Prime

ISF – SEGURANÇA EM REDES E COMUNICAÇÕES

Phishing

- Phishing é uma forma de fraude na internet;
- Uma fraude é definida como a realização de uma transação não autorizada;
- Geralmente a vítima recebe um e-mail pedindo para verificar ou confirmar uma conta bancária com os números da conta, senhas e cartão de crédito, por exemplo.

Às vezes mensagens SMS são usadas.

Até mesmo contato telefônico já foi utilizado.

Spam

- Spam é nome para o coletivo de mensagens indesejadas;
- O termo é normalmente utilizado para e-mails indesejados, mas mensagens publicitárias indesejadas em sites também são consideradas spam;
- Um filtro de spam pode diminuir esse problema;
- Existem algumas coisas que os usuários de computador podem fazer para combater o spam. Algumas delas são:

Nunca responda uma mensagem de spam, até mesmo para cancelar a inscrição;

Não encaminhe mensagens de spam e não distribua endereços de e-mail (usar a funcionalidade CCO).

Malware: Um Software Malicioso

- Malware é uma combinação das palavras Malicioso e Software;
- Trata-se de um software indesejado, como vírus, worms, Cavalos de Troia e spywares;
- A solução padrão contra malwares é fazer varreduras com um antivírus e usar um firewall;
- A varredura do antivírus por si só não é tão eficaz contra malwares que surgem devido a ações humanas, tais como a abertura de e-mails suspeitos ou e-mails de remetentes desconhecidos.

Malware: Vírus

Definição:

- Pequeno programa de computador que se multiplica propositalmente, às vezes em formas alteradas;
- As versões replicadas do vírus original são, em virtude desta definição, também vírus;
- Para que o vírus se espalhe é necessário um programa que contenha um código executável.

Explicação:

- Assim que o programa é executado, o vírus procura novos programas para tentar infectá-los;
- Um vírus só pode se espalhar para fora do sistema infectado se um usuário transferir arquivos do sistema infectado para um novo sistema;
- Tradicionalmente, os hóspedes dos vírus eram apenas programas, mas atualmente podem ser documentos;

Malware: Vírus

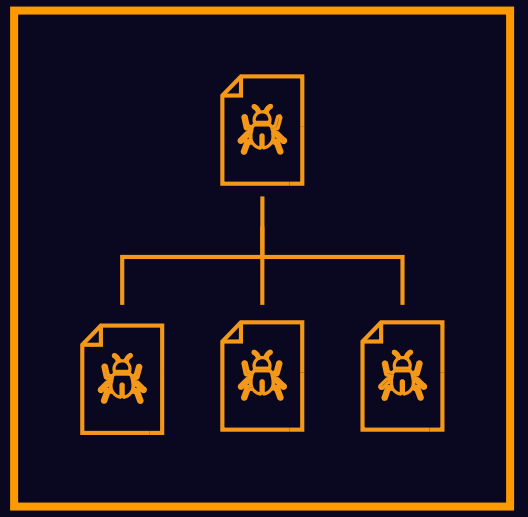
Explicação:

- Possuem códigos executáveis, como macros, VBScript ou ActiveX;
- Na grande maioria dos casos, os vírus são equipados com uma carga que abriga outros códigos executáveis – normalmente esta carga é de natureza destrutiva.

Medidas:

- Varredura de vírus no servidor de e-mail e nos computadores no local de trabalho;
- O assunto sobre vírus está incluído nas campanhas de conscientização de segurança;
- O tema está incluído na Política de Segurança da Informação da organização.

Malware: Worm



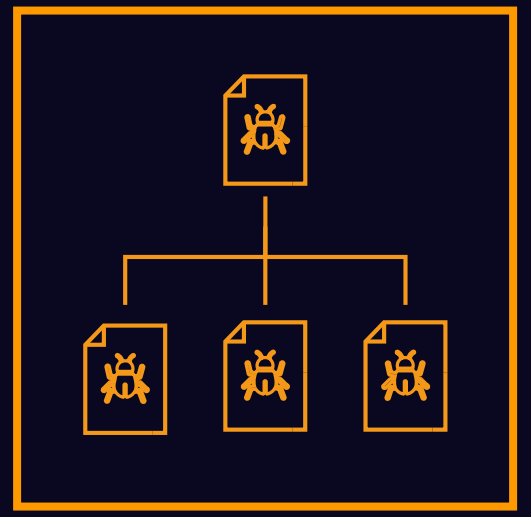
Definição:

- Pequeno programa que se multiplica propositalmente;
- O resultado da multiplicação são cópias do original;
- Se espalham por outros sistemas, fazendo uso dos recursos de rede do seu hospedeiro.

