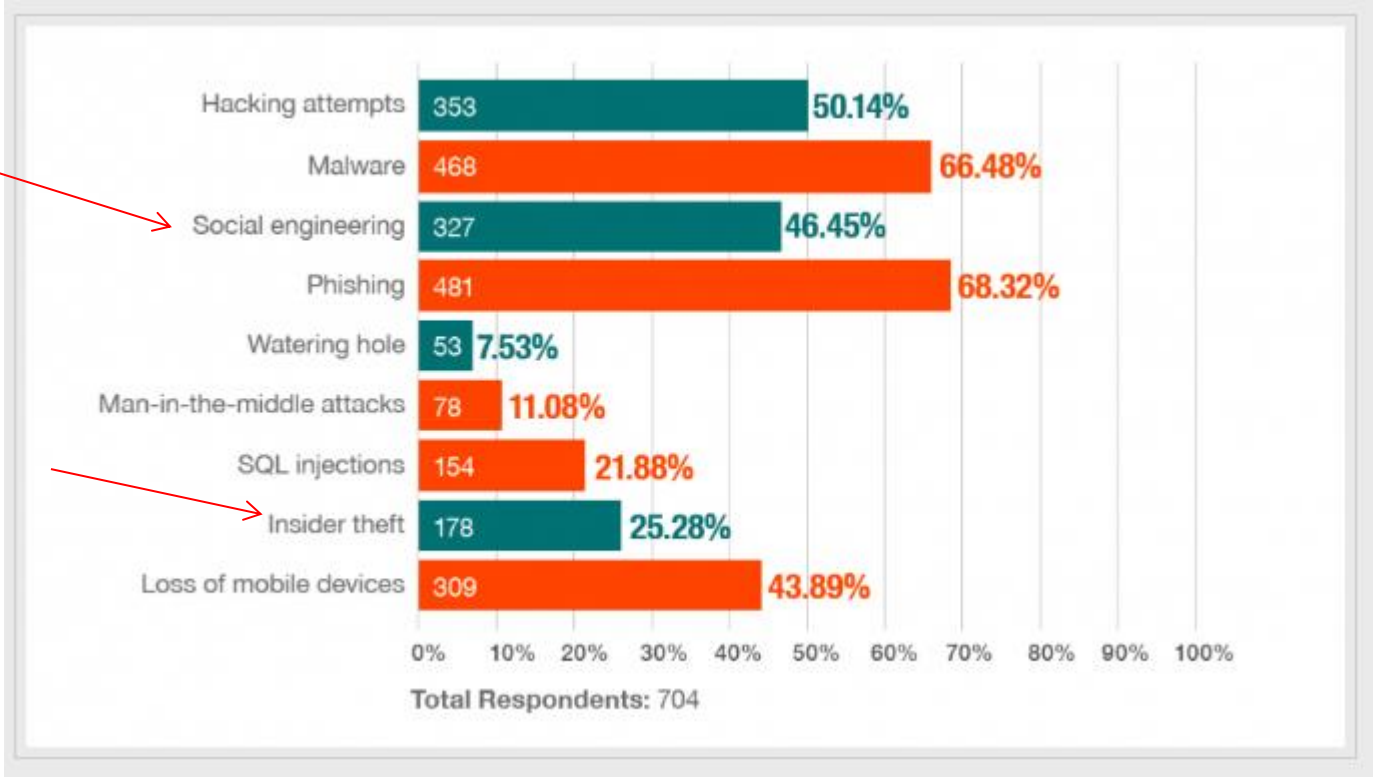


Engenharia Social



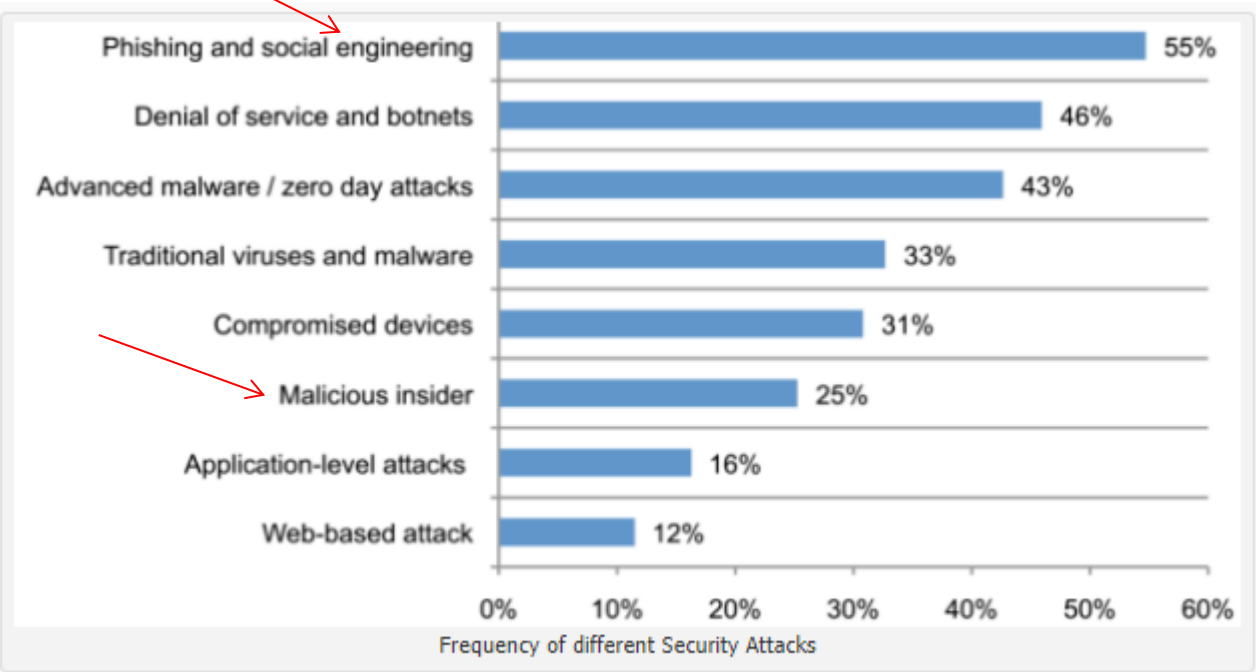
Engenharia Social

RSA Cybercrime 2015 report



https://project-sparks.eu/social-engineering-attacks-and-the-smart-grid/

Engenharia Social



Courtesy: http://securitywize.com/the-risk-of-an-uncertain-security-strategy/1430

Plano de Contingência.

- Um plano de contingência é RECEITA de atividades desenhada para ajudar uma empresa a reagir a um evento que pode ou não acontecer.
- É frequentemente chamado de “plano B”.
- É uma alternativa ao que cenários futuros desejados ou não.
- Possui uma série de ações que devem ser desenvolvidas para garantir a de continuidade do negócios (via recuperação de desastres e gerenciamento de riscos).
- Um padrão amplamente aceito é NIST 800-34.

Plano de Contingência.

Passos:

1. Desenvolver uma política que estabelece o plano de contingência dentro da empresa.
2. Conduza a análise de impacto nos negócios (BIA) para identificar as vulnerabilidades.
3. Identifique os controles e medidas para reduzir danos.
4. Nomear equipe e pessoal para cada parte do plano.
5. Desenvolver o plano de contingência para setor da organização (não apenas para a área de TI).
6. Testar o plano.
7. Manter o plano atualizado contra novas ameaças.

Exemplo de controle: Firewall ou Catraca
Medida/política: acesso a determinado site não é permitido.

Plano de Contingência.

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

CSRC

PUBLICATIONS

SP 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Date Published: May 2010 (Updated 11/11/2010)

Supersedes: SP 800-34 Rev. 1 (May 2010)

Author(s)

