8.0 - Auditoria de Sistemas

prof. Fábio Engel

fabioe@utfpr.edu.br

Conteúdo

Auditoria de Sistemas

- **Auditoria de Sistemas**
  - Quando audita um sistema computacional, você verifica como ele foi executado. Em termos simples, você verifica se tudo funciona de acordo com o planejado.
  - Auditoria também constantemente examina a configuração atual de um sistema, como se fosse um instantâneo no tempo, para verificar se está em conformidade com padrões.

Auditoria de Sistemas

- O sistema pode ser auditado manualmente ou por meio de software computacional automatizado. Testes incluem:
  - Entrevista do pessoal.
  - Realização de varreduras de vulnerabilidades.
  - Revisão de controles de acesso de aplicativos e de sistema operacional.
  - Analisar acesso físico aos sistemas.

Auditoria de Sistemas

- Com testes automatizado, 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 computacionais incluem: computadores pessoais, servidores, roteadores e switches e outros.

Auditoria de Sistemas

- Antes de auditar um sistema é preciso criar as políticas e os procedimentos que estabeleçam as regras e os requisitos desse sistema. Ou seja, antes de determinar se algo funcionou, primeiramente será preciso definir como se esperava que funcionasse. Isso é conhecido como **avaliação de sistema**.
- Você avalia todos os componentes de seu sistema e determina como cada um deve funcionar. Isso define suas expectativas de linha de base. Uma vez que tenha isso, você poderá auditá-lo. Você compara o desempenho do sistema a suas expectativas de linha de base para ver se tudo funcionou conforme planejado.

Auditoria e Análise de Segurança

- Auditoria e Análise de Segurança
  - A finalidade de uma auditoria de segurança é garantir que seus sistemas e controles funcionem conforme esperado.
  - Quando analisar seus sistemas, você deverá verificar o seguinte:
    - As políticas de segurança são sólidas e apropriadas para a empresa ou atividade?
    - Existem controles que apóiam suas políticas?
    - Existem implementação e manutenção e efetivas de controle?

Auditoria e Análise de Segurança

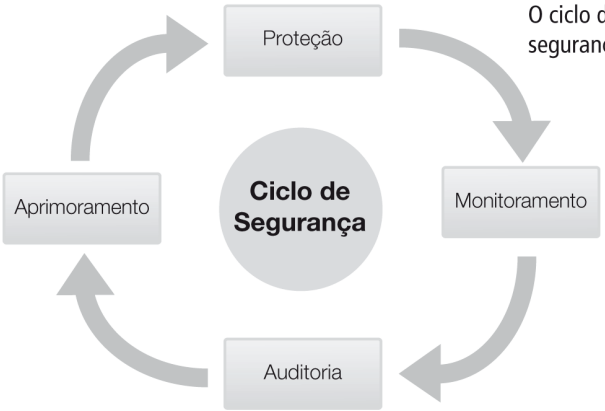
- Controles de segurança colocam limites em atividades que possam impor riscos à sua organização.
- É preciso rever segurança regularmente para garantir que os controles se mantém atualizado e efetivos. Essa revisão inclui as seguintes atividades:
  - **Monitoramento** - Reveja e meça todos os controles para capturar ações e mudanças no sistema.
  - **Auditoria** - Reveja os históricos e o ambiente geral para fornecer análise independente em relação ao funcionamento da política de segurança e dos controles.
  - **Aprimoramento** - Inclua propostas para aprimorar o programa e os controles de segurança nos resultados da auditoria. Esta etapa se aplica à mudanças consideradas aceitas pela gerência.
  - **Proteção** - Garanta que os controles funcionem e protejam o nível de segurança pretendido.

Auditoria e Análise de Segurança

- Embora controles de segurança protejam seus computadores e redes, é preciso garantir que cada um seja necessário e efetivo.
- Cada controle deverá proteger sua organização de uma ameaça específica, é aceitável ter vários controles para a mesma ameaça.
- Um controle não deve custar mais do que a perda em potencial.
  - Pode-se calcular a perda esperada multiplicando a probabilidade de risco pelo custo do ativo.

Auditoria e Análise de Segurança

- Umas das melhores maneiras para evitar desperdício de recursos é seguir o ciclo de revisão de segurança, como mostra a figura abaixo:



O ciclo de revisão de segurança.

Determinando o que é aceitável

- O primeiro passo para colocar os controles de segurança corretos em funcionamento é determinar quais ações são aceitáveis:
  - A política de segurança de sua organização deverá definir ações aceitáveis e não aceitáveis.
  - Sua organização poderá criar seus próprios padrões com base naqueles desenvolvidos ou endossados por agências de padronização.
  - Comunicações e outras ações permitidas por um documento de política serão aceitáveis.
  - Comunicações e outras ações especificamente proibidas em sua política de segurança serão inaceitáveis.

Níveis de permissão

- Níveis de permissão
  - O nível de permissão apropriado para sua organização dependerá de suas necessidades e políticas.
  - É essencial combinar o nível de permissão exigido em sua organização com sua estrutura de segurança. Caso contrário você poderá perder muitos dados e comprometer sua reputação.

