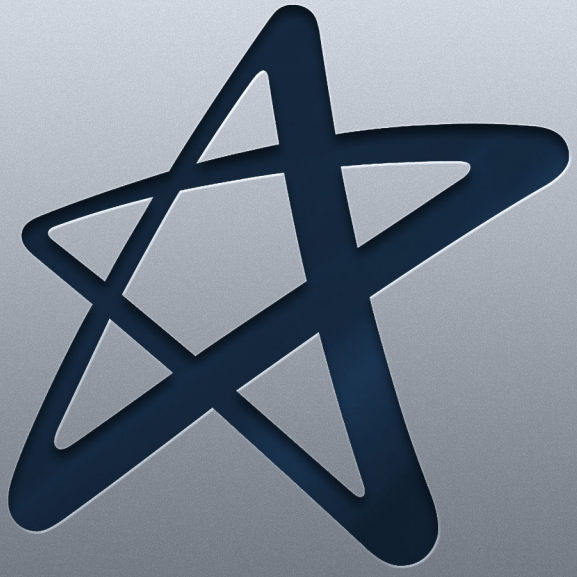
Computação em Nuvem



Cruzeiro do Sul Virtual
Educação a distância

Material Teórico

Segurança de Computação em Nuvem

Responsável pelo Conteúdo:
Prof. Esp. Allan Piter Pressi

Revisão Textual:
Prof.ª Me. Natalia Conti

v1.1

UNIDADE Segurança de Computação em Nuvem

- Protegendo Serviços na Nuvem;
- Implementando o Gerenciamento de Identidades;
- Criptografando Dados;
- Conclusão.

OBJETIVOS DE APRENDIZADO

- Entender como a segurança deve fazer parte de qualquer projeto de computação em nuvem;
- Entender como os provedores lidam com a segurança e quais os impactos para a governança corporativa.

Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:

Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como seu "momento do estudo";
- ✓ Procure se alimentar e se hidratar quando for estudar; lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo;
- ✓ No material de cada Unidade, há leituras indicadas e, entre elas, artigos científicos, livros, vídeos e *sites* para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados;
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e de aprendizagem.

Protegendo Serviços na Nuvem

Um gerente de TI pensando sobre o impacto da computação em nuvem na corporação se preocupa com a segurança em primeiro, segundo e terceiro lugar.

Se você está olhando para criar uma nuvem privada ou aproveitando uma nuvem pública, você precisa ter uma estratégia de segurança.

Sem um ambiente é seguro, não compensaria à organização implementar a computação em nuvem.

Figura 1
Fonte: iStock/GettyImages

Mesmo que sua organização de TI já tenha uma estratégia de segurança bem projetada, questões relevantes surgirão com a computação em nuvem.

Portanto, sua estratégia tem que levar em consideração este modelo diferente de computação. Na verdade, você quer ter certeza de que sua estratégia de segurança de TI está alinhada com sua estratégia de segurança na nuvem.

Cada um dos provedores de serviços de nuvem tem seu próprio modo de gerenciar a segurança. Eles podem ser compatíveis com o plano de conformidade e segurança geral do seu negócio.

Por outro lado, a abordagem de segurança pode entrar em conflito com as regras da sua empresa. Nenhum órgão de governança aceitará a desculpa de que você simplesmente não sabia como seu provedor protegia suas informações.

Convém considerar como as informações e a tecnologia da sua empresa será integrada à estratégia de segurança em computação em nuvem.

Colocando Segurança na Nuvem

Começamos com uma lista de problemas e perguntas que podem contribuir para a organização enquadrar a sua maneira de entender a importância da segurança de uma perspectiva de computação em nuvem.

Aqui estão as questões de segurança mais críticas para perguntar ao potencial provedor de nuvem:

- Quais são a arquitetura e a política de segurança do provedor de nuvem?
- O provedor de nuvem usa um terceiro para avaliar seus próprios riscos de segurança?
- O provedor de nuvem entende suas responsabilidades de governança? Questões como transferências de dados transfronteiriços?
- Qual é a abrangência do contrato de nível de serviço entre você e o provedor de nuvem?

- O provedor de nuvem entende sua necessidade de preservação e proteção de dados?
- Onde seus dados estão fisicamente? Você tem do provedor da nuvem a garantia de que seus dados permaneceram privados?
- O seu provedor de nuvem separa (particiona) seus dados, aplicativos, e/ou ferramentas de gerenciamento de outros usuários de seus serviços em nuvem?
- Existem penalidades claras para uma violação de dados ou sistema?
- A portabilidade de dados faz parte do serviço fornecido pelo fornecedor da nuvem?
- O provedor de nuvem tem uma linha de base de segurança?
- Você tem permissão para inspecionar a instalação da nuvem?
- O seu provedor de nuvem tem um gerenciamento de *patches* bem implementado? Políticas e procedimentos?
- O provedor de nuvem tem *firewalls* de nível de aplicativo e outras ferramentas que ajudam a manter seu aplicativo ou código seguro?
- O provedor de nuvem pode manter informações de segurança, como chaves criptográficas privadas?
- O provedor de nuvem fornece criptografia e gerenciamento de chaves?
- O provedor de nuvem tem uma identidade bem definida e bem executada e arquitetura de gerenciamento de acesso?
- O *single sign-on* foi implementado para os clientes de um provedor de nuvem?

