Segurança para Defensores de DH

junho - 2016

Segurança (definição 1)

- O que é segurança?
- Não existe segurança absoluta e nem vigilância total.
- Existirão programas de computador que nos ajudarão, mas o elemento humano é o central.
- Segurança é também uma forma de ver; é um "mindset" (mentalidade). Um processo, uma cultura, estado de espírito, enfim...

Segurança (definição 2)

Segurança é o oposto da paranóia!
Segurança é um procedimento para permitir a ação e não nos deixar imóveis.

Segurança (definição 3)

- Segurança é um trade-off: é uma troca e um balanço.

Segurança (definição 4)

A segurança é uma forma de prevenção.
Uma prevenção contra consequências adversas da ação intencional de outros.
Prevenir significa fazer **trocas** (abrir mão) de algumas coisas.
Fazer troca extrema é fácil:

- Quer evitar ser assaltado a noite na rua? Não ande na rua a noite!
- Quer evitar ser alvo de fraude de cartão de crédito? Não use cartão de crédito!
- Não quer ser preso na manifestação? Não vá na manifestação!

Segurança (definição 5)

Você estaria mais seguro se nunca saisse de casa, mas que vida é essa?

Aquilo que é trocado é que é importante, não a segurança absoluta.

Pela razão da segurança envolver trocas, mais segurança nem sempre é melhor.

Segurança (definição 6)

E há diferentes tipos de segurança.
Segurança da Informação (InfoSec)
Como as informações são transmitidas? Qual é o protocolo para comunicar um fato sensível?
Definição
Defender a informação de ser acessada (modificada, copiada, destruida) por agentes não autorizados. Pode ser tanto uma informação digital como física (papeis). Conceitos: Confidencialidade, Integridade, Disponibilidade, Não Repúdio.

Segurança (definição 7)

DigSec: Segurança digital. Ferramentas e programas que nos ajudam a transmitir ou armazenar uma informação de forma segura.

Segurança (definição 8)

Segurança Operacional (OpSec): tudo o que envolve o procedimento, o processo, a parte humana, o ato de realizar uma ação.

Definição

Uma informação ou ação aparentemente inútil/trivial obtida ou observada pela inteligência inimiga que quando agregada com outras é capaz de desarticular ou minar uma ação/organização. O conjunto de medidas tomados para evitar que essas informações sejam coletadas pelo adversário é chamado de OpSec.

Exemplo 1: você criptografou seu computador e seu email(infosec/digsec), mas foi almoçar e deixou seu computador ligado no escritório e sem senha. :D

Segurança (definição 9)

OrgSec: segurança organizacional
A segurança dos grupos parte do princípio que é praticamente inseparável da segurança na vida particular de seus/suas integrantes e a vida do grupo.
A falha de um membro pode colocar em risco toda a organização.

Segurança

Juntando tudo:
O desafio é: InfoSec + DigSec + OpSec + OrgSec.
Ou: como fazer um grupo todo acordar e consensuar uma política de segurança para implementar a segurança da informação e operacional utilizando ferramentas de segurança digital?
ou ainda: **como avaliar, fazer os acordos e implementar protocolos de segurança nas nossas próprias vidas e nos nossos grupos?**

Modelo de ameaças

Qual é o seu modelo de ameaça?
Princípio da segurança ativista: se você quer mudar o triste status quo, você terá adversários.
Contra quem ou o que você quer proteger sua organização?
Como sua organização investe os seus escassos recursos (tempo, dinheiro, pessoas. . .) para se proteger?

Modelo de ameaças (2)

Existem várias formas de fazer um modelo de ameaça.
Pode-se pensar centrado nos ativos, nos adversários,. . . .
mas isso geralmente é feito para softwares! E para organizações e pessoas?

Modelo de ameaças (3) - TRETA

Quatro entidades:
Ativos: tudo aquilo que é de valor para sua organização. No nosso caso, isso inclui o Staff!
Atacante (ou adversários)
Ataques (ou riscos/ameaças)
Mitigações (ou defesas)
TRETA ou ISO1312: - https://iso1312.fluxo.info/

Modelo de ameaças (4)

Exemplo da modelagem:
Ativo: plano de ação da organização
Atacante: a polícia
Ataque: obter informações sensíveis apreendendo, furtando ou espelhando o seu computador
Mitigações:

- Criptografia completa de disco nos computadores da organização.
- Não transferir/compartilhar esses documentos para armazenamentos não criptografados (“nuvem”, pendrives, hd externos)
- Se impresso, eliminar de forma segura.
- Se hospedado num hotel/conferência, usar um computador/dispositivo de viagem.

Ameaça e risco

No jargão dos profissionais de segurança há uma diferença entre **ameaça** e **risco**:
ameaça - potencial de um determinado ataque
risco - probabilidade de acontecer

Senso de segurança

A segurança é subjetiva e pode ser interpretada de forma diferente pelas pessoas, pois cada um determina seus próprios riscos e avalia suas trocas com diferente contramedidas.

- As pessoas exageram sobre casos espetaculares, mas subestimam os riscos comuns.
- Riscos personificados são mais percebidos do que riscos maiores anônimos - Stálin:"A morte de um é uma tragédia, a morte de milhões é uma estatística."
- As pessoas subestimam riscos que voluntariamente aceitam e superestimam os riscos em situações que não controlam. (Carro vs avião)
- As pessoas são reativas às notícias do dia. Isso resulta em más decisões de segurança.
- Conclusão: as pessoas fazem suas decisões de segurança baseada na *percepção*(subjetiva) dos riscos e nos riscos reais. Isso resulta em más decisões.

Segurança é tomada de decisões

Como são tomadas as suas decisões de segurança?

- Custo (mais barato)?
- Tempo (demora menos)?
- Usabilidade (mais prático)?

E em quais situações é um processo consciente, ou seja, optamos por uma dada solução e sabemos as implicações dessa escolha?

Gestão de riscos

Gestão de riscos: não é possível eliminar todos os riscos, mas podemos reduzi-los a níveis gerenciáveis.
Exemplo: não podemos acabar com os riscos de furto no metrô, mas carregando a mochila na frente do corpo com o braço protegendo os bolsos, diminui a chance de ter a mochila aberta e furtada.
Você deve olhar para as probabilidades dos riscos e não no potencial da ameaça!

5 passos

1. O que queremos proteger?
2. Quais são os riscos daquilo que queremos proteger?

   - O que está sendo defendido?
   - Quais as consequências se tiverem sucesso?
   - Quem quer atacar?
   - Como querem atacar?

3. O quão boa é a solução segura para mitigar esses riscos?
4. Quais os outros riscos que a solução segura causa?

   - Os novos problemas devem ser menores que os anteriores.

5. Quais são os custos e as trocas que a solução impõe?

Em outras palavras: O benefício da mitigação dos riscos (**3**) vale os riscos adicionais(**4**) e mais as outras trocas (**5**)?

5 passos (2)

Uma medida segura não se mede apenas pela eficiência, mas do que estamos abrindo mão.
Os **5 passos** não nos levam a uma resposta, mas permite **avaliar** uma proposta.

Reconhecimento de riscos

- Quais são os canais de comunicação em uso?
- Quais são os protocolos e procedimentos de segurança em uso? Quais são as suas vulnerabilidades ou limites?
- Como o grupo se organiza?

Dicas do que é importante para se resguardar:

- Grampos telefônico: https://grampo.org
- Anotações, atas, lista de inscritos, roubo de cadernos e documentos jogados no lixo.

Fim da parte 1

"Nunca escreva se você pode falar; nunca fale se você pode gesticular; nunca gesticule se você pode piscar."