Níveis de permissão

- Os níveis de permissão mais comuns são:
  - **Promíscuo** - Tudo é permitido. Esse nível de permissão é adequado para a maioria de usuários domésticos.
  - **Permissivo** - O que não for especificamente proibido é permitido. Esse nível de permissão é adequado para a maioria dos site públicos na Internet, algumas escolas e bibliotecas e muitos centros de treinamento.
  - **Prudente** - Há uma lista razoável de permissões. tudo o que não constar da lista é proibido. Esse nível de permissão é adequado para a maioria das empresas.
  - **Paranóico** - Há poucas permissões. todo o resto é proibido e cuidadosamente monitorado. Esse nível de permissão é adequado para instalações seguras.

Áreas de Auditorias de Segurança

- Áreas de Auditorias de Segurança:
  - Auditorias podem ser muito grandes em escopo e cobrir departamentos ou funções comerciais inteiras. Ou então podem ser estreitas e resolver apenas um sistema ou controle específico.
  - Uma auditoria fornece ao gerenciamento uma avaliação independente sobre se os melhores controles estão em uso e quão bem funcionam.
  - Exemplos:
    - A auditoria pode servir de análise para garantir que sua política de segurança esteja atualizada, seja relevante, comunicada e imposta.
    - Podem testar como sua infraestrutura protege seus dados de aplicativos.
    - Firewall e outros dispositivos podem ser auditados.

Finalidade de Auditorias

- Uma auditoria verifica se os controles:
  - **São apropriados** - O nível de controle de segurança é adequado para o risco que ele enfrenta?
  - **Estão instalados corretamente** - O controle de segurança está no lugar correto e funcionando bem?
  - **Estão atendendo à sua finalidade** - O controle de segurança é efetivo no tratamento do risco o qual foi projetado para enfrentar?

Finalidade de Auditorias

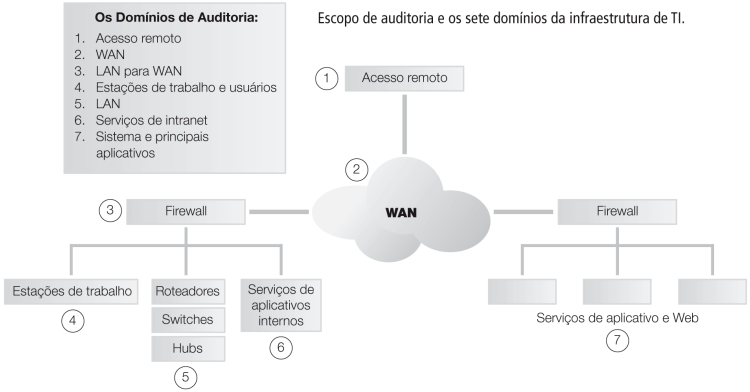
- O relatório de auditoria que os auditores criam deverá recomendar melhorias ou mudanças nos processos, infraestrutura ou outros controles na organização, conforme a necessidade.
- Auditorias são necessárias devido ao potencial de responsabilização, negligência e cumprimento de regulamentação obrigatória e podem expor problemas e oferecer garantia de conformidades.

Plano de auditoria

- Plano de auditoria
  - Ao planejar as atividades para uma auditoria, o auditor primeiro precisará definir os objetivos e determinar que sistemas ou processos de negócios deverá analisar. Também deverá definir quais áreas de segurança verificar.
  - Também será necessário identificar o pessoal - tanto da própria equipe como da organização auditada - que participará da auditoria. Essas pessoas se reunirão e juntarão para conduzir o processo.

Plano de auditoria

- É preciso definir os limites da análise do início do projeto. É fundamental determinar que áreas a auditoria analisará ou não.
- O escopo de uma auditoria pode se espalhar por todos os sete domínios na infraestrutura de TI, como mostra a figura abaixo



Plano de auditoria

- Veja o que você pode esperar de um auditor no decorrer das fases de planejamento e execução:
  - **Estudar o local** - entendimento do ambiente e as interconexões entre sistemas.
  - **Analisar documentação** - análise da documentação e configurações do sistema.
  - **Analisar resultados de análise de riscos** - entendimento da classificação de criticidade de sistemas que sejam um produto de estudos de análise de riscos.
  - **Analisar histórico de servidores** - exame de históricos de sistema para procurar mudanças em programas, permissões ou configurações.
  - **Analisar históricos de incidentes** - análise de históricos de incidentes de segurança para perceber tendências de problemas.
  - **Analisar resultados de testes de penetração** - Quando uma organização realiza testes de penetração, o testador prepara um relatório com as falhas encontradas. O auditor precisará analisar esse relatório e garantir que a auditoria trate de todos os itens.