Você provavelmente está se perguntando se é necessário fazer todas essas perguntas. É sua obrigação de manter sua empresa segura.

Enquanto você pode ser diretamente responsável para a estratégia de segurança da sua empresa, você também precisa de um bom entendimento como um provedor de nuvem pode abordar o tópico.

Mas, novamente, nada é tão simples. Muitas grandes empresas estão implementando nuvens privadas ou híbridas, essencialmente estão transformando seus *data centers* e adotando as características de um recurso escalonável de autoatendimento.

No entanto, até mesmo uma nuvem privada pode ser um desafio para a segurança tradicional, que tende a assumir um ambiente mais estático e controlado.

Não pense que você tem mais controle sobre seu destino de segurança se tiver sua própria nuvem.

Uma organização de TI deve garantir o equilíbrio certo entre proteção, privacidade e acessibilidade a recursos-chave - seja nos *datacenter* tradicionais, na nuvem privada ou na nuvem pública.

Medidas de segurança para monitoramento e controle de acesso e gerenciamento de identidade e a rede precisam ser mantidos de forma consistente em todo o *datacenter* interno e ambiente de nuvem híbrida.

A segurança de TI é uma área muito complicada da computação em nuvem, por três razões:

- Você estará confiando em sua segurança para o provedor de nuvem. Se esse provedor não fez um bom trabalho assegurando seu próprio ambiente, você pode estar com problemas.
- A segurança de TI é difícil de monitorar e os problemas podem não ser aparentes até que algo dê errado.
- Medir a qualidade da abordagem de um fornecedor para a segurança é difícil porque muitos provedores de nuvem não expõem sua infraestrutura para clientes.

Entendendo os riscos de segurança

A segurança na nuvem precisa fazer parte da estratégia geral de segurança de sua empresa.

Figura 2
Fonte: iStock/GettyImages

A maioria das empresas atribui alta prioridade ao teste e monitoramento de ameaças ao seu *data center*, edifícios, pessoas e informações.

Os riscos, ameaças e violações de segurança podem surgir de muitas formas e de muitos lugares, e muitas empresas adotam uma abordagem abrangente de segurança e gestão em TI e negócios. Por exemplo, muitas empresas usam tecnologia que rastreia a identidade de alguém se essa pessoa entra na empresa ou se está acessando informações corporativas, seja de perímetros da empresa ou de qualquer local externo.

Uma empresa que planeje proteger seu ambiente de TI geralmente se concentrará na ampla gama de vulnerabilidades potenciais de seu *data center*, bem como em maneiras de proteger informações corporativas, de clientes e de parceiros confidenciais, estando sempre localizada.

Os aplicativos de *software* de uma empresa podem incluir muitas proteções de nível de aplicativo e dados (como autenticação, autorização e criptografia), mas há muitas situações em que essas proteções não são suficientes.

As questões a seguir fornecem uma visão geral dos tipos de riscos de segurança que as empresas devem considerar em qualquer ambiente de TI, incluindo a nuvem.

Mesmo quando os operadores de nuvem têm boa segurança (física, rede, sistema operacional, infraestrutura de comunicação), é responsabilidade da empresa proteger seus aplicativos e informações.

Os serviços de segurança no nível da aplicação e da infraestrutura devem ser uma consideração importante para as organizações.

Dada a importância da segurança no ambiente de nuvem, você pode assumir que um provedor de serviços de nuvem importante teria um conjunto de acordos de nível de serviço para seus clientes. De fato, muitos dos padrões dos acordos são destinados a proteger o provedor de serviços - não o cliente. Portanto, uma empresa realmente precisa entender o contrato.

Os riscos são mais baixos se você estiver usando o armazenamento temporariamente do que se você usar um serviço de nuvem como um substituto para um serviço crítico que toca seus clientes.

Atualmente, a indústria de TI enfrenta um problema: abordagens de segurança (incluindo segurança do perímetro) estão se tornando menos eficazes.

Para entender porque você deve saber como surgem as ameaças de segurança, cerca de 70% das violações de segurança são causadas por pessoas de dentro da organização.

O ambiente de nuvem pode ter alguns dos mesmos problemas. Afinal, uma nuvem é gerenciada por pessoas que podem ser tentadas a violar segurança.

