SEGURANÇA EM REDES DE COMPUTADORES

PROTEÇÃO NO AMBIENTE COMPUTACIONAL

Autor: Me. Paulo André Zapparoli
Revisor: Rafael Rehm

INICIAR

introdução

Introdução

Nesta unidade, veremos os *softwares* maliciosos, vírus, Cavalos de Troia e outros que têm impacto direto na segurança dos sistemas computacionais e também nas atividades de um analista de segurança da informação, por isso conhecer seu funcionamento e identificação é crucial na área. Aprenderemos a importância de um controle de acesso e seus princípios aplicados a redes de computadores, quais são as técnicas envolvidas para sua implementação e de que forma ela é necessária em um ambiente organizacional, entenderemos também a importância da segurança nos ambientes de computação em nuvem, já que as organizações estão cada vez mais utilizando essa estrutura.

Outro ponto muito importante que será detalhado é o processo de autoria, seu planejamento, coleta de informações e relatórios, bem como os testes e monitoramento do ambiente de TI na busca da garantia de aplicação das políticas e normas de segurança.

Software Malicioso

Os *softwares* maliciosos são comumente chamados de *malware* , que é um termo proveniente do inglês. Esse termo é a forma contraída para a expressão *malicious software* (*software* nocivo), conhecido como pragas.

São programas que foram especificamente desenvolvidos para executar ações danosas e, muitas vezes, atividades maliciosas em sistemas computacionais como:

- Computadores;
- Equipamentos de redes:
  - Modems, *switches* , roteadores;
- Dispositivos móveis:
  - *Tablets* , celulares, *smartphones* .

Esses *softwares* podem ser instalados por um atacante após a invasão de um equipamento, através da exploração de alguma vulnerabilidade existente nos programas que estão instalados no sistema alvo ou através da ação de outro sistema já comprometido pela rede de computadores. Vejamos outras formas comuns de infecção:

- Autoexecução de mídias removíveis infectadas;
- Acesso às páginas *web* maliciosas, via navegadores vulneráveis;
- Execução de arquivos previamente infectados, obtidos:
  - anexos em mensagens eletrônicas;
  - via links recebidos por mensagens eletrônicas e redes sociais;
  - via mídias removíveis;
  - em páginas Web;
  - recursos compartilhados em rede.

Após infectar o seu equipamento, o código malicioso procura executar ações como se fosse você, com o acesso e a exclusão de informações/arquivos, ele pode criptografar seus dados, fazer conexão via *internet* , enviar mensagens e até instalar outros códigos maliciosos.

O que motiva seu desenvolvimento e propagação é sempre a obtenção de alguma vantagem em cima do usuário que está despreparado. Muitas vezes, focado em tirar vantagens financeiras, o *malware* pode ser usado para coleta de informações confidenciais e possível extorsão. Outra motivação seria o desejo de autopromoção, mas em muitos casos também é motivado por vandalismo.

Tipos de *Malware*

Existem diversos *softwares* maliciosos, agora serão destacados alguns tipos para análise e entendimento mais detalhado.

Vírus : é um pequeno programa de computador que ao ser executado se replica propositalmente, algumas vezes fazendo isso de forma alterada. Para que o vírus se propague, ele depende de um portador que contenha seu código executável, ou seja, ele se aloja em um arquivo do sistema, podendo ser arquivos de documentos. Assim que esse portador é executado, o vírus é ativado e passa a procurar novos possíveis portadores (arquivos de mesmo tipo do portador) para se alojar.

O vírus se espalha juntamente à transferência dos arquivos anteriormente

contaminados, quando esses arquivos são executados o vírus infecta o novo sistema. Alguns exemplos de vírus são:

- O vírus Brain (1986);
- O vírus Chernobyl (1998);
- ZEUS (2014);
- Cryptolocker (2014).

Worm : é um pequeno programa de computador que se replica propositalmente, fazendo cópias do programa original para outros sistemas, através do uso dos equipamentos da rede de seu hospedeiro.

Sua propagação é feita por meio da execução direta das cópias, explorando automaticamente as vulnerabilidades em programas. Geralmente, nesse processo são consumidos muitos recursos, devido à grande quantidade de cópias geradas no ambiente contaminado, afetando o desempenho de redes e dos equipamentos.

Processo de propagação e infecção do worm.

Identificação dos computadores alvos: infectado um computador, o worm procura

por novos alvos para se propagar.

São muito similares e, algumas vezes, até confundidos com vírus, sua diferença está nos processos de propagação e contágio que são independentes da ação do usuário.