Marianne Swanson (NIST), Pauline Bowen (NIST), Amy Phillips (BAH), Dean Gallup (BAH), David Lynes (BAH)

DOCUMENTATION

Publication:

SP 800-34 Rev. 1 (DOI)

Local Download

Supplemental Material:

Plano de Contingência.

Medidas

Ativos	QUANTO TEMPO É POSSÍVEL FICAR SEM...	QUAL O IMPACTO DE FICAR SEM...	QUAIS AS VULNERABILIDADES....	O QUE FAZER EM CASO DE DESASTRE...
EQUIPAMENTOS				
EDIFICAÇÕES				
PESSOAL				
MATERIA PRIMA				
SISTEMA DE COMUNICAÇÃO				
SISTEMA DE TRANSPORTE				

Plano de Contingência.

Exemplo de partes

1 INTRODUÇÃO
1.1 Objetivo
1.2 Alvo ou onde será aplicado
1.3 Escopo
1.4. Aprovado por
2 OPERAÇÕES
2.1 Descrição do Sistemas
2.2 Responsabilidades
3 PLANO DE NOTIFICAÇÃO → Celular instituicional
4 OPERAÇÕES DE RECUPERAÇÃO
5 RETORNAR ÀS OPERAÇÕES NORMAIS

Planejamento pós-ataques (incidente)

1. Toda e qualquer atividade suspeita já deverá ter sido percebida pelos sistemas de detecção de intrusão ou logs (de firewall)
2. A atividades suspeitas devem ser relatadas ao gerentes de TI.
3. Verificar o nível de severidade do ataque é relacionar as medidas possíveis que poderão ser tomadas.
4. Isolar a área atacada (cadeia de custódia).
5. Acionar os servidores de backup.
6. Acionar o departamento jurídico da empresa para avalia a situação e decidir se as autoridades competentes devem ser alertadas.
7. Se necessário alertar o provedor.
8. Verificar sistemas de logs.
9. Verificar se sistemas de acesso e senha foram ou não comprometidos.
10. Tentar identificar e esboçar a anatomia do ataque e perfil do atacante (modus operandis)
11. Tentar rastrear junto ao provedor de acesso os caminhos tomados pelo atacante.
12. Registrar todas as medidas tomadas para resolver o problema.