Se a sua empresa vai usar um serviço de nuvem, você precisa ter um planejamento para lidar com ameaças internas e externas.

A possibilidade de que pessoas de dentro abram uma porta para um *hacker* ou montem um ataque deixa claro que a segurança do perímetro por si só nunca será suficiente.

Uma pequena história

Inicialmente PCs não tinham segurança alguma, apenas um sistema de senha e permissões foi implemetado para garantir a segurança em toda a rede com base apenas no *login*. Neste contexto a segurança é simples e com um pequeno grau de proteção do perímetro de segurança ao redor da rede de computadores. Muitos produtos de segurança que as organizações implantam como *firewalls* e redes privadas virtuais (VPNs), que são linhas de comunicações criptografadas, estes e outros componentes também são produtos de segurança de perímetro.
Eles melhoram a segurança do perímetro, que é um pouco como tapar buracos na parede do castelo. Com o advento das redes, no entanto, um sistema operacional pode ser artificialmente estendido para trabalhar em uma rede. Com virtualização de tudo, desde servidores a redes, armazenamento e aplicações, o problema fica ainda mais complicado.

Reduzindo violações de segurança na nuvem

Certifique-se de que o provedor de nuvem tenha adotado uma abordagem estruturada e modelo de segurança próprio. Em geral, siga estas etapas para reduzir o risco de sofrer violações de segurança:

1. Autentique todas as pessoas que acessam a rede.

2. Enquadre todas as permissões de acesso para que os usuários tenham acesso apenas aos aplicativos e dados que eles receberam permissão específica para acessar.
3. Autentique todo o *software* em execução em qualquer computador - e todas as alterações para tal *software*. Isso inclui *software* ou serviços em execução na nuvem.

   Seu provedor de nuvem precisa automatizar e autenticar patches de *software* de alterações de configuração, bem como gerenciar os *patches* de segurança em um caminho ativo.

   Por que isso é tão importante de entender? Muitos serviços em nuvem e as interrupções do provedor normalmente vêm de erros de configuração. Se em um programa de nuvem a usuária não atualiza a segurança, seu produto pode estar em risco.
4. Formalizar o processo de solicitação de permissão para acessar dados ou aplicações. Isso se aplica aos seus próprios sistemas internos e aos serviços que exigem que coloque seus dados na nuvem.
5. Monitore toda a atividade de rede e registre todas as atividades incomuns. Na maioria dos casos, você deve implantar a tecnologia de detecção de intrusos. Embora seu provedor de serviços de nuvem possa permitir que você monitore em seu ambiente, você deve ter uma visão independente. Isto é especialmente importante para a conformidade.
6. Registre toda a atividade do usuário e atividade do programa e analise-a quanto a problemas e comportamentos inesperados.
7. Criptografe, até o ponto de uso, todos os dados valiosos que precisam de proteção.
8. Verifique regularmente a rede em busca de vulnerabilidades em todos os *softwares* expostos à *Internet* ou a qualquer usuário externo.

Se você acha que essas etapas são fáceis, não sabe como é complexo implementar todas essas regras em uma grande rede. Poucas redes chegam perto deste nível de proteção. Quando você considera um provedor de nuvem, essa lista de recursos e proteção deve ser observado no provedor selecionado.

As soluções pontuais geralmente cobrem vulnerabilidades específicas:

- Os *firewalls* protegem a rede interna da *Internet*.
- O *software* antivírus protege computadores individuais contra vírus conhecidos.
- VPNs protegem conexões externas que entram na rede.

Esses produtos reduzem o risco de ameaças específicas, mas não são integrados pela abordagem à segurança de TI. No momento, essa abordagem não existe fora do domínio de organizações governamentais, como a Agência Nacional de Segurança e pode não existir dentro dessas organizações também.

Como os serviços de nuvem o mercado amadurece, fornecedores bem-sucedidos terão que fornecer esse tipo de aproximação.

Mas alguns produtos importantes podem contribuir significativamente para a construção de uma plataforma de segurança de TI integrada. Eles vêm em três categorias:

- Gerenciamento de identidade;
- Detecção e perícia;
- Criptografia de dados.

Implementando o Gerenciamento de Identidades

O gerenciamento de identidades é um tópico muito amplo que se aplica à maioria das áreas do *datacenter*. No entanto, é particularmente importante proteger o ambiente da nuvem.

Quando falamos de nuvem falamos sobre compartilhamento e virtualização física de recursos em que muitos usuários tem acesso a diversos serviços e recursos.

O principal objetivo da gestão de identidade é gerenciar informações de identidade pessoal para que o acesso a recursos, aplicativos, dados e serviços do computador seja controlado corretamente.

O gerenciamento de identidades é a única área de segurança de TI que oferece benefícios genuínos, além de reduzir o risco de violações de segurança.