Padrões de referência de auditoria

- Um **padrão de referência de auditoria** (benchmark) é o padrão pelo qual seu sistema será comparado para determinar se está configurado de forma segura.
- A seguir, você encontrará maneiras comuns de auditar ou analisar sistemas, processos de negócios ou controles de segurança. Todos esses exemplos são as melhores práticas e normalmente são usados como diretrizes para auditar uma empresa ou um processo de negócios.
- A gerência de sua organização pode ter adotado formalmente um dos exemplos a seguir, o que pode ser especialmente verdadeiro se a empresa estiver sujeita a regulamentação ou legislação governamental. Se este for o caso, então o padrão de referência guiará o curso principal de sua auditoria.

Padrões de referência de auditoria

- **ISO 27002** - Documento de melhores práticas, que oferece boas diretrizes para gestão de segurança da informação. Para que uma organização declare conformidade, ela precisará realizar uma auditoria para verificar se todas as provisões são satisfeitas.
- **NIST SP 800** - 37-NIST SP 800-37 é um padrão publicado pelo governo americano especificamente para sistemas computacionais que o governo possua ou opere e inclui tanto uma seção de melhores práticas quanto de auditoria.
- **ITIL** - É a biblioteca de Infraestrutura de Tecnologia de Informação (*Information Technology Infrastructure Library*), conjunto de conceitos e políticas para gestão de infraestrutura, desenvolvimento e operações de tecnologia de informação.

Padrões de referência de auditoria

- Outras organizações desenvolveram diretrizes de auditoria comumente utilizadas. Exemplos:
  - **COBIT** - Os Objetivos de Controle para Informação e Tecnologia Relacionada (*Control Objectives for information and related Technology*) é um conjunto de melhores práticas para gestão de TI, criado pela ISA (*Information Systems Audit*), pela ISACA (*Control Association*) e pelo ITGI (*IT Governance Institute*).
  - **COSO** - O Instituto de Auditores Internos (IIA - *Institute os Internal Auditors*) produz o Comitê de Organizações Patrocinadoras da Comissão Treadway. Essa organização, dirigida por voluntários, fornece conselhos a gerências executivas e entidades de governança sobre aspectos críticos de governança organizacional, ética de negócios, controle interno, gerenciamento de riscos de empresas, fraude e relatórios financeiros.

Dados de Auditoria - Métodos de coleta

- Antes que possa analisar dados, você precisará identificá-los e coletá-los. Existem muitas maneiras de coletá-los, incluindo:
  - Questionários - Preparados tanto para gerentes como para usuários.
  - Entrevistas - Úteis para colher idéias sobre operações de todas as partes.
  - Observação - Refere-se à entrada usada para diferenciar os procedimentos teóricos e os que de fato serão executados.
  - Lista de verificação - Ajudam a garantir que o processo de coleta de informações abranja todas as áreas.
  - Documento de revisão - Avalia atualidade, aderência e completude.
  - Configuração de revisão - Envolver avaliar procedimentos de controle de mudança e a adequação de controles, regras e esquemas.
  - Política de revisão - Envolver avaliar relevância, atualidade e completude de políticas.
  - Testes de segurança - Teste de vulnerabilidade e teste de penetração envolvem reunir informações técnicas para determinar se existem vulnerabilidades nos componentes, nas redes e nos aplicativos de segurança.

Áreas de Auditorias de Segurança

- Áreas críticas que devem ser incluídas em uma auditoria de segurança.

TABELA 7.1 Áreas que você deve incluir em um plano de auditoria

ÁREA	OBJETIVO DE AUDITORIA
Software de antivírus	Aplicativo atualizado, universal
Políticas de acesso a sistemas	Atual com tecnologia
Sistemas de detecção de intrusos e de gerenciamento de eventos	Análises de histórico
Políticas de reforço de sistemas	Portas, serviços
Controles de criptografia	Chaves, uso (criptografia de rede de dados confidenciais)
Planejamento de contingência	Plano de continuidade de negócios (BCP), plano de recuperação de desastre (DRP) e plano de continuidade de operações (COOP)
Manutenção de hardware e software	Acordos de manutenção, serviços, previsão de necessidades futuras
Segurança física	Portas bloqueadas, fontes de alimentação monitoradas
Controle de acesso	Necessidade de saber, menor privilégio
Processo de controle de mudança para gerenciamento de configuração	Documentado, sem mudanças não autorizadas
Proteção de mídia	Idade de mídia, rotulagem, armazenamento, transporte

Verificação de Controle e Gerenciamento de Identidade

- É importante garantir que seus controles de segurança sejam efetivos e confiáveis e funcionem conforme pretendidos.
- Ao auditar um sistema de gerenciamento de identidade, você deverá focalizar estas áreas-chave:
  - **Processo de aprovação** - Quem concede aprovação para solicitações de acesso?
  - **Mecanismos de autenticação** - Que mecanismos são usados para requisitos de segurança específicos?
  - **Política e imposição de senha** - A organização tem uma política efetiva de senha, imposta uniformemente?
  - **Monitoramento** - A organização possui sistemas de monitoramento suficientes para detectar acesso não autorizado?
  - **Sistemas de acesso remoto** - Todos os sistemas são devidamente protegidos com autenticação forte?

