FOCO NO MERCADO DE TRABALHO

TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

QUAIS TÉCNICAS E FERRAMENTAS UTILIZAR EM UMA AUDITORIA?

As técnicas e ferramentas utilizadas em uma auditoria de sistemas envolvem interação com as pessoas, análises manuais e análises técnicas com uso de ferramentas.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você já montou um planejamento para melhorar a segurança do provedor de nuvem, que está crescendo de uma forma muito rápida. As ações de implantação dos controles foram adiante e agora você deve planejar as técnicas e ferramentas que serão utilizadas na auditoria.

Os controles implantados no data center foram resultados da avaliação de riscos, que direcionaram as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos. Além dos riscos, a definição dos controles foi feita a partir de requisitos que direcionam a seleção e implementação de controles e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa, como a norma de certificação de data centers TIA-942, o padrão de segurança PCI DSS da indústria de cartões de pagamento e as melhores práticas de gerenciamento de serviços ITIL.

O primeiro ponto da auditoria é a realização de uma avaliação de riscos, para que todos os riscos do escopo referente ao datacenter tenham sido mapeados. Na avaliação de riscos, devem ser identificados e mapeados ameaças, agentes de ameaças, ativos, suas vulnerabilidades, e calculados a probabilidade e os impactos. Os ativos são:

- A área segura.
- Os *racks* com os servidores e os equipamentos de comunicação.
- Os administradores de sistemas.
- As máquinas virtuais.
- Sistemas operacionais disponibilizados para os clientes.
- Sistema de provisionamento de acesso aos clientes.

Após a avaliação dos riscos, o tratamento dos riscos pode se basear nos controles do TIA-942, PCI DSS, ABNT NBR ISO/IEC 27002, NIST *Cybersecurity Framework*, ITIL e COBIT, entre outros, focando nestes ativos. Os controles das diferentes normas, padrões e frameworks são equivalentes e complementares.

A verificação dos controles pode ser feita pensando nos controles técnicos, físicos e processuais, que são utilizados pela empresa.

Os principais controles existentes na empresa devem estar cumprindo os objetivos de, pelo menos:

- Políticas de segurança da informação.
- Organização da segurança da informação.
- Segurança em recursos humanos.
- Gestão de ativos.
- Controle de acesso.
- Criptografia.
- Segurança física e do ambiente.
- Segurança nas operações.
- Segurança nas comunicações.
- Aquisição, desenvolvimento e manutenção de sistemas.
- Relacionamento na cadeia de suprimento.

As técnicas e ferramentas para a auditoria no provedor de nuvem podem incluir, pelo menos:

- Análise das políticas, processos e procedimentos de segurança e privacidade.
- Entrevistas com todas as áreas da empresa para percepção sobre se a política de segurança é de conhecimento organizacional e se está sendo seguida.
- Visita ao data center para analisar a segurança física.
- Análise de configuração do *firewall*.
- Análise do fluxo para gestão de identidades.
- *Pentest* para identificar vulnerabilidades do ambiente.
- Análise de *logs* do banco de dados.
- Análise dos relatórios do IDS/IPS.
- Análise dos antivírus.
- Análise de código do sistema corporativo.

- Teste de *phishing*.

Sobre a segurança física, no exemplo do PCI DSS, um requisito é que “haja câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual a áreas sensíveis. Analise os dados coletados e relacione com outras entradas. Armazene, por pelo menos três meses, a menos que seja restringido de outra forma pela lei”.

Os procedimentos de testes recomendados são:

> Verifique se câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) foram implantados para monitorar os pontos de entrada/saída das áreas sensíveis. Verifique se câmeras de vídeo ou outros mecanismos de controle de acesso (ou ambos) estão protegidos contra adulteração ou desativação. Verifique se câmeras de vídeo e/ou outros mecanismos de controle de acesso são monitorados, e se os dados são armazenados por, pelo menos, três meses.
> — (PCI DSS, 2013, p. 82 -83)

A orientação para a avaliação pelo PCI DSS é:

> Ao investigar violações físicas, esses controles podem ajudar a identificar indivíduos que acessaram fisicamente as áreas confidenciais, bem como quando eles entraram e saíram. Criminosos que tentam obter acesso físico às áreas confidenciais muitas vezes tentarão desativar ou desviar os controles de monitoramento. Para proteger estes controles contra adulterações, câmeras de vídeo podem ser posicionadas de forma que fiquem fora de alcance e/ou sejam monitoradas para detectar falsificações. Da mesma forma, os mecanismos de controle de acesso podem ser monitorados ou ter proteções físicas instaladas para evitar que sejam danificados ou desativados por indivíduos mal-intencionados. Exemplos de áreas confidenciais incluem salas do servidor do banco de dados corporativo, salas do setor administrativo em local de revenda que armazene dados do titular do cartão e áreas de armazenamento de grandes quantidades de dados do titular do cartão. As áreas confidenciais devem ser identificadas por cada organização para garantir que os controles de monitoramento físicos adequados sejam implementados.
> — (PCI DSS, 2013, p. 82 - 83)

AVANÇANDO NA PRÁTICA

AUDITANDO MINHA EMPRESA QUE FOI CONTAMINADA POR UM *WORM*

Apesar de todos os controles preventivos implantados na sua empresa, ela foi alvo de um ataque de *worm* que paralisou a empresa por várias horas, causando um prejuízo grande. Você irá conduzir uma auditoria no perímetro da rede, mais especificamente no *firewall*, para verificar se o controle está eficiente e eficaz. O que deve ser considerado nesta auditoria, em termos de técnicas e ferramentas?

RESOLUÇÃO

As técnicas e ferramentas relacionadas ao *firewall* são:

- Avaliar os padrões de configuração do *firewall*.
- Avaliar se há um processo formal para testar e aprovar todas as conexões de redes e alterações nas configurações do *firewall*.
- Conversar com o responsável pelo *firewall* e verificar os registros em busca das aprovações e testes.
- Analisar o diagrama de rede para validar as conexões existentes.
- Analisar se o diagrama de rede está atualizado.
- Analisar o diagrama de rede com as configurações do *firewall*.
- Analisar se o gerenciamento do *firewall* está formalizado quanto às funções e responsabilidades.
- Analisar a documentação em busca das aprovações para cada serviço, protocolo e porta configurada no *firewall*.
- Identificar serviços, protocolos e portas não seguros permitidos.
- Analisar se os recursos de segurança estão implementados para cada porta, serviço e protocolo não seguros.
- Verificar se há uma formalização de que uma revisão e análise das regras do *firewall* devem ser feitas a cada seis meses.
- Conversar com o responsável pelo *firewall* para verificar se ele fez a revisão e análise das regras do *firewall* nos últimos seis meses.
- Analisar os logs do *firewall* em busca de informações específicas do *worm*.