Documentação e ações relativa à segurança

Metodologia para projetos de segurança:

1. Levantamento de Campo (é a rede da empresa!)

Deverá ser realizado para possamos mapear a rede. Caso já exista um desenho da rede, fazer um novo levantamento não fará mal. Os principais passos são:

1.1. Detectar ativos e passivos da rede (port scanner e host scanner, identifcação visual))
1.2. Montar um mapa da rede (Cisco config maker, zabbix, Nagios, NetCracker 3.0)
1.3. Identificar pessoal técnico
1.4. Identificar hardware e software

Documentação e ações relativa à segurança

2. Levantamento da utilização da rede.

É feito, mediante uma análise de trafego e com uma consulta usuários. Nem sempre os usuários falam para que estão usando a rede, Realizar os seguintes passos:

2.1. Descobrir o tamanho da comunidade de usuários
2.2. Contas ativas e desativadas
2.3. Aplicativos mais usados e menos usados
2.4. Serviços de rede mais usados e onde
2.5. Criar matriz Recursos X Pessoal
2.6. Sub-redes com maior trafego e de que tipo
2.7. Criar mapa de trafego
2.8. Detectar máquinas com portas abertas (de serviços), e hardware não utilizado
Cartão PCMCIA (MODEM ou placa de rede)

Documentação e ações relativa à segurança

3. Análise de vulnerabilidade

Nos permite, após localizar os servidores da rede tentar achar que computadores possuem problemas e de que tipo, o mesmo vale para as máquinas usadas pelos usuários. O resultado disto é uma relação de problemas encontrados dentro de nossa rede interna (problemas de software). Realizar os seguintes passos

3.1. Rodar um scanner de portas em servidores
3.2. Rodar um scanner de portas em clientes
3.3. Detecção de versão e coleta de dados de vulnerabilidade para o sistema em uso
3.4. Inventário de softwares (exemplo belarc, System Center Configuration Manager)
3.5. Criar tabela contendo os softwares em uso, versão e os patches/services packs utilizados
3.6. Usar softwares para achar vulnerabilidades em clientes
3.7. Usar força bruta em bancos de senhas, servidores, etc

Documentação e ações relativa à segurança

4. Classificar máquinas e sub-redes

Realizar uma classificação de Recursos da rede, o critério de classificação pode ser determinado pela própria empresa.

Criar um mapa ou diagrama (usando ícones) onde representamos máquinas mais importantes, perímetros de segurança, firewalls, máquinas com problemas, usuários públicos (convidados), máquinas de monitoração, etc

5. Correções

Uma vez detectadas as falhas no sistema é hora de corrigi-las, más atenção alguns servidores simplesmente não podem ser desligados, o mesmo vale para as máquinas dos usuários, algumas devem sofrer manutenção a noite e outras nos finas de semana, passos que deverá seguir são:

5.1. Aplicar correções em hardware defeituoso

5.2. Aplicar correções em softwares com problemas ou desatualizados

Documentação e ações relativa à segurança

6. Auditoria e Monitoração

A auditoria lhe permitirá saber quem fez o que uma vez que o evento tenho ocorrido, já a monitoração permite saber o que está acontecendo durante o evento. A monitoração lhe dá dados atualizados em períodos de tempos regulares e mostra sua rede (ou serviços) em “tempo real”. A auditoria serve para esclarecer questões relacionadas a eventos que já passaram e que queremos mais detalhes sobre eles. Recomendamos as seguintes atividades:

6.1. Montar um cronograma de Auditoria
6.2. Montar um cronograma de Monitoração
6.3. Montar um plano de Backup

Spice Works
Ground Works
Iris SolarWinds (vuln)