Atividades Pós-auditoria

- Depois que as atividade de auditoria forem concluídas, os auditores ainda terão mais trabalho a fazer.
- Tarefas adicionais de auditores incluem:
  - Entrevista de saída
  - Análise de dados
  - Geração de relatório de auditoria
  - Apresentação das descobertas à gerência

Atividades Pós-auditoria

- Entrevista de saída
  - O Auditor realiza uma entrevista de saída com o pessoal-chave, para alertá-los sobre os principais problemas e recomendações que virão mais adiante no relatório de auditoria.
  - Isso permite que a gerência responda rapidamente e atue em questões sérias.
  - Fora esses primeiros alertas, os auditores não deverão fornecer detalhes antes do relatório final, pois poderiam dar uma falsa visão de como a segurança da organização está preparada.

Atividades Pós-auditoria

- Análise de dados
  - Auditores normalmente analisam dados que coletam longe do local da organização, o que permite que analisem tudo o que descobriram e apresentem observações usando um formato de relatório-padrão.
  - Realizar análise de dados em um local externo à empresa auditada pode ajudar a encorajar uma análise imparcial.

Atividades Pós-auditoria

- A maioria dos relatórios de auditoria contém pelo menos três seções gerais:
  - **Descobertas** - Normalmente listadas por nível de conformidade em relação ao nível de referência-padrão.
  - **Recomendações** - Auditores recomendam como reparar os riscos encontrados e relatam o possível descumprimento de uma política ou processo por parte do pessoal. Recomendações devem incluir:
    - **Linha de tempo para implementação** - Recomendações de mudança não devem ter pontas abertas. Cada uma deverá ter um prazo sugerido.
    - **Nível de risco** - Deve-se deixar claro o nível de risco que a organização enfrenta.
    - **Resposta à gerência** - Auditores deverão dar à gerência uma oportunidade para responder a uma cópia de rascunho do relatório de auditoria. Eles deverão então colocar, no relatório final, a resposta, que normalmente esclarece questões e explica por que controles não foram usados.
  - **Acompanhamento** - Quando necessário, auditores deverão agendar uma auditoria de acompanhamento para garantir que a organização tenha executado as recomendações.

Atividades Pós-auditoria

- Apresentação de descobertas
  - Quando os auditores concluem o relatório de auditoria, eles apresentam suas descobertas à organização.
  - Dependendo da estrutura e do tamanho da empresa, a apresentação de descobertas pode ser uma reunião formal ou simplesmente a entrega de um relatório a uma única pessoas.
  - É importante que a organização auditada examine o relatório e faça as mudanças necessárias.

Monitoramento de Segurança

- **Monitoramento de Segurança**
  - O primeiro objetivo de um programa de segurança é detectar comportamento anormal.
  - Sistemas de monitoramento de segurança podem ter natureza técnica, como um sistema de detecção de intrusos (IDS), ou administrativa - por exemplo, observando comportamento de funcionários ou clientes em um circuito fechado de tv.

Monitoramento de Segurança

- Algumas ferramentas e técnicas para monitoramento de segurança incluem as seguintes:
  - **Linhas de base** - Para reconhecer algo como anormal, primeiramente você precisará saber o que é normal.
  - **Alarmes** - Notificam o pessoal de um possível incidente de segurança.
  - **Circuito fechado de tv** - Envolve monitorar e gravar o que as câmeras veem.
  - **Sistemas que detectam comportamento irregular** - Alguns exemplos incluem IDSs e *honeypots*.

- Monitoramento de Segurança para Sistemas Computacionais
  - Assim como existem muitos tipos de controles de monitoramento físico, também existem muitas maneiras de monitorar atividades em sistemas computacionais e rede.
  - Você precisará selecionar os controles que monitoram os muitos aspectos de seu ambiente de computação para detectar atividade maliciosa.
  - Existem diversas ferramentas para ajudá-lo a monitorar atividades de seu sistema, tanto durante quanto depois de sua ocorrência.

- **Monitoramento em tempo real** fornece informações sobre o que está acontecendo no momento. Alguns exemplos incluem:
  - **IDS de servidor** - Um sistema de detecção de intrusos em servidor (HIDS - *Host Intrusion Detection System*) é excelente para "observar" atividades em um computador no momento em que estiver acontecendo. Regras de IDS ajudam a identificar atividade suspeita quase em tempo real.
  - **Monitoramento de integridade de sistema** - Sistemas como Tripwire permitem que você observe sistemas computacionais em busca de mudanças não autorizadas e as informe aos administradores quase em tempo real.

- Monitoramento que não seja em tempo real mantém registros históricos de atividades. Você pode usar esse tipo de monitoramento quando não for tão crítico detectar e responder a incidentes imediatamente. Alguns exemplos desse tipo de controle incluem:
  - **Histórico (logging) de aplicativo** - Todo aplicativo que acesse ou modifique dados sensíveis devem ter históricos que registrem que usou ou alterou os dados e quando.
  - **Histórico (logging) de sistema** - Esse tipo de histórico fornece registros de quem acessou o sistema e quais ações foram realizadas.

