
UNAERP
Universidade de Ribeirão Preto
Campus Ribeirão Preto · Campus Guarujá

Segurança da Informação

Tópicos Especiais em Engenharia

Novo Cronograma

17/04	Medidas de Segurança Físicas / Medidas de Segurança Técnicas
24/04	Medidas de Segurança Técnicas
01/05	**FERIADO**
08/05	Medidas de Segurança Técnicas (malware) + Organizacionais
15/05	Ataques
22/05	**AV1 - Lista de Exercícios**
29/05	Desenvolvimento Seguro
05/06	Desenvolvimento Seguro
12/06	**FERIADO**
19/06	Ferramentas
26/06	Ferramentas
03/07	**AV2**

Maior Dúvida

- ✘ Como funcionam os antivírus e antimalware? e porque alguns não são reconhecidos na varredura?
- ✘ Em relação aos malwares, qual a diferença da vulnerabilidade de cada SO? Dizem que o linux e macOS são mais seguros que o windows, que não pegam vírus. Quão verdade é esta afirmação? E os smartphones, ios e android? São também vulneráveis aos malwares?
- ✘ Como saber qual o melhor tipo de criptografia para cada caso? Existe algum critério utilizado para ajudar na escolha de como criptografar as informações?

Medidas de Segurança Técnicas

Proteção contra códigos maliciosos (malwares)

Continuação...

Tipos de Malware – Bot

- ✘ Dispositivo infectado se comunica com invasor
- ✘ Execução de comandos remotamente
- ✘ Processo de infecção e propagação parecido com worms
  - se propaga automaticamente

Tipos de Malware - BotNet

- ✘ Rede de computadores zumbi (bots)
- ✘ Ataques em massa
  - Negação de Serviço Distribuída (DDOS)
- ✘ Roubo de informações e envio de SPAM
- ✘ Mirai Botnet (2016)

Tipos de Malware - Backdoor

- ✘ Forma de acessar um software contornando os controles de segurança. Ex: entrar sem autenticação
- ✘ Pode ter uso legítimo.
  - Tratamento de erros
  - Atacantes podem explorar backdoor existentes
- ✘ Vírus e outros malwares tentam criar backdoors

Tipos de Malware - RootKit

- ✘ Conjunto de aplicações que garantem acesso contínuo do atacante ao dispositivo (computador) comprometido
- ✘ Remove evidências da invasão (logs)
- ✘ Instala outros malwares (backdoor)
- ✘ Mapeiam vulnerabilidades

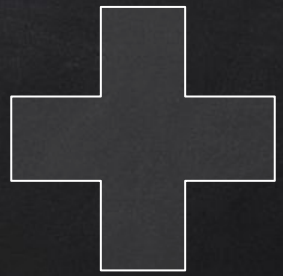
Tipos de Malware – RansomWare

- ✘ Sequestro de Dados
- ✘ Com técnicas de criptografia, bloqueia acesso aos arquivos e exige um resgate
- ✘ 2017 – WannaCry 300.000 computadores afetados

Como se proteger?

Proteção

Software Antivírus
Antimalware



Conscientização
dos usuários

Anti Malware / AntiVírus

Como funcionam os Anti Malwares

- ✘ Escaneamento no acesso
- ✘ Escaneamento Total do Sistema
- ✘ Definições de vírus
- ✘ Heurísticas
- ✘ Falso Positivo

Conscientização do Usuário

- ✘ Reconhecer códigos maliciosos
- ✘ Importância de utilizar antivírus
- ✘ Reportar suspeitas de ataques

Medidas de Segurança Organizacionais

Medidas Organizacionais

- ✘ Controles administrativos (organizacionais) que complementam e dão suporte aos controles técnicos
- ✘ Garantir comunicação das regras de *SegInfo*
- ✘ Revisão periódica dos controles administrativos
  - políticas, normas, processos e procedimentos
- ✘ Pessoas geralmente são um dos controles mais valiosos para *SegInfo*

Segurança em R.H.