Explicação:

- As diferenças entre vírus e worms estão se tornando cada vez mais tênues;
- Um vírus depende da ativação do usuário, o worm não;
- O worm se espalha e é ativado automaticamente em um curto período de tempo;
- Ambos dependem de um código executável.

Malware: Worm



Medidas:

- Varredura no servidor de e-mails e nos computadores no local de trabalho;
- Como os worms podem ser descobertos na rede, utilize um monitor de rede;
- O assunto está incluído nas campanhas de conscientização e política de segurança;
- Formas eficazes de relatar incidentes e bons procedimentos de follow-up.

Malware: Cavalo de Troia

Definição:

- Programa que executa atividades secundárias sem que o usuário do computador perceba;
- Pode prejudicar a integridade do sistema infectado.

Explicação:

- À primeira vista, se apresenta como algo útil, mas, quando é ativado, realiza atividades indesejadas;
- Muitas vezes instala uma "backdoor", para ter acesso não autorizado ao sistema infectado;
- Pode enviar informações confidenciais para outro local onde serão recolhidas e analisadas;
- Diferente do vírus e Worms, o Cavalo de Troia não pode se replicar, por isso permanece despercebido por um longo período de tempo executando suas atividades maliciosas.

Malware: Cavalo de Troia

Medidas:

- Varredura de Cavalo de Troia e/ou vírus no servidor de e-mail e nos computadores;
- Assunto Cavalo de Troia está incluído nas campanhas de conscientização e política de segurança;
- Ferramentas de monitoramento de rede podem ajudar com a descoberta.

Malware: Hoax

Definição:

- Uma hoax (em tradução literal, “embuste” ou “mentira ardilosa”);
- Uma forma de engenharia social;
- Mensagem que tenta convencer o destinatário de sua veracidade;
- Em seguida, levar o leitor a realizar uma determinada ação;
- A disseminação depende dos leitores enviarem deliberadamente a mensagem para outras vítimas.

Explicação:

- A carga de uma hoax não é de natureza técnica, mas, sim, psicológica;
- Ao jogar com as emoções das pessoas, a hoax tenta convencer o leitor a compartilhá-la com outros);

Malware: Hoax

Explicação:

- Pode, ocasionalmente tentar convencer as pessoas a:
  - ✓ Depositarem dinheiro;
  - ✓ Fornecerem informações pessoais (phishing);
  - ✓ Ou outras atividades maliciosas;
- Correntes de e-mail são a forma mais significativa e bem sucedida de hoax.

Medidas:

- Varredura de vírus e solução antispam. Uma hoax muitas vezes contém textos que podem ser reconhecidos por esses filtros;
- O assunto sobre as hoaxes está incluído nas campanhas de conscientização e política de segurança;
- Funcionários devem estar atentos para perguntas estranhas em e-mails;
- Formas eficazes de relatar incidentes e de que existam bons procedimentos de follow-up.

Malware: Bomba Lógica

Definição:

- Pedaço de código que é construído em um sistema;
- Este código irá, em seguida, executar uma função quando reunir condições específicas.

Explicação:

- Os gatilhos detonam depois que uma condição é atendida;
- Ou os gatilhos lançam uma bomba lógica quando uma condição não for atendida;
- Bombas lógicas, muitas vezes, contêm malwares, que normalmente demoram algum tempo para serem “detonadas”, ou seja, para que o vírus ou worm se propague.

Medidas:

- Para softwares desenvolvidos por funcionários da empresa ou sob contrato com terceiros, realize uma análise minuciosa do código por outra parte.

Malware: Spyware

Definição:

- Programa que recolhe informações sobre o usuário e as encaminha para terceiros, com fins monetários;
- Não prejudica o computador e/ou o software instalado, mas, viola a privacidade do usuário.