Alguns exemplos de *worms* são:

- Blaster (2003);
- Storm Worm (2007);
- Stuxnet (2010).

Cavalo de Troia ou *trojan* : é um programa que conduz propositalmente atividades secundárias, além da função que aparenta desempenhar, geralmente, é imperceptível ao usuário do computador e pode prejudicar a integridade do sistema infectado.

Para entrar em ação, necessita ser explicitamente executado para ser instalado. Sua instalação pode ser feita pelo próprio usuário sem que ele se dê conta ou também por atacantes que, após invadirem o equipamento, modificam programas para executar a função original e uma função maliciosa em segundo plano.

A intenção de um *trojan* é conduzir a atividade maliciosa sem ser notado, então, ele se apresenta como um programa útil enquanto faz a atividade maliciosa em segundo plano. O trojan, em muitos casos, instala também um *backdoor* , que é uma forma de conquistar acessos não autorizados ao sistema. Além disso, constantemente, os *trojans* enviam informações confidenciais para outros locais para futura análise.

Alguns exemplos de cavalo de troia:

- Back Orifice (2000);
- Netbus (1998);
- Sub7 (1999);
- Storm Worm (2007).

A principal diferença com relação aos vírus e *worms* é que os *trojans* não podem se autorreplicar.

Backdoor : são programas que permitem a entrada ou o retorno de um invasor no equipamento comprometido, por meio da modificação ou inclusão de serviços criados para esse fim.

Ele pode ser atividade pela ação de outros códigos maliciosos que tenham infectado o equipamento, por atacantes que tenham invadido o equipamento, a sua inclusão assegura ao atacante o acesso futuro ao equipamento de forma remota, sem que para isso necessite recorrer novamente ao método de ativação.

Ransomware : são programas que fazem o sequestro dos dados, geralmente, usando criptografia, exigindo pagamento para resgate dos dados.

Dois tipos principais:

- *Locker* : impede o acesso ao equipamento;
- *Crypto* : impede o acesso aos dados armazenados no equipamento, geralmente, usando criptografia.

saiba mais

Saiba mais

Veja o capítulo de códigos maliciosos da "Cartilha de Segurança para Internet", em que são descritos os diferentes tipos de códigos maliciosos e suas respectivas formas de infecção, apresentando um resumo comparativo para a classificação dos seus diferentes tipos.

ACESSAR

Prevenção

A melhor forma de prevenção é impedir que a infecção aconteça, principalmente, porque em caso de identificação do incidente nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente os dados. Vejamos as recomendações gerais para prevenção:

- Atualizações dos *softwares* : manter atualizadas as versões dos softwares utilizados, sistemas operacionais e aplicativos. Remova completamente as versões antigas e também todas as aplicações que não são utilizadas;
- Use mecanismos de proteção:
  - Tenha um antivírus instalado (*antimalware*): são sistemas que analisam os arquivos, inclusive, de e-mails, e comportamento dos sistemas, evitando surpresas indesejáveis, mas não adianta somente instalá-los, deve-se atualizá-los e fazer as varreduras periódicas no sistema;
  - *Firewall* pessoal: tenha um *firewall* pessoal instalado e ativo, mas não se esqueça de periodicamente checar seus *logs* para analisar comportamentos estranhos;
  - *Backup* : faça cópia de segurança dos seus arquivos e do sistema periodicamente, se possível com cópias redundantes.
- Instalação de aplicativos de terceiros: faça *download* dos aplicativos apenas de fontes confiáveis e faça a varredura do antivírus antes da instalação. Muito cuidado com as permissões cedidas aos aplicativos instalados;
- *Link* : antes de acessar um *link* , certifique-se de que este é confiável;
- Privilégios: evitar utilizar a conta administrativa do sistema, isso já irá restringir qualquer ação indesejável que fere as diretivas de segurança dos sistemas.

Controle de Acesso

Em um primeiro momento, podemos dizer que os controles de acesso devem atender aos objetivos do negócio, aos processos, aos subprocessos ou à atividade de negócio. Deve-se utilizar a avaliação de risco para determinar o quão rigoroso esses controles devem ser para conseguir mitigar os riscos identificados.

Para se estabelecer um controle de acesso adequado, é necessário fazer uma combinação de controles de acesso físico e controle de acesso lógico que estão relacionados aos sistemas de informação. De acordo com a ISO 27002:2013, os controles de acesso devem ser uma política estabelecida, documentada, periodicamente revisada e baseada nos requisitos de negócio e de segurança da informação.