- Segue uma lista parcial de atividade que você precisa registrar em histórico:
  - **Atividade baseada em servidor** - Inclui mudanças em sistemas, solicitações de acesso, desempenho, partidas (*startups*) e paradas (*shutdowns*)
  - **Rede e dispositivos de rede** - Inclui acesso, tipo e padrões de tráfego, malware e desempenho.

Questões de Monitoramento

- Questões de Monitoramento:
  - Históricos têm seus custos, precisam de dispositivos físicos para seu armazenamento.
  - Outras questões que impedem o monitoramento:
    - Distribuição espacial - É difícil perceber ataques com históricos, se vierem de uma série de atacantes e por uma ampla área.
    - Redes comutadas - Pode ser mais difícil capturar tráfego em redes muito segmentadas pelo uso de switches e LANs virtuais.
    - Criptografia - Dificulta a elaboração de um histórico, pois monitores não podem ver todos os dados para decidir se são suspeitos.

Questões de Monitoramento

- Questões de Monitoramento:
  - Outras questões que impedem o monitoramento:
    - Criptografia de camada de enlace (WEP e WPA sem fio) - Com esse tipo de criptografia, você criptografa tudo acima da camada de enlace.
    - Criptografia de camada de rede (IPSec e alguns outros protocolos de tunelamento) - Com esse tipo de criptografia, você criptografa tudo acima da camada de rede.
    - Criptografia de camada de aplicativo (SSL, SSH e outros) - Esse tipo de criptografia criptografa acima da camada de transporte.

Histórico de Anomalias

- Histórico de Anomalias:
  - Um aspecto importante do monitoramento é determinar a diferença entre ataques reais em entradas de histórico e atividade que seja simplesmente um ruído ou evento secundário. Ao fazer isso, monitores de todos os tipos cometem dois tipos básicos de enganos:
    - **Falsos positivos** - São alertas que parecem maliciosos, embora não sejam eventos de segurança reais.
    - **Falsos negativos** - Falha do sistema de alarme em detectar um evento sério.

Gerenciamento de Histórico

- Gerenciamento de Histórico
  - Arquivos de histórico podem ajudar a fornecer evidências de atividade normal e anormal de um sistema e oferecer informações valiosas sobre quão bem seus controles estão realizando as respectivas tarefas.
  - Os administradores de segurança e de sistemas precisam considerar vários aspectos para garantir que você mantenha as informações certas e que elas estejam seguras.
    Primeiramente, você deverá armazenar históricos em um local central, para protegê-las e mantê-las à mão para análises completas. Tenha bastante espaço de armazenamento e monitore seus requisitos de espaço de disco para arquivos de histórico.

Gerenciamento de Histórico

- Se um arquivo de histórico ficar cheio, você deverá escolher uma ou mais das três escolhas seguintes, todas ruins:
  - Deixar de fazer histórico.
  - Sobrescrever as entradas mais antigas.
  - Parar de processar (de forma controlada ou por falha).
- Atacantes às vezes enchem um histórico de propósito para causar uma dessas falhas. O dispositivo de armazenamento para seus arquivos de histórico precisa ser grande o suficiente para prevenir isso.

Gerenciamento de Histórico

- Para vincular atividades entre sistemas e históricos, computadores e dispositivos em sua rede precisam ter relógios (*clock*) sincronizados. O Protocolo de Hora de Rede (NTP - *Network Time Protocol*) sincroniza horário para todo computador e dispositivo que o suporte.
- Para prevenir sobrescrita ou modificação, alguns sistemas gravam históricos em um CD-ROM ou outro dispositivo de somente escrita.

Tipos de Informação de Histórico a Capturar

- Tipos de informação de histórico a capturar
  - Você deverá registrar toda atividade suspeita, erros, tentativas de acesso não autorizado e acesso a informações confidenciais. Como resultado, você não apenas rastreará incidentes, mas também manterá seus usuários responsáveis por suas atividades.

Tipos de Informação de Histórico a Capturar

- O **Sistema de Informação de Segurança e Gerenciamento de Evento (SIEM)- Security Information and Event Management** ajuda organizações a gerenciar os arquivos de histórico e fornece uma plataforma comum para capturar e analisar entradas.
  - Organizações coletam históricos de diferentes fontes, além disso possuem várias marcas ou versões diferentes dessas fontes.
  - Dispositivos de coleta e análise de SIEM pegam os dados de históricos em qualquer formato que tenham sido criados, de qualquer dispositivo que os crie e os padronizam para um formato comum.