Explicação:

- Um Spyware pode ser reconhecido através de diversas maneiras, por exemplo:
  - ✓ O computador está mais lento do que de costume;
  - ✓ Programas estão sendo executados sem terem sido iniciados ou vistos antes;
  - ✓ Há uma nova barra de ferramentas no seu navegador e você não consegue removê-la;
  - ✓ Vários tipos de pop-ups aparecem sem mais nem menos.

Malware: Spyware

Medidas:

- Varreduras dos registros do Windows por chaves suspeitas de registros;
- Muitos programas antivírus também detectam spywares;
- Use um firewall para detectar o tráfego da rede de um computador sem nenhum motivo aparente;
- O assunto sobre spywares está incluído nas campanhas de conscientização e política de segurança;
- Formas eficazes de relatar incidentes e bons procedimentos de follow-up.

Malware:
Botnet / Storm Worm

Definição:

- Combinação das palavras robot e network, com uma conotação negativa ou maliciosa;
- Programas conectados a outros similares, via internet, a fim de realizar tarefas no computador de alguma pessoa.

Explicação:

- Esses programas se comunicam por vários canais para enviar e-mails de spam ou DDoS;
- É possível se tornar parte de um botnet clicando em um link em um e-mail, página da web ou anexo;
- Muitas vezes podem ser baixados sem qualquer noção do usuário;
- Quando um computador se torna um bot, ele se torna uma espécie de “zumbi”, recebendo ordens;
- A rede Storm Worm ou botnet é considerada por muitos como o futuro do malware;

Malware: Botnet / Storm Worm

Explicação:

- Ele é paciente, e, portanto, difícil de ser detectado;
- Empregam uma variedade de vetores de ataque, e também existem várias etapas defensivas.

Medidas:

- Garantir que os softwares sejam atualizados regularmente, assim como o antivírus;
- Scanners que inspecionem o registro do Windows;
- Usar um firewall pessoal a fim de detectar tráfego de rede suspeito ou ferramentas de monitoramento;
- Assunto “botnet” está incluído nas campanhas de conscientização e política de segurança;
- Formas eficazes de relatar incidentes e de que existam bons procedimentos de follow-up.

Malware: Rootkit

Definição:

- Conjunto de ferramentas de software que são frequentemente usadas por um terceiro (normalmente um hacker);
- Usado após ter obtido acesso a um sistema (computador);
- O rootkit se esconde com profundidade no S.O., fazendo com que este se torne instável;
- É quase impossível remover um rootkit sem danificar o sistema operacional;
- O propósito é criar e esconder arquivos, conexões de rede, endereços de memória e entradas de índice.

Malware: Rootkit

Explicação:

- Rootkits podem trabalhar em dois níveis: nível do kernel e nível do usuário;
  - ✓ Kernel: pode fazer quase qualquer coisa no sistema. O objetivo é ler, alterar ou influenciar os processos em execução, dados ou arquivos do sistema;
  - ✓ No nível do usuário são limitados a segmentos específicos da memória(.
- Um rootkit ajuda o intruso a obter acesso ao sistema sem a consciência do usuário;
- Existem rootkits para quase todos os sistemas operacionais.

Malware: Rootkit

Medidas:

- Garantir que os softwares sejam atualizados regularmente, assim com o antivírus;
- Scanners que inspecionem o registro do Windows;
- Usar programas que podem detectá-los na memória;
- Assunto “rootkit” está incluído nas campanhas de conscientização e política de segurança;
- Formas eficazes de relatar incidentes e de que existam bons procedimentos de follow-up.

Controle: Proteção Contra Malware

Objetivo:

Garantir que as informações e outros ativos associados estejam protegidos contra malware.

Além de um anti-malware, o que precisamos considerar?

- Lista de aplicativos permitidos;
- Lista de bloqueio;
- Reduzir vulnerabilidades que podem ser exploradas por malware;
- Investigar a presença de arquivos não aprovados ou alterações não autorizadas;
- Proteção contra obtenção de arquivos e software de redes externas;
- Verificar regularmente dados recebidos na redes, e-mail, mensagens etc.;
- Escanear páginas da web em busca de malware;
- Onde posicionar a ferramenta de detecção, como no gateway de rede, dispositivos, servidores ou endpoint de usuário;

Controle: Proteção Contra Malware

Além de um anti-malware o que precisamos considerar?