Benefícios do gerenciamento de identidade

O gerenciamento de identidades ajuda a evitar violações de segurança e desempenha um papel importante na função de ajudar sua empresa a atender aos regulamentos de conformidade de segurança de TI. Os benefícios de manter seus dados financeiros de clientes ou empresas protegidos de acesso não autorizado pode ser enorme.

Além disso, você obtém muitos benefícios do gerenciamento de identidades que ocorre todos os dias e não apenas durante uma grande ameaça.

- **Melhoria da produtividade do usuário:** a melhoria da produtividade vem de simplificar a interface de logon e a capacidade de alterar rapidamente os direitos de acesso. A produtividade é provável que melhore ainda mais onde você fornece o autoatendimento do usuário.
- **Melhor serviço ao cliente e parceiro:** clientes e parceiros também se beneficiam de um processo seguro e simplificado ao acessar aplicações e dados.

- **Custos de *help desk* reduzidos:** os *help desks* geralmente recebem menos chamadas sobre senhas esquecidas quando um processo de gerenciamento de identidade é implementado.
- **Custos de TI reduzidos:** o gerenciamento de identidades permite o provisionamento automático - Fornecer ou revogar os direitos de acesso dos usuários a sistemas e aplicativos. Provisionamento acontece se você automatizar ou não. Quando o provisionamento é manual, normalmente é realizado por membros da equipe operacional de TI pessoal ou pessoal do departamento. Economias consideráveis de tempo e custo são possíveis ao automatizar o processo.

Depois de entender os fundamentos do gerenciamento de identidades, você precisa entender as condições especiais necessárias para a nuvem.

Porque a nuvem é altamente um ambiente importante, o gerenciamento de identidades precisa ser federado para se beneficiar do processo. O gerenciamento de identidade federada permite que as pessoas mantenham a mesma identificação em diferentes aplicativos, serviços e redes de diferentes empresas independentes.

Isso elimina alguns dos limites de acesso para seus funcionários, clientes e parceiros para que eles possam usar os aplicativos e as informações de vários ambientes (incluindo a nuvem).

Aspectos do gerenciamento de identidade

Neste ponto, vamos conhecer os aspectos de um programa de gerenciamento de identidade.

Corrigindo os dados

Os dados de identidade geralmente estão espalhados pelos sistemas. Estabelecer um banco de dados comum ou diretório como primeiro passo para obter o controle dessas informações. Esta etapa envolve a entrada de dados e a coleta de dados de vários usuários.

Integrando um sistema de gerenciamento de identidades, deve integrar-se efetivamente a outros aplicativos.

Em particular, o sistema deve ter uma interface direta com os seguintes pontos:

- Sistema de recursos humanos, em que os novos marcantes e os que saem são os primeiros gravados;
- Sistemas de cadeia de suprimentos, se parceiros e fornecedores usarem sistemas corporativos;
- Bancos de dados do cliente, embora o gerenciamento de identidade do cliente normalmente seja tratado por um componente separado de um sistema de gerenciamento de identidade.

Autenticação Forte

Quando você exige uma autenticação mais forte de senhas, o gerenciador de identidade e o sistema de gestão devem funcionar com produtos que fornecem essa autenticação, sistemas biométricos (como impressões digitais, verificação de íris, identificação fácil, etc.) e sistemas de *token* de identidade.

Provisionamento

Ao vincular todos os sistemas que usam informações de identidade, você pode automatizar provisionamento. Se este processo for automatizado, uma única mudança de *status* (de um funcionário ou qualquer outra pessoa com direitos de acesso) pode ser definida na identidade de sistema de gerenciamento e enviada a todos os sistemas afetados a partir daquele ponto.

Quando o provisionamento é automatizado, os usuários raramente (ou nunca) obtêm mais acesso do que necessário. Proporcionar amplos níveis de acesso acontece com frequência em aprovisionamento, porque é mais fácil especificar um acesso amplo. Além disso, um processo combinado nunca falha em revogar o acesso de ex-funcionários à rede.

Logon único

Logon único significa fornecer a todos os usuários uma interface que valide a identidade de um usuário, essa interface exige que o usuário insira uma senha única. Depois disso, todos os sistemas devem conhecer o usuário e suas permissões.

Alguns produtos do tipo *single sign-on* (acesso único) não fornecem toda a gama de recursos de gerenciamento de identidade, mas todos os produtos de gerenciamento de identidades fornecem a capacidade de uma única conexão à vários recursos.

Em vez das permissões serem atribuídas a indivíduos, elas são atribuídas a funções. Assim sendo o *single sign-on* permite capturar as informações sobre a hierarquia dos acessos administrados através de um *logon* único.

O *logon* único naturalmente acompanha a tecnologia de portal, com o usuário tendo uma interface inicial baseada na *Web* que fornece acesso a todos os aplicativos que ele tem direito de acessar. Assim, o *single sign-on* pode precisar interagir com um produto de portal.

