Segurança na nuvem e a sua empresa

A segurança da informação não é algo que se tem, é algo que se faz. A segurança também não é garantida por uma ou duas coisas que você fez no passado e depois se esqueceu. Como o seu superintendente da segurança da informação lhe dirá, a segurança é um processo permanente e contínuo, que requer vigilância constante. Uma segurança bem-sucedida depende de haver pessoas comprometidas em aplicar constantemente as ferramentas, tecnologias e processos mais confiáveis, a fim de reduzir os riscos a um nível razoável. Nunca é possível reduzir os riscos a zero, mas é possível diminuir seus riscos a um n que corresponda à probabilidade e ao impacto de uma violação de segurança, a custos cabíveis.

Nesse contexto, o debate sobre a computação em nuvem ser mais ou menos segura do que manter dados em dispositivos físicos é algo que foge ao objetivo primário. Contanto que o seu sistema esteja conectado à Internet pública, quer seja uma solução em nuvem ou um software fisicamente instalado, você corre o risco de uma violação de segurança dos dados. A questão essencial é se você adotou os controles apropriados para minimizar o risco à confidencialidade, integridade e disponibilidade de seus dados.

Não é exagero destacar a importância e a urgência da segurança e da privacidade dos dados. Em 2017, aconteceram algumas das maiores violações de dados da história, enquanto o custo direto da resolução de uma violação de dados foi, em média, de **3,62 milhões de dólares**. Porém, os custos diretos não são nada comparados aos incalculáveis e permanentes danos à marca, reputação e aos negócios que um incidente de segurança de dados pode causar.

Índice

Entendendo a ameaça

Os riscos associados às ameaças à segurança da informação aumentam diariamente. O número de possíveis invasores também está se expandindo para incluir não apenas invasores independentes e pequenos grupos, como também organizações de hackers patrocinadas por governos, que são muito mais bem organizadas e financiadas. Esses grupos maiores podem dedicar vários recursos para violar as defesas de pequenas e grandes organizações durante um longo período, que é um nível de comprometimento de comprometimento antes reservado apenas para os alvos mais estratégicos.

A menos que a sua organização mantenha um ambiente que proíba qualquer acesso externo à Internet, é provável que o seu ambiente corporativo já sofreu algum tipo de ataque bem-sucedido, mesmo que seja algo tão simples quanto a liberação não autorizada de alguns dados pessoais. Como diz **John Chambers, CEO da Cisco**, "existem apenas dois tipos de empresas: as que foram hackeadas e as que ainda não sabem que foram hackeadas".

Isso não é culpa de sua organização interna de TI. O ambiente corporativo da atualidade exige um nível de agilidade e eficiência que requer que as organizações abram suas redes de maneiras até recentemente consideradas inimagináveis. Essa abertura, embora essencial para manter a competitividade de uma empresa, tornou ainda mais difícil a tarefa de manter a segurança de uma rede.

Organizações como a Cloud Security Alliance e outros grupos de pesquisa frequentemente citam motivos convincentes para buscar a melhor segurança possível, seja através da utilização de software em nuvem ou de soluções instaladas fisicamente.

5 principais motivos para atualizar sua segurança:

1. **Há uma grande probabilidade de sua organização sofrer interrupções**—**Especialistas concordam** que uma variedade crescente de ameaças de segurança aumenta os riscos de interrupção de quase todas as empresas. As interrupções mais caras são o resultado de negações de serviço, pessoas mal-intencionadas dentro de uma organização e ataques através da internet. No entanto, inúmeras causas podem causar interrupções dispendiosas na confidencialidade, integridade e disponibilidade de seus dados.
2. **Pessoas mal-intencionadas dentro de uma organização causam uma proporção surpreendente de ataques**—Os funcionários são os culpados mais frequentemente citados no caso de ataques à segurança de dados, de acordo com uma **pesquisa feita pela PWC**. Nesse ponto, os dados mantidos em dispositivos físicos e os dados em nuvem são igualmente vulneráveis. Isso torna essencial que a infraestrutura de segurança de uma organização abranja tanto os dados em nuvem quanto os dados mantidos em dispositivos físicos com vigilância idêntica.
3. **Os ataques cibernéticos continuam custando muito dinheiro**—Um estudo realizado pelo **Ponemon Institute** mostrou que o custo médio de um ataque cibernético foi de US$ 3,62 milhões em 2016.
4. **As TIs clandestinas estão em alta**—– Mais de 80% dos funcionários usam aplicativos em nuvem ou SaaS que não foram aprovados pela TI, de acordo com um estudo realizado pela **Frost & Sullivan**. Esse hábito persiste, apesar de 15% dos funcionários afirmar já ter passado pessoalmente por incidentes de segurança (incluindo infecções por malware e perda de dados) resultantes do uso desses aplicativos.

5. **As práticas de BYOD trazem novos riscos** —— Hoje em dia, quase todos os funcionários chegam ao trabalho com um ou mais dispositivos conectados à internet, principalmente smartphones e tablets, que podem criar riscos de segurança que fogem do controle do departamento de TI. Independentemente de haver ou não uma política oficial de "traga o seu próprio dispositivo (BYOD, bring your own device)", os riscos criados pelo grande número de dispositivos de funcionários no local de trabalho representam um desafio contínuo para o processo de segurança da informação.