- Proteção contra entrada de malware durante uma manutenção de emergência;
- Processo para autorizar a desativação temporária ou permanente de algumas ou todas as medidas contra malware, caso as ferramentas estejam interrompendo as operações normais;
- Preparar planos de continuidade de negócios para recuperação de ataques;
- Isolar ambientes onde possam ocorrer consequências catastróficas;
- Treinamento e conscientização de todos os usuários sobre recebimento de e-mails, arquivos ou programas infectados por malware;
- Assinar listas de discussão ou revisar sites relevantes;
- Ficar atualizado através de boletins de aviso de fontes confiáveis.

Controle: Segurança de Redes

Objetivo:

Proteger as informações em redes e seus recursos de processamento de informações de suporte contra comprometimento através da rede.

O que considerar ao proteger as informações em redes?

- O tipo e o nível de classificação das informações;
- Quem e como gerenciar os equipamentos de rede e os dispositivos;
- Manter a documentação atualizada, como diagramas, arquivos de configuração de roteadores, switches etc.;
- Segregar responsabilidade operacional pelas redes das operações de TIC;
- Controles de confidencialidade e a integridade dos dados que transitam em redes;

Controle: Segurança de Redes

O que considerar ao proteger as informações em redes?

- Registro e monitoramento para detecção relevante;
- Autenticação nos sistemas na rede;
- Restringir conexão dos sistemas à rede através de firewalls;
- Detectar, restringir e autenticar a conexão de equipamentos e dispositivos à rede;
- Endurecimento dos dispositivos de rede;
- Segregar os canais de administração da rede de outros tráfegos de rede;
- Isolar temporariamente sub-redes críticas se a rede estiver sob ataque;
- Desabilitar protocolos de rede vulneráveis.

Controle: Segurança dos Serviços de Rede

Objetivo:

Garantir a segurança no uso dos serviços de rede de provedores de serviços de rede.

O que é incluído nestes Serviços de Rede?

- Fornecimento de conexões (Gateway, DNS, DHCP, Proxy etc.);
- Serviços de rede sem fio;
- Soluções gerenciadas de segurança de rede, como:

Firewalls;

VPNs;

Sistemas de detecção de intrusão.

Controle: Segurança dos Serviços de Rede

Quais os recursos e regras de segurança dos serviços de rede devem ser considerados?

- Autenticação, criptografia e controles de conexão de rede;
- Conexão segura com os serviços de rede;
- Serviços de autenticação para acesso a diversos serviços de rede;
- Procedimentos de autorização para determinar quem tem permissão para acessar quais redes e serviços;
- Gerenciamento de rede e procedimentos para proteger o acesso às conexões;
- Monitoramento do uso dos serviços de rede.

Controle: Segregação de Redes

Objetivo:

Dividir a rede em limites de segurança e controlar o tráfego entre eles com base nas necessidades do negócio.

O que é segregar uma rede?

- É dividir em domínios com base em níveis de confiança, criticidade e sensibilidade:
  - ✓ Domínio de acesso público;
  - ✓ Domínio de desktop;
  - ✓ Domínio de servidor;
  - ✓ Sistemas de baixo e alto risco;
  - ✓ De unidades organizacionais, como RH, finanças, marketing;
  - ✓ Ou alguma outra combinação.

Controle: Segregação de Redes

Como segregar?

- Usando um gateway:

Firewall;

Roteador de filtragem.

Considerações

- Uma rede sem fio requer tratamento especial devido a um perímetro mal definido;
- Uma rede de acesso sem fio para convidados deve ser separada da organização.

Controle: Filtragem da Web

Objetivo:

Proteger os sistemas de serem comprometidos por malware e impedir o acesso a sites e recursos não autorizados.

Que tipo de site a organização deve evitar que seu pessoal acesse?

- Que contenham informações ilegais;
- Que contenham vírus;
- Sites maliciosos com conteúdo de phishing ou malware;
- Sites com função de upload de informações;

Como bloquear esses acessos?

