PROFESSOR : EWANDRO LIMA

DISCIPLINA: INFORMÁTICA

SEGURANÇA DA INFORMAÇÃO

Parte da informática que estuda os métodos de proteção da informação contra o acesso por pessoas não autorizadas, seus princípios básicos são:

1. **DISPONIBILIDADE:** Determina que uma informação esteja disponível para acesso no momento desejado.
2. **INTEGRIDADE:** Determina que a informação não seja alterada no trajeto de origem até o destino.
3. **CONFIDENCIALIDADE/PRIVACIDADE**: Determina que a informação seja acessível apenas por pessoas autorizadas.
4. **AUTENTICIDADE:** Determina a identidade que quem está enviando os dados, este princípio gera o não-repúdio que implica que o emissor não poderá se esquivar da autoria da mensagem (irretratabilidade).

TERMOS RELACIONADOS A SEGURANÇA

1. FIREWALL: Conjunto de procedimentos de segurança na rede.
2. ENGENHARIA SOCIAL: Termo atribuído aos métodos utilizados por um invasor para obter informações de uma pessoa, computador ou sistema de forma irregular.
3. MALWARE: Programa malicioso, sua função é enganar o usuário.
4. CRACKER: invasor do sistema.
5. HACKER: usuário com conhecimento avançado em informática, também pode ser considerado como invasor do sistema.
6. HTTPS: As referencia “S” quando apresentada em um endereço, indica que a área utilizada é segura.

7. CRIPTOGRAFIA: codificação dos dados para proteger as informações, basicamente são de dois tipos:

•Criptografia Simétrica: Utiliza uma chave para encriptar e decriptar dados, tanto o remetente quanto o destinatário devem compartilhá-la.

•Criptografia Assimétrica: utiliza uma chave para encriptar e outra para decriptar dados, onde a chave publica é compartilhada e a chave privada fica com o autor, geralmente utilizada para um pequeno volume de dados.

8.CERTIFICAÇÃO DIGITAL: Certificado Digital é um documento eletrônico que identifica uma pessoa física ou jurídica e também servidores web (site seguro), quando emitido por Autoridade Certificadora credenciada, o certificado pode ser usado como assinatura digital com força de assinatura de próprio punho. Documentos que trafegam por meios eletrônicos, para possuírem reconhecimento legal, não mais precisam ser convertidos em papel, assinados com reconhecimento de firma dos signatários e enviados via postal, diminuindo custos.

9.ASSINATURA DIGITAL DSA (Digital Signature Algoritm): Procedimento em que o arquivo recebe a identificação do seu autor, sendo assim, o destinatário da informação receberá o arquivo sem que o mesmo tenha sofrido alterações no trajeto de origem até o destino.

10. BACKBONE: local de segurança onde se encontram os servidores dos sub-níveis da rede, esta área permite o gerenciamento mais seguro das informações e também aumenta a velocidade de transmissão de dados.
11. ADWARES: são softwares que exibem propagandas irregulares no seu computador.
12. SPYWARE (programa espião): programa com a função de verificar as informações de um determinado sistema e em seguida as envia para o invasor.
13. AD-AWARE/ANTISPYWARE: programas utilizados para remover e evitar a entrada de adwares e spywares.
14. BACKDOOR: Programa que permite o retorno do invasor a um determinado computador, equivale a “retornar a porta”
15. Spam: Mensagem não autorizada, geralmente seu conteúdo é de cunhocomercial ou pornográfico.

16. KEYLOGGER: é um programa registrador de teclado cuja função é registrar tudo que for digitado para capturar dados como números e senhas de cartão.
17. SCREENLOGGER: é um programa registrador de tela cuja função é obter as imagens do monitor no momento que você clica com o mouse, seu objetivo é capturar os dados da tela.
18. RANSOMWARE**:** Este software rouba ou bloqueia os dados do usuário e em seguida pede um “resgate” para devolver os arquivos.
19. SNIFFERS: Também chamados de “farejadores” são utilizados para monitorar as conexões e capturar as informações de seu interesse como as senhas dos usuários.

20. PORT SCAN (varredura de portas): Programa utilizado para descobrir os IPs de um ou mais computadores
21. IP SPOOFING (Falso IP) O IP spoofing consiste na troca do IP original do invasor por um outro, podendo assim se passar por outro computador.
22. PHISHING: Esta técnica permite o roubo das informações da máquina de um usuário, o mesmo é atraído por um falso link ou pagina criada pelo invasor.
23. PHARMING: consiste basicamente em modificar a relação que existe entre o nome de um site na Internet e seu respectivo servidor Web, ou seja, ao digitar um endereço o usuário é redirecionado para outro indicado pelo hacker.

24. IDS/IPS/VNC (Intrusion Detection System) Ferramenta de detecção de intrusão, tem como um dos objetivos principais detectar invasões ou se algum usuário da empresa está fazendo uso incorreto do mesmo.
25. WORM (verme) - são programas parasitas que se multiplicam, mas diferentemente dos vírus. Os worms podem criar um número indefinido de cópias de seus arquivos ou enviá-los para outros usuários (de sua lista de distribuição), são, em geral, propagados via chats.
26. VPN (Virtual Private Network): Rede Virtual Privada representa um canal de criptografia entre os pontos, sua função é elevar a segurança da conexão.
27. BIOMETRIA: Equipamentos cuja função é identificar um determinado usuário para que o mesmo tenha acesso ao sistema. Ex: Leitor de impressões digitais e mapeamento da íris para acesso.