Administração de segurança

O gerenciamento de identidades reduz os custos de administração de segurança porque a segurança dos administradores não precisa ser autorizada manualmente; o sistema de gerenciamento de identidade manipula esse fluxo de trabalho automaticamente.

O manuseio automático de gerenciamento de IDs é particularmente útil para organizações que distribuíram a administração de segurança em vários locais porque permite que a administração de segurança seja centralizada.

Analisando dados

Depois de centralizar todos os dados do usuário, você pode gerar relatórios úteis sobre uso de recursos e aplicativos ou realizar auditorias de segurança. Por exemplo:

- Se você está tendo problemas com o *hack* interno, você pode verificar um *log* que lista as atividades de todos os usuários.
- Se você possui *software* de registro para bancos de dados e arquivos, você pode monitorar o que fez um usuário a qualquer item de dados e quando, incluindo quem olhou itens de dados. Esta capacidade de auditoria é importante para a implementação de dados de privacidade e conformidade de proteção de dados.

Existem três grupos específicos de produtos de segurança de TI:

- *Logs* de atividade;
- Sistemas de proteção contra intrusão baseados em *host* e intrusão baseada em rede de sistemas de proteção;
- Auditoria de dados.

Ninguém - intruso ou usuário legítimo - deve ser capaz de usar os recursos sem deixar provas. Você quer detectar qualquer atividade ilegítima assim que acontece, mas em muitas situações, não pode separar o legítimo do ilegítimo. Se não detectar um ataque enquanto está acontecendo, pelo menos tem um registro do que aconteceu.

Logs de atividades

Muitos recursos de registro estão incluídos nos sistemas operacionais, aplicativos, bancos de dados e dispositivos, como *firewalls* de *hardware* e monitores de rede.

Esses custos para registrar as atividades em uma rede ou computador requer que o sistema grave os registros de *log* constantemente e também que envolva o gerenciamento e arquivamento desses dados até que eles não sejam mais necessários.

Os arquivos de registro geralmente fornecem algumas evidências de como uma fraude pode ter sido realizada. Os autores de fraudes digitais conseguem escapar da justiça simplesmente porque a vítima não tem provas suficientes para provar o que foi feito.

HIPS e NIPS

Empresas que gostariam de ver um provedor de serviços em nuvem assumir plataforma interna e serviços de infraestrutura precisam dar uma olhada cuidadosa em proteção de infraestrutura.

Sistemas de proteção contra invasão baseados em *host* (HIPS) e programas de intrusão baseados em rede sistemas de proteção (NIPS) são a mesma coisa: uma coleção de recursos que fazem a proteção e dificultam a intrusão em uma rede.

O HIPS e o NIPS podem incluir os seguintes elementos:

- **Monitores de sistema e de arquivo de *log*:** este *software* procura vestígios de *hackers* em arquivos de *log*. Os monitores podem assistir a contas de *login*, por exemplo, e emitir alertas quando as permissões da conta forem alteradas - geralmente uma indicação que algo desagradável está acontecendo.
- **Sistemas de detecção de invasão de rede (NIDS):** esses programas de segurança monitoram pacotes de dados que viajam através de uma rede, procurando sinais reveladores de atividade de *hackers*. A eficácia de um NIDS depende do poder de classificar os perigos reais de ameaças inofensivas e de legitimar atividade de mate. Um NIDS ineficaz gera muitos alarmes falsos e, assim, perda de tempo.
- ***Software* de decepção digital:** este *software* engana deliberadamente qualquer um que esteja tentando atacar a rede de TI.

Pode variar da simples falsificação de vários nomes de serviço para configurar armadilhas conhecidas como *honeypots* ou *honeynets*.

Definir armadilhas de segurança é incomum e pode ser caro. Normalmente é feito por *sites* do governo ou por empresas que suspeitam de espionagem.

- **Lista de acessos:** este recurso habilita o uso de recursos válidos. Esta lista dificulta severamente *hackers*, porque mesmo se acessarem um computador, não podem fazer o *upload* de seu próprio *software* para executá-lo.

  O *software* informa sobre qualquer tentativa de execução não autenticada. Também impede que o *software* de vírus seja morto.
- **Gerenciamento unificado de ameaças:** essa função central coleta informações de todos os componentes anteriores e identifica as ameaças por meio da análise da informação combinada.

Enganando invasores

Como termo técnico de TI, *spoofing* significa tendendo a ser outra coisa. Em um chamado ataque de *phishing*, um *site* falso finge ser genuíno. Um *site* de *phishing* pode fingir ser o *site* de um banco, por exemplo, e tentar convencer os usuários a revelar seus detalhes. É possível falsificar endereços de *e-mail* e, em algumas circunstâncias, os protocolos da *Internet*, endereços. Mas montando um ataque dessa maneira é difícil, porque um computador responde diretamente ao endereço real, em vez do endereço falso.