- Bloqueando o endereço IP;
- Bloqueando domínio do(s) site(s) em questão;
- Alguns navegadores e tecnologias antimalware fazem isso automaticamente;
- Treinamento ao pessoal sobre o uso seguro e apropriado de recursos online.

Criptografia e Gerenciamento de Chaves

Política de Criptografia:

- Onde a organização deve usar a criptografia;
- Quais tipos de criptografia a organização usa e em quais aplicativos;
- Controle e gerenciamento de chaves;
- Cópia de segurança das chaves;
- Controle das chaves.

Criptografia e Gerenciamento de Chaves

Criptografia: Gerenciamento de Chaves

- As chaves criptográficas devem ser protegidas contra alteração, perda e destruição;
- Chaves secretas e pessoais precisam ser protegidas contra a divulgação não autorizada;
- Registro dos pares de chaves: quais pares foram emitidos a quem e quando;
- Quando uma chave irá expirar?
- O que deve ser feito quando uma chave for comprometida?
- Evite usar a mesma chave em sistemas diferentes (por exemplo, notebooks).

Criptografia Simétrica

Simétrico

A mesma chave secreta foi compartilhada

Criptografia Assimétrica

Simétrico

Como você está?

Criptografia

Chave pública

%RT$@<SW?S<MG_(*

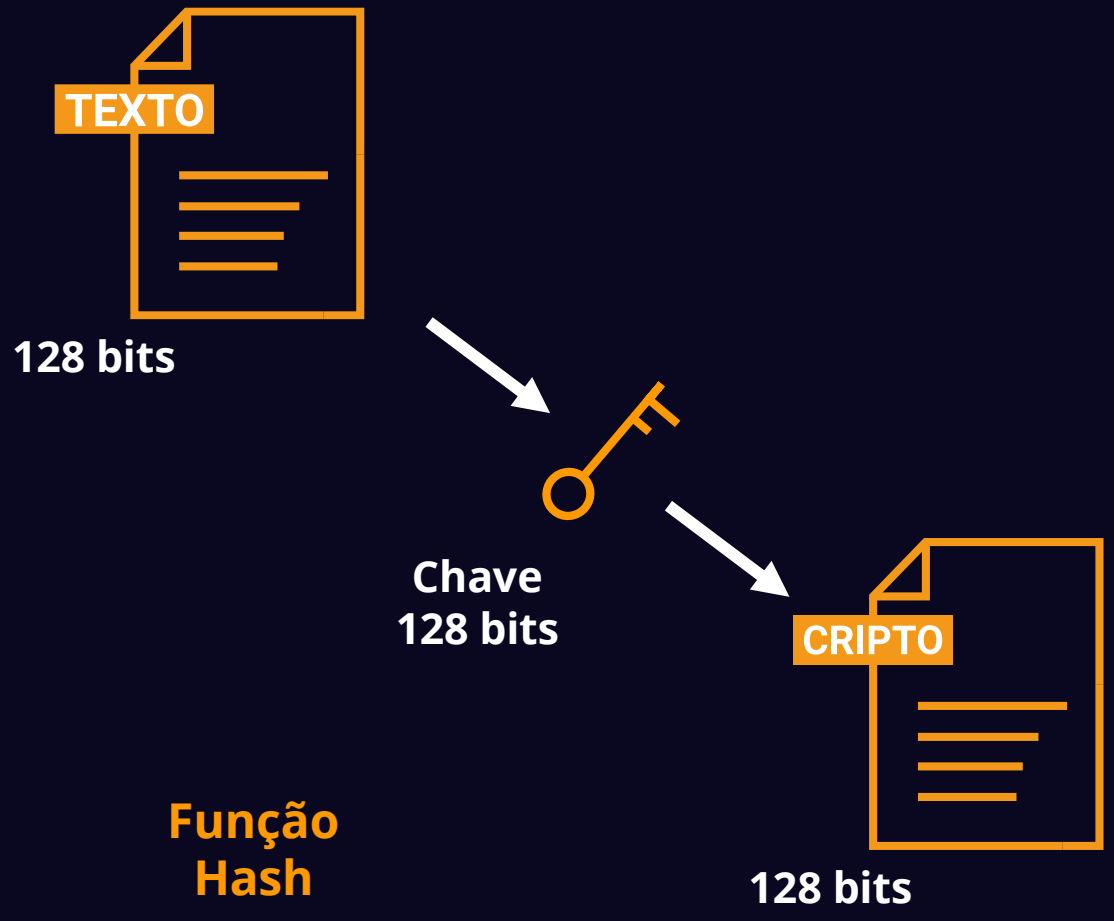
Descriptografia

Chave privada

Como você está?