É preciso destacar que o controle de acesso lógico visa prevenir que pessoas não autorizadas tenham acesso a qualquer informação que possua valor para a organização. Isso significa que é necessário estabelecer uma maneira formal de o responsável pela informação autorizar as pessoas que poderão ter acesso à informação. Essa autorização é um conjunto de permissões que concede o direito de leitura ou de alteração a um determinado arquivo ou

registro em banco de dados.

Os itens mais comuns de tipos de acesso a serem considerados no momento de definir controles de acesso são:

- Acesso aos equipamentos de TI;
- Acesso às redes e serviços de redes;
- Acesso à informação;
- Acesso às aplicações de negócio.

Gestão de Acesso do Usuário

Visa garantir que ativos sejam acessados somente por usuários autorizados, prevenindo seu acesso por usuários não autorizados. Segundo Hintzbergen *et al* . (2015), para isso, são necessárias as seguintes atividades:

- Registro e cancelamento de registro de usuário;
- Provisionamento de acesso ao usuário;
- Gestão de direito de acesso privilegiado;
- Administração de informações confidenciais da autenticação de usuários;
- Verificação das permissões de acesso de usuário;
- Retirada ou ajuste das permissões de acesso.

Para se efetivar à concessão de acesso, para um usuário usar determinado ativo, envolve-se uma série de etapas que incluem:

- **A identificação do usuário** : por exemplo, é ideal a utilização de algo que represente unicamente o usuário, a digital ou ires, outra possibilidade é algo que ela possua, como um *token* ;
- **A autenticação desse usuário** : por exemplo, um sistema checa se o nome do usuário existe dentro do sistema, caso positivo, solicita-se a senha. Se a senha for confirmada, o usuário é autenticado;
- **A autorização do usuário** : por exemplo, com o usuário autenticado, o sistema verifica, em uma base de permissões, a quais recursos ele tem acesso concedido.

Responsabilidade do Usuário

Os usuários são os responsáveis por suas próprias informações de autenticação e devem salvaguardar essas informações, ou seja, não podem compartilhar suas senhas, sendo seu dever manter suas senhas seguras. Quando se usa *token* , não se pode compartilhá-lo e, ainda, deve-se ter cuidado para que o *token* não seja roubado e, em caso de perda, avisar imediatamente o responsável pela segurança da organização.

É fundamental que os colaboradores da organização conheçam suas responsabilidades em termos de manter as informações e os ativos seguros e protegidos.

Acesso ao Sistema e às Aplicações

O passo mais importante ao configurar um controle de acesso aos sistemas e às aplicações é conseguir um equilíbrio na hora de aplicar as restrições, porque temos dois pontos antagônicos que precisamos atender:

- Evitar que usuários não autorizados tenham acesso ao sistema;
- Permitir aos usuários autorizados o acesso necessário ao sistema.

Essa é uma tarefa que deve ser feita com bastante cuidado para não deixar o sistema permissivo ou restritivo demais. Outra parte do controle de acesso são as medidas de segurança no procedimento de *logon* , restringindo ao máximo as informações que podem ser utilizadas por um atacante. Exemplos:

- Não mostrar informações sobre o sistema ou aplicativo relacionado ao logon, para evitar que uma atacante consiga determinar o sistema que está procurando;
- Não apresentar nome padrão de usuário;
- Se o nome ou usuário informado estiver errado, não informar qual está incorreto;
- Informar, após logon com êxito, data de hora de último logon com êxito, a fim de identificar uso indevido da conta pelo usuário.

Manter os sistemas com poderes administrativos separados e com controles de acessos o mais restritivo possível.

Quando os sistemas e aplicativos são desenvolvidos na própria organização é importante ter controles de acesso rígidos ao código fonte e às informações afins, não só por questões de segurança, mas para preservar também a propriedade intelectual usada no desenvolvimento dos sistemas e aplicativos.

Controle de acesso à Rede e Segurança em Nuvem

A segurança da rede de computadores é composta por diversas camadas, podemos destacar entre essas camadas a que determina o acesso ou não do usuário à rede. Veremos, agora, a segurança de rede, com enfoque em dois tópicos principais: controle de acesso em redes e segurança na nuvem.