Sobre o uso correto dos sistemas

1. Sobre a internet: como os usuários devem usar a Internet, que sites devem ou não visitar
2. Sobre o uso da intranet: Que partes do sistema que está na Intranet é público? Que partes somente um determinado grupo de usuário pode acessar?
3. Sobre o uso do hardware:
4. Os usuários podem vir trabalhar com notebooks próprios?
5. Eles ganham notebooks da empresa?
6. Como podemos garantir que seus notebooks não serão roubados e os dados também?
7. Os funcionários podem levar disquetes para trabalhar em casa?
8. Os funcionários podem trazer HD, Palms, CDs e Pendrives, seus e de terceiros para dentro da empresa?
9. Os funcionários tem permissão para concertar o próprio hardware?
10. Sobre o uso dos sistemas internos da empresa: Quem usa que sistema?
11. sobre o uso do email coorporativo: todos tem acesso ao email? É um sistema Notes, MS Exchange ou x.400?
12. É permitido o tráfego de piadas?
13. Sobre o uso do acesso remoto: existe acesso remoto a intranet? Por quem? A que horas? De que cidade?

Documentação e ações relativa à segurança

Classificação do uso da informação

É criada uma tabela que classifique os dados de acordo com os seguintes critérios:

a) valor da informação para a empresa

b) tipo de proteção necessária

c) tempo de guarda

Documentação e ações relativa à segurança

Exemplos de use da classificação da informação :

1. TopSecret: planos de expansão, investimentos, parcerias secretas, ou qualquer informação que sua empresa considerar tão segura que se for exposta a espiões, concorrentes ou pública seria desastroso para a empresa!

2. Secreta: emails, qualquer informação que possa colocar a credibilidade e reputação da organização em dúvida ou em desvantagem competitiva frente a seus concorrentes

3. Interna: emails, comunicação interna da empresa, relatórios entre gerentes, etc

4. Setorial: emails, comunicação interna setorial, é o tipo de tráfego de dados que não deve trafegar por outros setores, como por exemplo informações exclusiva da gerencia ou informações exclusiva do setor de pessoal (CPF, folha de pagamento, etc)

5. Pública: De livre acesso a todos inclusive os que estão fora da empresa

Documentação e ações relativa à segurança

Sobre o tipo de proteção necessária:

1. Muito alta: Proteção muito forte, diversas soluções de hardware e software, inclusive segurança física
2. Alta: proteção forte um mix de soluções de software e talvez pelo menos um solução hardware
3. Média: de dois a três mecanismos de proteção
4. Pouca: um mecanismo de proteção
5. Nenhuma: nenhum mecanismo de proteção

Classificação de propriedade dos sistemas de informação:

Autor da informação: possui os direitos sobre propriedade intelectual.

Usuário: pessoa que não é o criador da informação más tem autorização para usá-la.

Tipos de usuário: depende do tipo de sigilo que a informação terá: o usuário pode apenas ler, pode ler e alterar, executar, distribuir, etc...

Documentação e ações relativa à segurança

Classificação dos tipos de riscos

1. Crimes cibernéticos: o atacante passou bom tempo tentando derrubar sua empresa ou roubar dados que ele poderá se aproveitar depois
2. Infrator : ele achou uma falha no seu site, não estava procurando nada de específico e decidiu aproveitar-se da falha
3. Acidentes: Devido a desconhecimentos operacionais os próprios funcionários podem cometer erros ao usar os sistemas da empresa e isto poderá provocar uma falha de segurança
4. Falhas de sistema: por falhas no sistema temos desde falhas de projeto que não previam a segurança até panes que podem comprometer a segurança

Documentação e ações relativa à segurança

Treinamento de usuários

1. Estipular treinamento para os usuários para informá-los sobre a informação da proteção da informação e sua importância para o devido funcionamento da organização.
2. Os usuários devem obrigatoriamente participar de um treinamento e palestras sobre conscientização sobre segurança.
3. Os usuários devem ser conquistados, pois se sentirem-se oprimidos podem se tornar futuros inimigos internos.
4. Alerta sobre responsabilidades e punições.
5. Cada reunião com os usuários deverá ser registrada.

Documentação e ações relativa à segurança

Documento aos empregados

1. Deverá levar em consideração os seguintes itens:
2. Porque a informação é importante
3. Uma descrição das informações sob responsabilidade desse funcionário
4. Deixar claro que determinadas informações são confidenciais e importantes para a continuidade dos negócios
5. Deixar claro que informações o funcionário não poderá tornar públicas e quais são as barreiras de trafego dessas informações dentro da organização (por exemplo: informações sobre salário devem circular apenas dentro de setor de recursos humanos)
6. Deixar claro sobre a responsabilidade do funcionário ao sair da empresa no final de expediente e sobre seu desligamento da empresa.
7. Procedimentos disciplinares, regras do jogo!

Observação: algumas empresas podem exigir que o funcionário assine uma renuncia de propriedade intelectual, isto as vezes é feito por empresas de tecnologia de ponto, tudo o que o funcionário criar durante sua estadia como funcionário da empresa é de propriedade da empresa!!