- ✘ Controles de segurança acompanhem ciclo de vida de colaboradores e terceiros
  - Seleção
  - Contratação
  - Trabalho
  - Desligamento

Segurança em R.H.

- ✘ Funcionários, terceiros e fornecedores compreendem seus papéis e responsabilidades
  - documentados na P. S. I.
- ✘ Responsabilidades pela SegInfo são determinadas antes da contratação
- ✘ Candidatos ao emprego, terceiros e fornecedores são analisados
- ✘ Todos usuários concordam/assinam termos de responsabilidade

Conscientização

- ✘ Assegurar que os colaboradores conheçam as regras de SegInfo adotadas pela empresa
- ✘ Sejam capacitados para lidar com ameaças e riscos

Conscientização e Treinamento

- ✘ Processo formal de introdução da PSI
- ✘ Requisitos de S.I e responsabilidades legais
- ✘ Uso correto dos recursos que manipulam informações
- ✘ Sanções, processo disciplinar e punições
- ✘ Adequados e relevantes para papéis do colaborador
- ✘ Periodicidade

Conscientização

- ✘ Estabelecer metas e objetivos realistas
- ✘ Desenvolver o programa e o treinamento
- ✘ Implementar o programa
- ✘ Monitorar a eficácia e melhorar o programa

Materiais de Conscientização

- ✘ Palestras
- ✘ Hotsite
- ✘ Banners/Folhetos
- ✘ Cartilhas
- ✘ Comunicados Oficiais
- ✘ Treinamentos
- ✘ Workshops

Sanções e Punições

- ✘ Verificar previamente evidências da violação da SegInfo
- ✘ Formalidade
- ✘ Tratamento justo
- ✘ Resposta de acordo com natureza e gravidade da violação
- ✘ Política de Segurança da Informação e Código de Conduta

Controle de Acesso Lógico

- ✘ Usuário correto acessa recurso correto no momento correto
- ✘ Triplo A
  - Autenticação
  - Autorização
  - Auditoria

Autenticação

- ✘ Confirmar a validade de usuário que solicita acesso a um serviço
- ✘ Identificação + Credencial
  - e-mail/login + senha/token/certificado digital

Autorização

- ✘ Nível de acesso de acordo com as regras da organização
  - Acessar E-mail?
  - Acessar Sistema de RH?
  - Acessar Sistema Financeiro?
- ✘ Princípio do Privilégio Mínimo

Auditoria

- ✘ Coletar ações de um usuário autenticado e autorizado
  - Acessos desnecessários
  - Acessos indevidos
  - Erros
  - Tentativas de Fraude

Política de Controle de Acesso Lógico

- ✘ Documento que define regras de acesso lógico aos recursos
  - Registro de Usuários
  - Cancelamento de Usuários
  - Gerenciamento de Usuários Privilegiados (superusuários)
  - Revisão de Acessos
  - Tratamento de acessos conflituosos
  - Ajustes nos acessos

Classificação da Informação

Valor, Requisitos Legais, Sensibilidade e Criticidade

Controles adequados a sua proteção

Classificação da Informação

- ✘ Pública
- ✘ Uso interno
- ✘ Confidencial

Classificação da Informação

- ✘ Nível de classificação
  - Pública, Interna ou Confidencial
- ✘ Rotulagem, independente do formato
- ✘ Responsável pela classificação
- ✘ Manuseio seguro
- ✘ Descarte

Atividade

- ✘ Definição de Gestão de Continuidade de Negócios (GCN)
- ✘ Importância da Segurança da Informação na GCN
- ✘ Individual
- ✘ Máximo 2 páginas
- ✘ Entregar até dia 15/05

DÚVIDAS?

- ✘ Não esqueça de enviar sua maior dúvida pelo link que está no ClassRoom.
- ✘ Críticas/Sugestões: ezarpelao@unaerp.br
- ✘ Próxima aula: Ataques

Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Photographs by Unsplash