Controle de Acesso à Rede

A função do Controle de Acesso à Rede (NAC – Network Access Control) é autenticar os usuários que estejam se logando na rede de computadores e autorizar quais dados eles podem acessar e as ações que eles podem executar. Ele também pode examinar a saúde do computador ou dispositivo móvel do usuário (os terminais). NAC é um termo genérico para identificar o gerenciamento do acesso a uma rede. Sistemas NAC lidam com três elementos de um sistema de controle de acesso à rede:

- solicitante de acesso (AR – Access Requestor): é o dispositivo ou nó que está tentando acessar a rede. Ex.: computadores, servidores, impressoras, câmeras etc. também são conhecidos como

requerentes ou simplesmente clientes;
- servidor de políticas: é o servidor que determina qual o acesso deve ser concedido com base na postura do cliente e na política definida pela empresa;
- servidor de acesso à rede (NAS – Network Access Server): é o ponto de controle de acesso para usuários que pode incluir seus próprios serviços de autenticação.

Muitos clientes buscam acessar um servidor de rede por meio de algum tipo de NAS e seguirão os seguintes passos:

1. Fazer a autenticação do cliente: pode ser realizada pelo NAS ou o NAS pode intermediar o processo de autenticação:

> *O processo de autenticação serve para vários propósitos. Ele verifica a identidade com que o requerente se identifica, o que habilita o servidor de políticas a determinar quais privilégios de acesso, se houver, o AR (Access Requestor - Solicitante de acesso) pode ter. A mudança na autenticação pode resultar na determinação de chaves de sessão para permitir comunicações seguras no futuro entre o requerente e os recursos na rede corporativa (STALLINGS, 2014, p. 389).*

2. O servidor de políticas verificará o cliente para determinar se pode ser permitida a conectividade.

O Servidor fará uma triagem ou controle checando o cumprimento de certos requisitos:

- a atualização *software antimalware* do usuário;
- se o sistema operacional está completamente atualizado;
- se pertence e pode ser controlado pela organização.

Essas verificações são feitas antes de dar acesso ao cliente à rede corporativa. Com base no resultado desses dois passos, decide-se como tratar esse cliente:

- acesso franqueado, se todos os passos tiverem êxito;

- colocado numa rede intermediário (segregada) até que atenda às políticas necessárias, pela intervenção de um atendente ou automaticamente, no caso de atualização;
- negado o acesso por falta de autenticação ou algum problema grave constatado na política.

Métodos de Imposição de Acesso à Rede

Métodos de imposição são as ações para regulamentar o acesso à rede da empresa aplicado aos clientes. Existem vários métodos de imposição e podemos, inclusive, fazer uma combinação de métodos. Vejamos, agora, os métodos NAC de imposição mais comuns:

- **IEEE 802.1X** : esse é um protocolo de camada de enlace que impõe autorização antes de ser atribuído um endereço IP a uma porta. IEEE 802.1X faz uso do EAP (Extensible Authentication Protocol) como processo de autenticação. As seções 16.2 e 16.3 cobrem o Extensible Authentication Protocol e o IEEE 802.1X, respectivamente;
- **Redes Locais Virtuais (VLANs – Virtual Local Area Networks)** : nessa abordagem a rede da empresa é segmentada logicamente em VLANs. O sistema NAC decidirá à qual das VLANs da rede o cliente será direcionado, baseado na aplicação das políticas, para a VLAN das correções de segurança, para a VLAN que apenas acessar a Internet ou outras possibilidades com diversos níveis de acesso aos recursos da empresa que estão disponíveis na rede. A criação das VLANs pode ser dinamicamente e os membros da VLAN, tanto servidores corporativos quanto clientes, podem se sobrepor, ou seja, um servidor ou um cliente pode pertencer a mais de uma VLAN;
- **Firewall** : um *firewall* pode fornecer uma forma de NAC, já que sua função é permitir ou negar tráfego de rede entre um interlocutor da empresa e um usuário externo;
- **Gerenciamento de DHCP** : o Dynamic Host Configuration Protocol (DHCP) é um protocolo que tem a função de alocar, dinamicamente, endereços IP aos dispositivos da rede. Dessa forma, é possível a imposição do NAC acontecer na camada IP, baseada em sub-rede e na atribuição do endereço IP.

Segurança em Nuvem

Muitas organizações tendem a transferir uma parte substancial ou até todas as suas operações de Tecnologia da Informação (TI) para uma infraestrutura de computação em nuvem corporativa. Veja a representação da computação em nuvem na Figura 2.1.