Quando você usa *spoofing* como defesa, seu objetivo é confundir um *software* de ataque. Uso de *hackers* de *sniffing software* para procurar servidores em execução, versões específicas do *Microsoft Windows*, por exemplo.

Auditoria de dados

Embora os bancos de dados registrem o nome do indivíduo que alterou os dados, eles normalmente não registram quem leu qualquer dado. Mas ler dados é facilmente roubável. Se você planeja armazenar dados em um ambiente de nuvem, essas questões sobre como os dados e as informações serão protegidas devem ser considerados.

O entusiasmo por preencher esta lacuna aumentou consideravelmente após o *Sarbanes-Oxley*. Legislação foi promulgada em 2002, exigindo especificamente que os dados financeiros fossem protegidos de olhos não autorizados.

Consequentemente, uma série de produtos de *software* possui aquele *log* que olha para o que rapidamente passou a existir.

Esses produtos referidos servem como produtos de auditoria de dados.

Criptografando Dados

O mundo da TI tem todo um conjunto de técnicas de criptografia que podem ser consideradas como completamente seguro. Assim, você pode facilmente criptografar dados e garantir que apenas o destinatário pretendido possa descriptografá-lo.

Figura 3
Fonte: iStock/GettyImages

Você poderia criptografar tudo. Dados quando os escreve para o disco, quando envia um dado, quando envia através do rádio, e assim por diante.

Criptografando tudo de maneira abrangente, considere que habilmente se reduz a sua exposição ao roubo de dados. Os *hackers* não podem cobrir seus rastros porque não são capazes de descriptografar os arquivos de *log*.

A criptografia representa uma penalidade de desempenho, portanto, concentre-se na criptografia de dados específicos que precisam de proteção.

Pense em como você usa a criptografia. Um caso recente de roubo incluiu dados que foram criptografados até serem entregues ao aplicativo que precisava para usá-lo.

Nesse momento, os dados foram descriptografados para uso e é exatamente onde o *hacker* atacou. A perda poderia ter sido evitada se o próprio aplicativo que controla a descriptografia fizesse isso em uma base de dados com cada registro.

Devido às complexidades que ele adiciona, a criptografia é usada com menos frequência do que talvez devesse ser. A mídia cobriu muitos casos de laptops roubados contendo dados valiosos - incluindo segredos militares. Esses roubos não ocorreriam se todos os dados desses *laptops* tivessem sido criptografados devidamente.

A criptografia de dados se torna ainda mais importante ao usar serviços em nuvem.

Mas tenha em mente que sua empresa ainda é responsável pela qualidade e integridade de suas informações.

Criando uma estratégia de segurança na nuvem

Vamos conhecer alguns indicadores importantes:

- Na maioria das circunstâncias, aborde a segurança na nuvem a partir de uma perspectiva de desenvolvimento. Se sua organização tiver especialistas em gerenciamento de riscos, envolvê-los no planejamento de segurança na nuvem.
- O monitoramento de segurança de TI não possui indicadores-chave simples de desempenho, mas é ciente do que organizações similares gastam em segurança de TI. Também faz sentido manter o controle do tempo perdido devido a qualquer tipo de ataque - uma medida útil de custo que você pode reduzir com o tempo.
- Você precisa de gerenciamento de identidade por vários motivos, o que oferece muitos benefícios. Dar prioridade ao aprimoramento do gerenciamento de identidade.
- Tente criar uma consciência geral dos riscos de segurança educando e avisando os membros da equipe sobre perigos específicos. É fácil tornar-se complacente, especialmente se você estiver usando um provedor de serviços de nuvem. Contudo, ameaças vêm de dentro e de fora da organização.
- Regularmente, consultores externos de segurança de TI verificam a TI da sua empresa, política de segurança e rede de TI e as políticas e práticas de todos os seus prestadores de serviços em nuvem.
- Determinar políticas específicas de segurança de TI para gerenciamento de mudanças e gerenciamento de patches, e certificar-se de que as políticas sejam bem compreendidas por sua equipe de gerenciamento de serviços e por seu provedor de serviços de nuvem.
- Fique por dentro das novidades sobre violações de segurança de TI em outras empresas e as causas dessas violações.
- Revise os sistemas de *backup* e recuperação de desastres à luz da segurança de TI.

Além de qualquer outra coisa, as violações de segurança de TI podem exigir recuperação de aplicativos.

Quando uma violação de segurança ocorre em um computador específico, os aplicativos nesse computador provavelmente terão que ser interrompidos. Consequentemente, a violação de segurança pode ser ocasionada de forma direta através de interrupções nos serviços e pode contribuir para diminuir os níveis de serviço. Além disso, o roubo de dados resultante de uma violação de segurança resulta em uma violação real ou percebida da confiança dos clientes em sua organização.