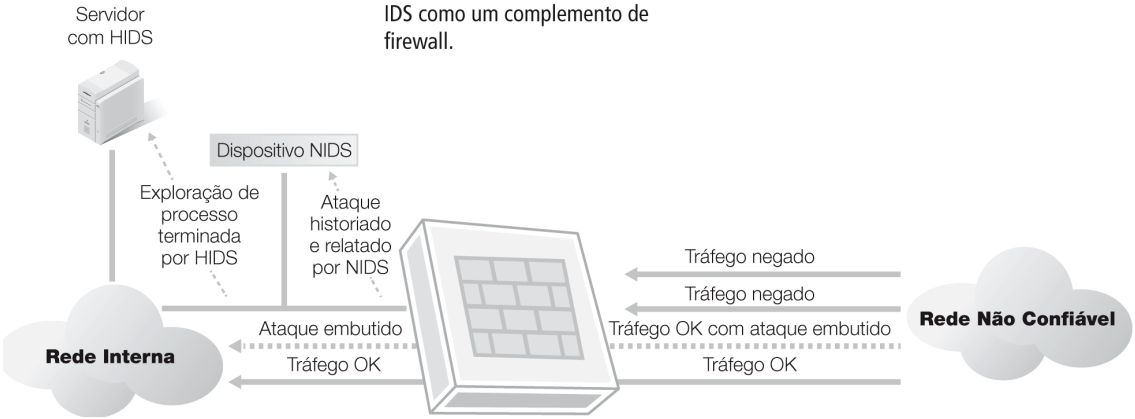
Como verificar controles de segurança

- Como verificar controles de segurança
  - Uma classe específica de controles de monitoramento pode fornecer uma camada de segurança muito boa. Essa classe monitora atividade de rede e de sistema para detectar comportamento incomum ou suspeito.
  - Alguns controles nessa classe podem ainda responder a atividades suspeitas detectadas e possivelmente interromper um ataque em andamento.
  - Controles que monitoram atividade incluem sistemas de detecção de intrusos (IDSs), sistemas de prevenção de intrusos (IPSs) e firewalls.

Como verificar controles de segurança

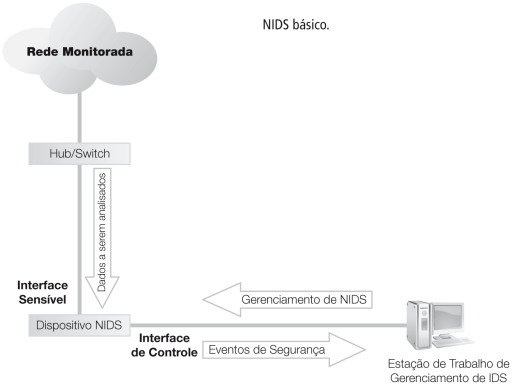
- Sistemas de Detecção de Intrusos (IDS)
  - Um dos mais comuns mecanismos de defesa em camadas é colocar um IDs atrás de um firewall para fornecer maior segurança.
    - Um sistema de detecção de intrusos de rede (NIDS - Network IDS) monitora o tráfego que passa pelo firewall para detectar atividade maliciosa.
    - Um sistema baseado em computador (HIDS) faz o mesmo para tráfego destinado a um computador ou dispositivo em particular.
  - A figura a seguir mostra uma rede com um NIDS e um dispositivo HIDS.

Como verificar controles de segurança



Como verificar controles de segurança

- Você poderá conectar um NIDS a um switch ou a um hub. O IDS então capturará todo tráfego no switch e o analisará para detectar atividade não autorizada.



Métodos de Análise

- Métodos de Análise
  - Dispositivos de monitoramento e detecção precisam examinar e analisar atividade para saber quando disparar um alarme.
  - Os dispositivos podem usar vários métodos para analisar tráfego e atividade. Alguns métodos comparam pacotes ou endereços de rede a regras, enquanto outros examinam a frequência e o tipo de atividade. Esses dois métodos são chamados de IDSs baseados em padrão (assinatura) e em anomalia (estatística).

Métodos de Análise

- **IDSs baseados em padrão (assinatura)**, conhecidos como detecção baseada em regra.
  - Utilizam casamento de padrões com estado para comparar o tráfego atual com padrões de atividade (assinaturas) de ataques de rede conhecidos.
  - Sistemas de casamento padrão varrem pacotes para ver se sequências de bytes específicos, conhecidas como assinaturas, casam com a assinatura de ataques conhecidos, geralmente relacionados com certo serviço e porta.
  - Sistema de casamento com estado aprimora o casamento de padrões procurando sequências específicas que aparecem em vários pacotes em um fluxo de tráfego, em vez de apenas pacotes individuais.

Métodos de Análise

- **IDSs baseados em anomalia**, as vezes chamados de sistemas baseados em perfil.
  - Comparam a atividade atual com perfis armazenados de atividade normal (esperada).
  - Sua precisão é a mesma que a de sua definição de "atividade normal".
  - Uma vez que você defina o que é uma operação normal de sistema, o IDS irá comparar a atividade atual com sua definição de atividade normal.
  - Qualquer aspecto que o IDS considere anormal será um candidato à análise e resposta.