As características principais da computação em nuvem incluem:

- **Amplo acesso à rede** : recursos disponíveis através da rede e acessados por meio da plataforma do cliente (por exemplo, telefones celulares, *laptops* e PDAs) ou através de outros serviços de *software* tradicionais ou baseados em nuvem;
- **Elasticidade rápida** : capacidade de expandir e reduzir os recursos, conforme necessidade do serviço;
- **Serviço mensurável** : controle e otimização dos recursos, por meio de monitoração, controle e reporte da utilização do recurso, oferecendo transparência ao consumidor acerca do serviço utilizado;
- **Auto serviço sob demanda** : um consumidor pode provisionar recursos de computação, conforme sua necessidade, sem precisar de interação humana com o prestador de serviço;
- **Agrupamento de recursos** : os recursos de computação são agrupados de forma que possam atender a vários consumidores com um modelo multilocatário.

Figura 2.1 - Computação em nuvem
Fonte: Cloud Computing / Wikimedia Commons.

Riscos e Contramedidas de Segurança na Nuvem

Podemos considerar os controles de segurança na computação em nuvem iguais a qualquer outro ambiente de TI, no entanto, a computação na nuvem pode apresentar riscos específicos, devido ao ambiente da nuvem. Um dos conceitos é que a empresa perde o controle sobre recursos, serviços e aplicações, mas deve manter a responsabilidade pelas políticas de segurança e privacidade. Vejamos as maiores ameaças à segurança em relação à computação em nuvem e suas respectivas contramedidas sugeridas:

Abuso e uso nefasto da computação em nuvem : na maioria dos provedores de nuvem, é fácil se registrar e começar a usar os serviços, alguns até com períodos gratuitos para teste, isso facilita a atacantes entrarem na nuvem na intenção de realizar ataques. Cabe ao provedor de nuvem se proteger desses ataques, mas os clientes de serviços em nuvem precisam monitorar seus dados e recursos na busca de comportamento malicioso.

Contramedidas incluem:

- Processos mais rigorosos para de registro e validação de clientes;
- Monitorar fraude de cartão de crédito;
- Introspecção total do tráfego de rede do cliente;
- Monitorar listas negras para os próprios blocos de rede.

Interfaces inseguras e APIs : provedores de nuvem necessitam revelar aos clientes um conjunto de interfaces de software ou APIs usado para gerenciar e interagir com os serviços em nuvem. Como são difundidas a todos, essas interfaces devem estar preparadas para proteção contra tentativas acidentais e maliciosas de burlar suas políticas.

Contramedidas incluem:

- analisar o modelo de interfaces de segurança do provedor de nuvem;
- garantir a implementação dos controles de autenticação e de acesso mais forte e que esteja encriptando as transmissões;
- entender a cadeia de dependência associada à API.

Funcionários maliciosos : essa é uma grande preocupação em uma rede e, também, deve ser em nuvem, consistindo no risco de atividade interna maliciosa. Existem certos papéis que possuem risco extremamente alto, como os administradores de sistema do provedor de nuvem e os prestadores de serviços de segurança gerenciados.

As contramedidas incluem:

- regras rigorosas da gestão da cadeia de suprimentos e avaliação abrangente dos fornecedores;
- especificar os requisitos de recursos humanos como parte de contrato legal;
- exigir relatórios de conformidade e transparência nas práticas gerais de segurança e de gerenciamento de informações;
- determinar processos de notificação em caso de violação de segurança.

Perda de dados ou vazamento : uma quebra de segurança que pode ser devastadora aos clientes de nuvem, consistindo nas perdas ou nos

vazamentos de dados.

Contramedidas incluem:

- implementar uma forte API de controle de acesso;
- proteger a integridade dos dados em trânsito pela encriptação;
- analisar a proteção dos dados em tempo de projeto e de execução;
- implementar chaves fortes e práticas de armazenamento, gerenciamento e destruição.

Auditoria, Testes e Monitoramento

A auditoria em sistemas computacionais é a checagem se seu funcionamento está de acordo com o planejado, examinando a configuração para verificar se ele está em conformidade com os padrões definidos.

> *Com testes automatizados, o sistema cria um relatório de quaisquer mudanças em arquivos e configurações importantes, que podem se relacionar com o sistema operacional ou com o software aplicativo. Sistemas podem incluir computadores pessoais, servidores, grande porte (mainframe), roteadores de rede e switches. Alguns exemplos desses tipos de aplicativos incluem software associado a acesso à Internet, bancos de dados ou quaisquer recursos compartilhados por usuários (KIM, 2014, p. 164).*

O resultado de uma auditoria é a comparação do ambiente esperado, de acordo com as políticas e normas de segurança e com a estrutura real de funcionamento da organização. A análise do ambiente de produção, muitas vezes, é obtida de relatórios e evidências de uso extraídos das ferramentas de monitoramento e teste dos sistemas computacionais. Baseando-se nisso, é

possível determinar se o desempenho do sistema funcionou conforme planejado.