A segurança é uma área muito complexa para organizações internas de TI, bem como os provedores de serviços em nuvem. Muitas organizações terão ambiente híbrido que incluem nuvens públicas e privadas. Sistemas internos serão conectados a ambientes de nuvem. Novas fronteiras acrescentam complexidade e risco.

Áreas críticas em uma estratégia de segurança para a nuvem

A preocupação com algumas áreas da computação em nuvem devem fazer parte da estratégia das organizações quando as mesmas começam a fazer seus projetos de computação em nuvem.

Esses pontos críticos devem compor as estratégias e também as questões táticas de segurança dentro de um ambiente em nuvem e podem ser aplicados a qualquer combinação de modelo de serviço em nuvem e de implantação.

Podemos dividir essas questões em duas categorias: Governança da Nuvem e Operação da Nuvem.

A questão da governança é ampla e trata de questões estratégicas e políticas dentro de um ambiente de computação em nuvem, enquanto as questões operacionais concentram-se em questões de segurança mais táticas e de implantação dentro da arquitetura de nuvem.

As áreas em que devemos considerar em um projeto de computação em nuvem são as seguintes:

Gerenciamento de Governança e Risco

A organização deve ter capacidade de governar e medir os seus riscos e os riscos que a computação em nuvem pode trazer para dentro das empresas.

Questões legais e a capacidade de avaliar adequadamente os riscos de um fornecedor de nuvem, ou seja, a responsabilidade de proteger dados importantes pode afetar os projetos de computação em nuvem.

Questões legais

Neste item estão inclusos os requisitos de proteção para os sistemas de informação e computação, as regras e condições sobre as descobertas de brechas de segurança, questões regulatórias e de privacidade, entre outras, incluindo leis internacionais que devem ser avaliadas sob a ótica do negócio.

Compliance e Auditoria

A avaliação de como a computação em nuvem pode afetar o cumprimento das políticas de segurança interna, normativos e acordos de confidencialidade, como também requisitos de conformidade (regulatórios, legislativos, etc.). Como garantir o *compliance* se houver a necessidade de uma auditoria.

Segurança de Dados e Gestão da Informação

Uma vez que os dados estejam na nuvem, aspectos que envolvem a identificação e o controle dos mesmos devem ser pensados, os controles que podem ser utilizados para tratar a perda do controle físico ao mover dados para a nuvem devem ser considerados.

Outro ponto importante diz respeito às questões sobre quem é responsável pela confidencialidade, integridade e disponibilidade dos dados.

Portabilidade

Nada é eterno, ou seja, pode existir a necessidade da organização mover seus dados para outro provedor de nuvem ou simplesmente voltar à situação dos dados serem hospedados em um *datacenter* local dentro da organização.

Então em um projeto de computação em nuvem, a avaliação da capacidade de mover dados ou serviços para outro provedor ou localidade deve ser considerada.

Continuidade de Negócios e Recuperação de Desastres

A computação em nuvem pode afetar a forma como os processos de negócios funcionam bem como os processos e os procedimentos operacionais utilizados para a segurança da informação, continuidade de negócios e a recuperação de desastres. O ponto é que se deve analisar os riscos da computação e melhorar os modelos de gestão e governança. Esta questão pode proporcionar à organização alguns benefícios como, por exemplo, diminuir riscos de segurança ou trazer vantagens em outras áreas da mesma.

Operação no *Datacenter* em Nuvem

Compreender e conhecer as características e os serviços disponíveis pelos provedores que podem ser prejudiciais àqueles em curso, bem como as características que são fundamentais para a estabilidade em longo prazo.

Respostas a Incidentes

O correto tratamento à detecção de incidentes, o tempo de resposta, a notificação e a correção do problema devem estar presentes em qualquer projeto de migração para a nuvem, isto também compreende a complexidade que esta traz para o seu programa de gerenciamento e tratamento de incidentes.

Segurança de Aplicações

Proteger o *software* de aplicação que está em execução ou em desenvolvimento na nuvem inclui questões como se é apropriado migrar ou criar uma aplicação para ser executado na nuvem e, em caso afirmativo, qual o tipo de plataforma em nuvem mais adequado (SaaS, PaaS, ou IaaS).

Criptografia

A criptografia é uma técnica que pode ser implementada como uma camada adicional de segurança ao ambiente em nuvem, isso se aplica aos dados e também aos recursos computacionais utilizados na nuvem.

Gerenciamento de Identidade e Acesso

O gerenciamento de identidade e acesso se faz necessário para garantir as permissões corretas para as operações e utilização dos recursos dentro da nuvem.