28. TRACKWARE: são programas que tem a função de rastrear atividades do sistema e os hábitos do cliente e em seguida envia estas informações para terceiros, é geralmente associado aos Adwares.
29. HOAXES: Mentira, farsa com o objetivo de enganar usuários na rede.
30. ROOTKITS: Programa utilizado para esconder ou camuflar procedimentos maliciosos dos métodos de proteção e permitir acesso exclusivo a um computador e suas informações
31. DEEP WEB (Internet Profunda): termo atribuído a uma zona da internet que não é ser detectada facilmente pelos motores de busca comuns, gerando assim maior privacidade para seus usuários. Esta condição de anonimato e privacidade em muito casos favorecem as atividades ilegais.
32. DARK WEB (Internet Obscura): Parte mais profunda e restriva da Deep Web.

VÍRUS

Rotinas programáveis com a função de danificar arquivos ou alterar o funcionamento da máquina.

ANTIVÍRUS

Programa com a função de encontrar e remover um possível vírus do sistema.
EX: PANDA – AVG - AVAST – AVIRA - MALWAREBYTES

FORMAS DE CONTAMINAÇÃO

- Discos infectados
- Redes (locais, expandidas, intranet, internet, extranet etc...)

FORMAS DE PROTEÇÃO

- Utilizar programas antivírus
- Atualizar o antivírus
- Utilizar antivírus que possam executar a verificação do sistema automaticamente (Verificação Heurística)
- Não abrir anexos de origem desconhecida

TIPOS DE VÍRUS

1. VÍRUS DE ARQUIVOS - são tipos de vírus que normalmente substituem ou se anexam a arquivos tipo COM ou EXE.

2.MACRO VÍRUS - são vírus maliciosos, escritos em linguagem de programação macro e anexados a um documento (como Word ou Excel).

3.MAILBOMB - mensagem muito grande enviada para a caixa de correio com o propósito de evitar o recebimento de outras mensagens.

4.VÍRUS MUTANTES - este tipo de vírus se modifica à medida que contamina os arquivos, consequentemente dificultando sua identificação.

5. **ATAQUES A SENHAS** – Seu objetivo é obter a senha (password) utilizada pelo usuário.
6. **VÍRUS DE BOOT** - Este tipo de vírus infecta o setor de inicialização da máquina localizado nos discos rígidos (Master Boot Record - MBR).
7. **STEALTH VÍRUS (VÍRUS SECRETO)** - são vírus que tentam disfarçar sua aparência quando analisados por softwares antivírus.
8. **RETROVÍRUS** - São vírus que tem como alvo antivírus, como o Avast e Avira.
9. **TIME BOMB** – Projetado para ser executado em uma data e hora específicas e com funções definidas pelo seu criador.

PROCEDIMENTOS DE BACKUP

Termo atribuído às copias de segurança realizadas pelo usuário.

COMPACTAÇÃO E DESCOMPACTAÇÃO

Procedimento em que os dados são copiados de forma compactada, ou seja, serão enviados para uma unidade de destino com uma solicitação de espaço menor que na de origem.

PROGRAMAS COMPACTADORES

Winzip , Winrar, Arj, Pkzip, Ark.

TIPOS DE BACKUP

1. Normal, Total, Completo ou Global: Consiste em armazenar tudo que foi solicitado, permitindo-se ainda ser feita a compressão dos dados ou não, quando gravamos todas as informações existentes no computador.

2. Backup Incremental: Um backup incremental copia e os arquivos criados ou alterados desde o último backup completo ou incremental e os marca como arquivos que passaram por backup (o atributo de arquivo é desmarcado). Se você utilizar uma combinação dos backups normal e incremental, precisará do último conjunto de backup normal e de todos os conjuntos de backups incrementais para restaurar os dados.

3. Backup Diferencial: Um backup diferencial copia arquivos criados ou alterados desde o último backup completo ou incremental. Não marca os arquivos como arquivos que passaram por backup (o atributo de arquivo não é desmarcado). Se você estiver executando uma combinação dos backups normal e diferencial, a restauração de arquivos e pastas exigirá o último backup normal e o último backup diferencial.

4. Backup de Cópia: Um backup de cópia copia todos os arquivos selecionados, mas não os marca como arquivos que passaram por backup (o atributo de arquivo não é desmarcado). A cópia é útil caso você queira fazer backup de arquivos entre os backups normal e incremental, pois ela não afeta essas outras operações de backup.

5. Backup Diário: Um backup diário copia todos os arquivos selecionados que foram criados ou alterados no dia de execução do backup diário. Os arquivos não são marcados como arquivos que passaram por backup (o atributo de arquivo não é desmarcado).

FORMAS DE BACKUP

QUENTE: cópia de segurança on-line, ou seja, o sistema permanece em execução enquanto a cópia é realizada.

FRIA: Gerenciamento do backup sem interferências.