Segurança da informação é uma disciplina muito dinâmica e exige que seus controles se mantenham atualizados e efetivos. Essa revisão inclui as seguintes atividades:

- **monitoramento** : controle de todas as ações e mudanças no sistema;
- **auditoria** : mantém o histórico das atividades desenvolvidas em sistemas computacionais baseadas na política de segurança e nos controles;
- **aprimoramento** : aprimora o programa e os controles de segurança baseados nos resultados da auditoria;
- **proteção** : implementa novas ações para atingir o nível de segurança pretendido.

A busca por um melhor aproveitamento em segurança da informação passa pela manutenção desse ciclo de revisão de segurança, no qual após a Proteção, retornamos ao monitoramento.

Auditoria e Análise de Segurança

O objetivo de uma auditoria de segurança é garantir que os sistemas e controles funcionem de acordo com o esperado. Os questionamentos abaixo nos auxiliam na busca da direção correta e, para tais, procure tornar positivas as respostas a eles:

- As políticas de segurança são sólidas e apropriadas para a empresa ou atividade?
- Existem controles que apoiam suas políticas?
- Existe implementação e manutenção efetiva de controles?

É fundamental determinar no planejamento da auditoria quais serão as áreas que a auditoria analisará ou não e, nessas áreas, quais serão os responsáveis, sendo importante programar auditorias futuras para as áreas que não

participarem da atual. Quem terá ciência da auditoria em andamento? Uma vez que, em muitos casos, o conhecimento da auditoria pode mudar o comportamento dos usuários, o que impactará no resultado da auditoria, ao mesmo tempo em que todos deverão estar cientes da colaboração para permitir os acessos às informações necessárias.

O planejamento : uma auditoria bem-sucedida deve passar pela preparação da equipe que fará sua execução. São pontos substanciais a essa preparação o conhecimento dos seguintes aspectos:

- **ambiente** : conhecer o ambiente e os relacionamentos dos sistemas;
- **documentação** : análise da documentação e configurações de sistema;
- **resultados de análise de riscos** : entender as classificações de criticidade de sistemas;
- **análise de históricos** : históricos de sistema para procurar mudanças em programas, permissões ou configurações e de incidentes de segurança para perceber tendências de problemas;
- **análise de resultados de testes de penetração** : se aplicados testes de penetração, é necessário analisar o relatório produzido para garantir que a auditoria trate de todos os itens.

Dados de Auditoria – Métodos de Coleta : não há como fazer análise antes da coleta das informações, vejamos algumas maneiras de se coletar a informação:

- **questionários** : aplicar questionários preparados para gerentes ou para usuários;
- **entrevistas** : entender as operações de todas as partes;
- **observação** : diferença entre os procedimentos teóricos e os executados;
- **listas de verificação** : garantir que a coleta de informações atinja todas as áreas;
- **documentação de revisão** : avalia atualidade, aderência e completude;
- **configurações de revisão** : avalia procedimentos de gerenciamento

de mudança e a adequação dos controles, regras e esquemas;
- **política de revisão** : avalia a relevância, atualidade e completude de políticas;
- **testes de segurança** : testes de vulnerabilidade e de penetração produzem informações técnicas que determinam as vulnerabilidades nos componentes, nas redes e nos aplicativos de segurança.

Relatório de auditoria : após a conclusão das atividades de coleta, a auditoria ainda tem as seguintes tarefas a realizar: análise de dados, geração do relatório de auditoria e uma apresentação das descobertas à gerência.

A maioria dos relatórios de auditoria apresentam três seções gerais:

- **Descobertas** : compara as descobertas da auditoria às políticas estabelecidas ou às melhores práticas do setor, indicando os pontos a melhorar;
- **Recomendações** : recomendam como reparar os riscos encontrados, indicando o possível descumprimento de uma política ou processo por parte dos colaboradores. Recomendações de auditoria devem incluir:
  ○ **Linha de tempo para implementação** : cada recomendação deverá ter um prazo sugerido, baseado nas criticidades;
  ○ **Nível de risco** : indicar o nível de risco enfrentado pela organização;
  ○ **Resposta à gerência** : espaço para os responsáveis indicarem os motivos pelos quais as normas e políticas não foram atendidas ou controles não foram usados. Essa resposta pode incluir planos de ação para resolver lacunas em controles.
- **Acompanhamento** : garantir a execução das recomendações pela organização, somente quando necessário.