IDSs baseados em anomalia

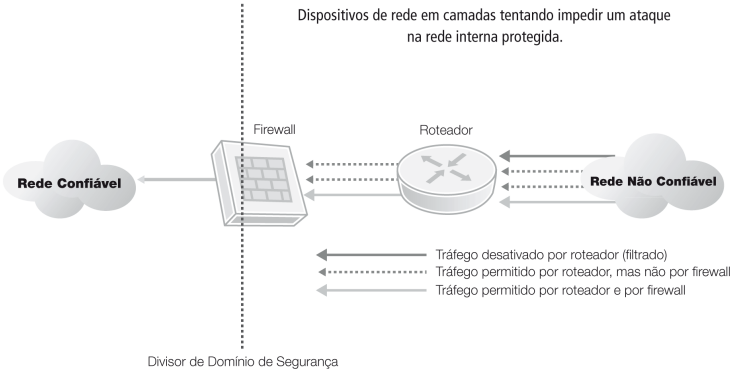
- Os métodos mais comuns de detecção de anomalias incluem:
  - **Métodos baseados em estatística** - Desenvolvem linhas de base de tráfego normal e de atividade de rede. O dispositivo cria um alerta quando identifica um desvio. Esse métodos podem pegar ataques desconhecidos, mas falsos positivos acontecem com frequência.
  - **Métodos baseados em tráfego** - Sinalizam um alerta quando identificam qualquer desvio inaceitável a partir de um comportamento esperado com base em tráfego. Também podem detectar ataques desconhecidos e inundações.
  - **Padrão e protocolo** - Outra forma de identificar ataques sem uma assinatura é procurar desvios a partir de protocolos. Funciona para protocolos bem definidos, mas pode causar falsos positivos para os não tão bem definidos.

IDSs baseados em anomalia

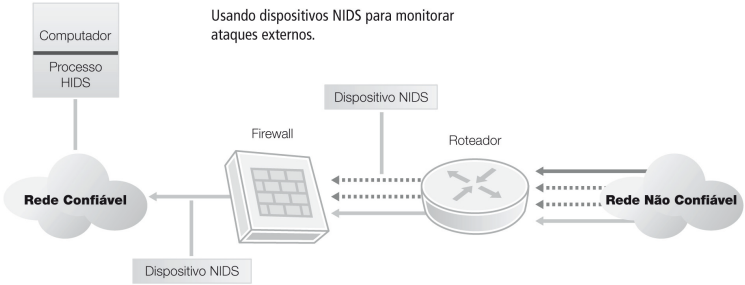
- Os métodos mais comuns de detecção de anomalias incluem:
  - **Métodos baseados em estatística** - Desenvolvem linhas de base de tráfego normal e de atividade de rede. O dispositivo cria um alerta quando identifica um desvio. Esse métodos podem pegar ataques desconhecidos, mas falsos positivos acontecem com frequência.
  - **Métodos baseados em tráfego** - Sinalizam um alerta quando identificam qualquer desvio inaceitável a partir de um comportamento esperado com base em tráfego. Também podem detectar ataques desconhecidos e inundações.
  - **Padrão e protocolo** - Outra forma de identificar ataques sem uma assinatura é procurar desvios a partir de protocolos. Funciona para protocolos bem definidos, mas pode causar falsos positivos para os não tão bem definidos.

- **HIDS**
  - Aumenta a proteção do seus sistema inteiro, vigiando processos sensíveis em um computador, também chamado de host. Geralmente possuem as qualidades:
    - Normalmente são processos ou serviços de software projetados para executar em computadores servidores.
    - Interceptam e examinam chamadas de sistemas ou processos específicos (banco de dados e servidores web, por exemplo) em busca de padrões ou comportamento que normalmente não devem ser permitidos.
    - Processos (*daemons*) HIDS podem tomar uma ação predefinida, como interromper ou relatar a infração.

- Defesas em Camadas: Controle de acesso a rede
  - A melhor defesa é ter várias camadas de controles em funcionamento. A figura abaixo mostra como dispositivos de rede funcionam em múltiplas camadas para tentar impedir um ataque na rede interna protegida. O roteador detecta e impede o tráfego, e o firewall detecta e evita o tráfego indesejado.



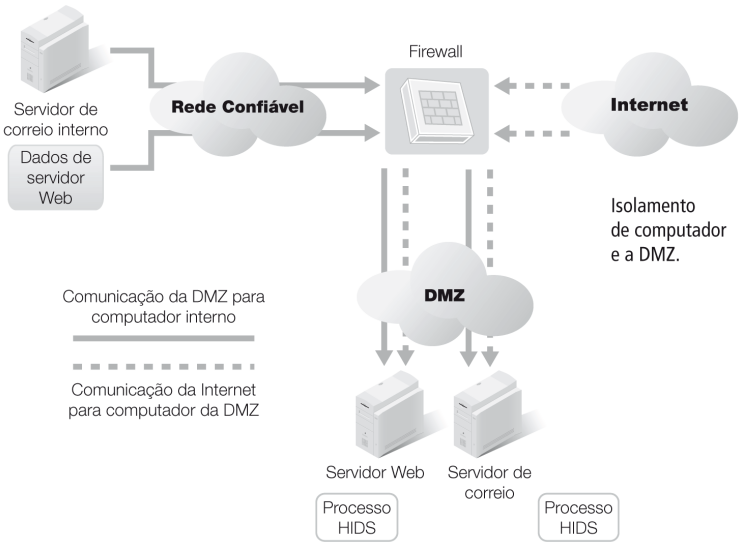
- Verificações de Controle: Detecção de Intrusão
  - Um NIDS é um componente importante em qualquer estratégia de defesa em múltiplas camadas. A figura abaixo mostra como ele pode monitorar ataques externos:



Isolamento de Computador (*host*)

- Isolamento de Computador *host*
  - Alguns servidores ou computadores precisam estar abertos para a Internet, por exemplo, os servidores web.
    - Você deseja que qualquer usuário possas acessar seu servidor web, mas não quer qualquer um possa chegar até sua rede interna.
  - Uma solução simples é isolar os computadores conectados à Internet do restante da rede. Isolamento de computador isola um ou mais computadores hospedeiros das redes internas e cria uma **zona desmilitarizada - DMZ**. Veja a figura a seguir.

Isolamento de Computador (*host*)



Isolamento de Computador (*host*)

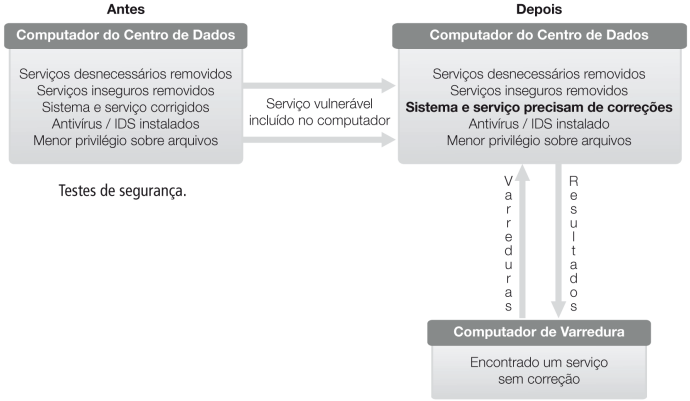
- Uma DMZ é uma sub-rede física ou lógica que contém e expõe serviços externos de uma organização a uma rede maior, não confiável, normalmente a Internet.
- Tráfego externo, vindo da Internet não é confiável, é permitido somente na DMZ, na qual ele pode chegar a certos serviços da empresa.
- Os aplicativos web na DMZ, então, acessam a rede interna confiável, mas impedem que o usuário de fora entre diretamente nela.

Reforço de Sistema

- Reforço de Sistema
  - É importante que administradores de segurança passem por um processo, chamado de reforço *hardening*, para mudar configurações de hardware e software para tornar computadores e dispositivos mais seguros possíveis. Para isso:
    - Desative serviços desnecessários
    - Mantenha atualizado e faça varreduras periódicas com o antivírus.

- Monitoramento e Teste de Sistemas de Segurança
  - Por mais difícil que seja proteger um sistema fechado, a tarefa se torna bem mais difícil quando sua rede se conecta à Internet. Dois dos riscos mais comuns são:
    - Atacantes que venham de fora, com acesso não autorizado, código malicioso e malwares.
    - Informações confidenciais que vazam de dentro da organização para pessoas não autorizadas e que podem prejudicar a empresa.

- Teste
  - Tem como finalidade identificar vulnerabilidade não corrigidas em um sistema, que pode ter sido seguro em algum momento, mas o acréscimo de um novo serviço ou aplicativo pode tê-lo tornado vulnerável.



Monitoramento e Teste de Sistemas de Segurança

- A frequência de seus testes dependerá de fatores como volatilidade (taxa de mudanças) e a sensibilidade ou criticidade do sistema.
- Novos testes devem ser agendados:
  - Durante a fase de certificação de segurança.
  - Após mudanças significativas em sistemas (atualizações de nova tecnologia, mudanças em aplicativos).
  - Novas ameaças.
  - Durante auditorias de sistema.
  - Periodicamente, dependendo da natureza do sistema.
  - Uma vez por ano em sistemas críticos.

Roteiro de Testes

- Tratando-se de testes, um profissional de segurança pode ter seu próprio roteiro de atividades. As atividades mais comuns incluem:
  - Reconhecimento - Envolve analisar o sistema para descobrir o máximo possível sobre a organização, seus sistemas e redes. Recursos públicos como WHOIS e DIG (*Domain Information Groper*) podem ser utilizados.
  - Mapeamento de rede - Usa ferramentas para determinar o esquema e os serviços que estão funcionando nos sistemas e redes da organização.
  - Teste de vulnerabilidade - Envolve descobrir todas as falhas em um sistema e determinar que locais podem ser pontos de ataque.
  - Teste de penetração - Nessa fase, você tenta explorar uma falha no sistema e provar que um atacante pode invadi-lo com sucesso.
  - Atividades de atenuação - Reduzem ou enfrentam vulnerabilidades encontradas em testes de penetração ou de vulnerabilidade.

Referências

- Fundamentos de Segurança de Sistemas de Informação - David Kim. Michael G. Solomon