Diferentes chaves são usadas para criptografar e descriptopgrafar

Criptografia One-Way (Hash)



Pode ser usado para:

- Checar dois valores;
- Validar apenas a integridade.

PKI, Autoridade Registradora e Autoridade Certificadora

- Public Key Infrastructure (PKI) é um conjunto de normas e requisitos técnicos;
- PKI inclui muito mais do que somente a criptografia;
- PKI fornece garantias referentes a quais pessoas ou sistemas pertencem a uma chave pública específica.
- Componentes de uma solução PKI:
  - ✓ Autoridade Certificadora (CA);
  - ✓ Autoridade Registradora (RA)

Autoridade Certificadora (CA):

- Emite, renova ou revoga certificados digitais.
- Atesta que a chave pública pertence à pessoa cujas credenciais são verificadas pela RA;

Autoridade Registradora (RA):

- Faz a interface entre o usuário e a CA;
- Recebe, valida e encaminha solicitações de emissão ou revogação de certificados digitais às CAs;
- Mantém registros de suas operações.

Assinaturas Digitais

- Assinaturas digitais são criadas utilizando criptografia assimétrica.
- Uma assinatura digital é o método utilizado para confirmar se a informação digital foi produzida ou enviada por quem ela afirma ser – semelhante à assinatura de caneta em documentos de papel.
- A assinatura digital é geralmente constituída por dois algoritmos:
  - ✓ Um para confirmar que a informação não foi alterada por terceiros;
  - ✓ Outro para confirmar a identidade da pessoa que "assinou" a informação.
- Em alguns países (por exemplo, os da União Europeia), uma assinatura digital possui a mesma validade que a assinatura no "papel“;
- Na maioria dos casos, é necessário usar um certificado atestado para verificar a veracidade desta assinatura digital (por exemplo, um smartcard).

Controle:
Uso de Criptografia

Objetivo:

Garantir o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade ou integridade das informações de acordo com os requisitos de negócios e segurança da informação, levando em consideração os requisitos legais, estatutários, regulatórios e contratuais relacionados à criptografia.

Controle: Uso de Criptografia

Qual o objetivo da Criptografia?

Confidencialidade:

- ✓ Proteger informações confidenciais ou críticas;
- ✓ Informações armazenadas;
- ✓ Informações transmitidas.

Integridade ou autenticidade:

- ✓ Assinaturas digitais ou códigos de autenticação de mensagens;
- ✓ Para fins de verificação de integridade de arquivos.

Não repúdio:

- ✓ Para evidenciar a ocorrência (ou não) de um evento ou ação.

Autenticação:

- ✓ Ao solicitar acesso;
- ✓ Para realizar transações com usuários, entidades e recursos do sistema.

Considerações sobre Criptografia

O gerenciamento de chaves requer processos para:

- Geração de chaves para diferentes sistemas criptográficos e diferentes aplicações;
- Emissão e obtenção de certificados de chave pública;
- Distribuição de chaves para entidades;
- Armazenamento de chaves;
- Alteração ou atualização de chaves;
- Lidar com chaves comprometidas;
- Revogação de chaves;
- Recuperação de chaves perdidas ou corrompidas;

Considerações sobre Criptografia

O gerenciamento de chaves requer processos para:

- Backup ou arquivamento de chaves;
- Destruição de chaves;
- Registro e auditoria das principais atividades relacionadas à gestão;
- Definir as datas de ativação e desativação das chaves;
- Lidar com solicitações legais de acesso a chaves criptográficas, por exemplo, como prova em um processo judicial;
- Definir as datas de ativação e desativação das chaves.

OBRIGADO

ISF – SEGURANÇA EM REDE E COMUNICAÇÕES