Monitoramento e Teste de Sistemas de Segurança

Objetivo principal do profissional de segurança da informação é proteger os dados confidenciais da organização contra atacantes, implantando estratégias para controlar acesso a seus sistemas. Embora existam muitos riscos associados à segurança de informação, dois dos mais comuns são: os atacantes que vêm de fora através de acesso não autorizado, código malicioso, cavalos de Troia e malware, bem como de dentro da organização transferindo informações confidenciais para pessoas não autorizadas.

As técnicas empregadas pela área de segurança da informação seguem duas principais estratégias. A primeira é o **monitoramento** , analisando o tráfego e comportamento na rede e a segunda diz respeito às rotinas de **testes** com a finalidade de identificar vulnerabilidades não corrigidas nos sistemas.

Monitoramento de Segurança para Sistemas Computacionais

É necessário selecionar em quais controles se deseja detectar atividades maliciosas. Há várias ferramentas de monitoração de atividades do sistema, que analisam tanto durante quanto depois de sua ocorrência.

O **monitoramento em tempo real** fornece informações sobre o que está acontecendo no momento, que possibilitam conter incidentes e preservar operações de sua organização. Alguns exemplos desse tipo de controle incluem:

- IDS (Intrusion Detection Systems – Sistema de Detecção de Intrusos): observa atividades no momento em que estão acontecendo e aplica suas regras para identificar se as atividades são suspeitas. São sistemas que podem analisar a rede de computadores (Network – NIDS) ou servidores (Hosts – HIDS);
- Monitoramento de integridade de sistema: observa sistemas computacionais, checando se suas alterações são autorizadas.

Outros monitoramentos essenciais são os que mantêm registros históricos de atividades. Alguns exemplos desse tipo de controle incluem:

- Histórico (*logging*) de aplicativo: é necessário que todos aplicativos, que acessem ou modifiquem dados, registrem quem usou ou alterou os dados e quando, armazenando essas informações em *log* ;
- Histórico (*logging*) de sistema: registros dos usuários que acessaram o sistema, quando acessaram e quais ações realizaram.

Sempre que optar pelo monitoramento à base de históricos lembre-se da necessidade de acompanhar os registros para checar possíveis ataques ou atividades indevidas. Os históricos também são importantes para definir o que é um comportamento normal nos sistemas e nas redes da organização.

Um aspecto importante do monitoramento é conseguir diagnosticar se a atividade é um ataque real, simplesmente um ruído ou evento secundário. Nessa execução, monitores de todos os tipos podem cometer dois tipos básicos de enganos:

Falsos positivos : são alertas que indicam comportamento malicioso, embora não sejam eventos de segurança reais. Muitas vezes, esses alarmes falsos são utilizados como distração para desperdiçar esforço administrativo enquanto o administrador ignora o ataque real;

Falsos negativos : é a falha do controle em detectar comportamento suspeito ou em detectar um evento sério. Ele pode ter ocorrido sem ser observado ou o monitor imaginou que o evento não fosse sério, quando na verdade foi.

reflita

Reflita

Um ambiente está monitorando a ação dos usuários na rede, utilizando, para isso, o *firewall* e o NIDS. Essas ferramentas estão configuradas com alertas que indicam as possíveis atividades maliciosas. Você sabe que existe a possibilidade de falsos positivos e falsos negativos. Reflita se você, na condição de responsável pela segurança da informação, preferia enfrentar uma situação de falsos positivos ou falsos negativos.

A configuração de alerta nas ferramentas de monitoração é o maior desafio nessa área e pode ser o diferencial entre o sucesso ou não da segurança de informação.