Gerenciamento de Risco Empresarial

O Gerenciamento de Risco permite às organizações o fornecimento de valor para as partes envolvidas, visto que os negócios podem enfrentar incertezas e um dos desafios é determinar como a empresa pode medir, gerenciar e mitigar.

Incertezas apresentam oportunidades e riscos que podem aumentar ou diminuir o valor da empresa. O gerenciamento de risco da informação é o processo de identificar e compreender a exposição ao risco e a capacidade de gerenciá-lo, de forma alinhada com o apetite ao risco e com a tolerância da organização.

O Gerenciamento de Risco inclui os métodos e processos usados pelas organizações para gerenciar riscos e para capturar oportunidades relacionadas aos objetivos do negócio.

Em um ambiente de computação em nuvem, a gerência seleciona uma estratégia de resposta para riscos específicos identificados e analisados que podem incluir:

- **Anular** – deixar de fazer as atividades que dão origem ao risco.
- **Reduzir** – agir para reduzir a probabilidade ou o impacto relacionado ao risco.
- **Compartilhar ou segurar** – transferir ou compartilhar uma parte do risco financiando-o.
- **Aceitar** – nenhuma ação é tomada em função de uma decisão relacionada ao custo-benefício.

O gerenciamento de risco é um processo com o objetivo de minimizar a incerteza e de maximizar o valor de forma alinhada com o apetite ao risco e com a estratégia.

Existem muitas variáveis, valores e riscos em qualquer oportunidade ou planejamento da computação em nuvem que afetam a decisão sobre se um serviço deve ser adotado a partir do ponto de vista do risco ou do negócio.

Cada empresa tem que ponderar tais variáveis para decidir se a computação em nuvem é uma solução apropriada.

A computação em nuvem oferece muitos benefícios para as empresas e alguns deles são:

- Uso otimizado de recursos;
- Redução de custos para os clientes de computação em nuvem;
- Transição de despesas de capital (CAPEX) para despesas operacionais (OPEX);
- Escalabilidade dinâmica de capacidade de TI para os clientes;
- Encurtamento do ciclo de vida de desenvolvimento ou de implantação de novas aplicações;
- Encurtamento do tempo necessário para a implementação de novos negócios.

Os clientes devem ver os serviços de computação em nuvem e de segurança como questões de segurança da cadeia de fornecimento. Isso significa analisar e avaliar a cadeia do fornecedor na medida do possível.

Isso também significa examinar a própria gestão de terceiros que é feita pelo provedor. A avaliação dos prestadores de serviços deve visar, especificamente, a gestão de incidentes feita pelos provedores, as políticas de continuidade de negócios e de recuperação de desastres, bem como processos e procedimentos, e deve incluir a revisão de instalações de locação compartilhadas e de *backup*.

Isso deve incluir a revisão das avaliações internas de conformidade dos provedores com as próprias políticas e procedimentos de avaliação de métricas usadas pelos mesmos para que se obtenham informações razoáveis em relação ao desempenho e eficácia dos controles nessas áreas. Informações sobre incidentes podem ser especificadas em contratos, SLAs, ou outros acordos e podem ser comunicadas automaticamente ou periodicamente, diretamente em sistemas de notificação ou entregues ao pessoal-chave da empresa.

O nível de atenção e de segurança deve estar conectado ao valor em risco – se o terceiro não acessar diretamente os dados da empresa, então o nível de risco cai significativamente e vice-versa.

Os clientes devem rever os processos de gestão de risco e de governança de seus fornecedores para garantir que as práticas sejam consistentes e alinhadas.

Conclusão

Computação em nuvem oferece inúmeras oportunidades e benefícios de negócios, os riscos, em certo ponto, são oportunidades dentro de um novo ambiente.

A segurança da informação deve ser um componente importante em qualquer projeto de computação em nuvem.

Material Complementar

Indicações para saber mais sobre os assuntos abordados nesta Unidade:

Leitura

Aprendizado sobre Segurança

https://goo.gl/4UvGGJ

7 Pecados Mortais de Segurança em Computação na Nuvem

Clique aqui para acessar.

Segurança das Nuvens Computacionais: uma Visão dos Principais Problemas e Soluções

Clique aqui para acessar.

O que é Segurança da Nuvem?

Clique aqui para acessar.

Referências

COULOURIS, George F.; DOLLIMORE, Jean; KINDBERG, Tim. **Sistemas distribuídos:** conceitos e projeto. 4. ed. Porto Alegre: Bookman, 2007.

OZSU, M.Tamer. ***Principles of distributed database systems.*** 3nd. ed. New York: Springer, 2011.

TAURION, Cezar. ***Cloud Computing:*** computação em nuvem, transformando o mundo da Tecnologia da Informação. Rio de Janeiro, RJ: Brasport, 2009.


Cruzeiro do Sul
Educacional