praticar

Vamos Praticar

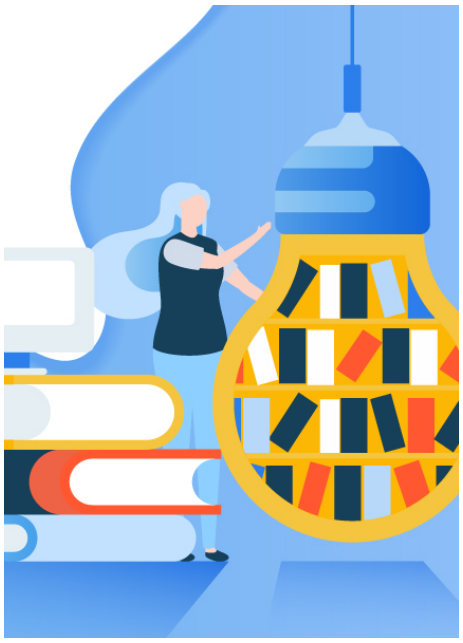
O Wireshark é uma ferramenta que serve para verificar pacotes transmitidos por dispositivos de comunicação. Esse tipo de software é chamado *packet sniffers* . É uma ferramenta poderosa que auxilia os desenvolvedores e administradores de rede, possibilitando uma fácil visualização de possíveis falhas, porém, quando usada de forma indevida, pode trazer várias consequências, como o vazamento de informações ilegais. Selecione a alternativa que indica a função correta do Wireshark, de acordo com a descrição.

- **a)** Auditoria.

- **b)** Teste.
- **c)** Autorização.
- **d)** Monitoramento.
- **e)** Autenticação.

indicações

Material Complementar



LIVRO

Contagem Regressiva até Zero Day: Stuxnet e o Lançamento da Primeira Arma Digital do Mundo

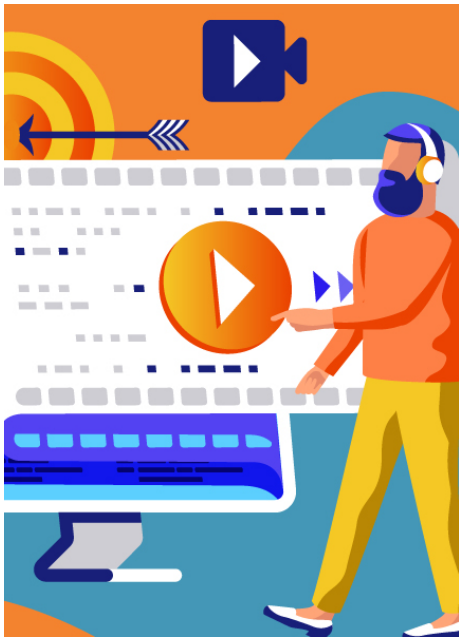
Editora : Brasport

Autor : Kim Zetter

ISBN : 9788574528274

Comentário : o livro aborda o desenvolvimento do *software* malicioso Stuxnet e, mais que isso, apresenta o cenário de uma guerra digital. O livro nos leva ao "mercado cinza" de *exploits zero-day* , que são *malwares* desenvolvidos com tecnologia desconhecida pelas ferramentas de teste e monitoração, em que existe o comércio de *softwares* maliciosos recém-desenvolvidos

e nunca diagnosticados.



FILME

Snowden: Herói ou traidor?

Ano : 2016.

Comentário : o filme conta a história de Snowden, que foi agente de segurança americano e divulgou informação a jornalistas sobre um sistema de coleta de informação que os EUA usam para controlar as pessoas e nações. Nesse filme, vemos a construção de *softwares* maliciosos para a extração de informação e também as regras de segurança para as pessoas que tratam das informações sigilosas.

TRAILER

conclusão

Conclusão

Nesta unidade, aprendemos sobre o desenvolvimento dos *softwares* maliciosos, vírus, *backdoor, worm* etc. e também a diferenciar as técnicas empregadas, as criticidades em cada um e a necessidade de uma ferramenta de contenção. Entendemos a necessidade de um controle de acesso e como isso está envolvido com as políticas e normas de segurança de uma empresa. Aprendemos também como criar políticas em uma rede para obrigar usuários e dispositivos a estar aderentes às normas de uso de computadores no uso dessa rede, sendo a autoridade nisso o NAS, que analisa se os *softwares* básicos de proteção estão instalados. Um Sistema Operacional atualizado para liberar acesso à rede e à segurança na computação em nuvem é um cuidado a mais que devemos ter, visto que a maioria das empresas tem aderido a esse serviço. Além disso, aprendemos que para muitas dessas preocupações existem, sendo ferramentas e procedimentos de apoio, como auditoria, testes e monitoração.

referências

Referências Bibliográficas

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002** :

tecnologia da informação: técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306582 . Acesso em: 24 dez. 2019.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação** : com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2015.

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação** . Rio de Janeiro: LTC, 2014.

STALLINGS, W. **Criptografia e segurança de redes** : princípios e práticas. 4. ed. São Paulo: Pearson Education do Brasil, 2015.