A importância das normas e da conformidade

As normas desempenham um papel vital na segurança da informação, ao garantir que as práticas sejam minuciosas, consistentes e eficazes. As normas mais conhecidas mundialmente, que prescrevem um sistema de gerenciamento da segurança da informação eficaz bem como os controles detalhados são, indiscutivelmente, a ISO/IEC 27001:2013 e a ISO/IEC 27002:2013, apesar de muitas organizações optarem por adotar a NIST 800-53, a Cloud Security Alliance, SSAE 18, SOC 1, SOC 2 ou outras normas que normalmente prescrevem controles parecidos. Essas normas descrevem detalhadamente os controles, procedimentos e processos de segurança que uma organização deve adotar para se considerar em conformidade com as melhores práticas vigentes na atualidade. Um host em nuvem em conformidade com a ISO 27001 também deve atender à norma em vários domínios importantes, incluindo:

- **Políticas de segurança** —— Todos os funcionários devem ser responsáveis pela segurança de informações não públicas e adotar as práticas definidas no sistema de gerenciamento da segurança da informação.
- **Organização da segurança da informação** —— O gerenciamento deve estar comprometido com a segurança e estabelecer uma organização responsável pela segurança das informações não públicas.
- **Gerenciamento de ativos** — Os ativos devem ser estritamente controlados e todos os dados classificados, a fim de determinar os requisitos apropriados para acesso e processamento.
- **Práticas de segurança de recursos humanos** —— A organização deve realizar uma verificação de antecedentes abrangente no momento em que cada funcionário é contratado, bem como exigir que os funcionários mantenham-se familiarizados e em conformidade com as responsabilidades de segurança. Quando os funcionários saem da empresa ou são transferidos, um processo formal deve ser implementado para remover ou atualizar seu acesso físico e virtual à infraestrutura da empresa.
- **Segurança física e do ambiente** —— Os componentes críticos devem ser colocados em espaços fisicamente controlados, com controles suficientes do acesso para proteger a infraestrutura. As organizações também devem implementar políticas sobre quem tem acesso a espaços controlados e sob quais circunstâncias, bem como monitorar consistentemente a conformidade com essas políticas. As medidas de segurança física e do ambiente podem incluir cartões de identificação, crachás ou controles biométricos de acesso, bem como devem limitar o acesso a locais seguros de acordo com a função de trabalho.

- **Gerenciamento de operações** — A organização deve estabelecer controles relacionados ao planejamento de sistemas, proteção contra códigos mal-intencionados, processos de backup, segurança de redes, utilização de mídias e troca de informações. Esses controles devem ser constantemente analisados e monitorados para assegurar o fornecimento de uma proteção razoável aos dados que eles protegem. Os prestadores de serviços terceirizados com acesso a informações confidenciais devem aderir a requisitos de segurança e privacidade que sejam consistentes com e, no mínimo, tão restritivos quanto as próprias políticas e procedimentos da organização em relação à proteção de informações confidenciais.
- **Controle de acesso** –– Todo o acesso a sistemas, redes e aplicativos deve ser controlado até o nível de usuário e de recursos, através de técnicas de privilégio de acordo com a função. Esse acesso deve ser revisado periodicamente para garantir que uma mudança de pessoal ou uma mudança de cargo não tenha modificado as necessidades de acesso do indivíduo.
- **Desenvolvimento do sistema** –– Os requisitos de segurança de todos os aplicativos que lidam com informações confidenciais devem ser definidos no início do estágio de desenvolvimento. Técnicas apropriadas de proteção de dados devem ser concebidas para o aplicativo e as alterações ao software desenvolvido devem passar por um processo maduro de gerenciamento de mudanças.
- **Gerenciamento de incidentes** –– No caso de um incidente de segurança real ou do qual haja suspeitas razoáveis, as equipes devem começar a trabalhar imediatamente para identificar o alcance do impacto, mitigar qualquer exposição, determinar a causa primária do incidente e tomar as ações corretivas apropriadas, incluindo o encaminhamento do caso à esfera competente e a notificação das partes afetadas, conforme a necessidade.

Manter a vigilância

Se a segurança da informação fosse pontuada com base no risco, a pontuação perfeita seria zero e, portanto, inalcançável. São muitas as ameaças que surgem todos os dias para esperar que haja um ano sem nenhuma exposição a riscos. Mas você pode desejar alcançar um ideal semelhante tomando algumas precauções essenciais:

- **Adote uma estrutura em nuvem segura**. Coloque o máximo possível de sua capacidade de computação em uma estrutura que foi certificada por estar em conformidade com normas reconhecidas, tais como a ISO 27001, ITAR e a FedRAMP. Os principais provedores de infraestrutura em nuvem geralmente atendem a essas normas e mantêm um processo contínuo para manter a conformidade com as normas de segurança apropriadas.

- **Certifique-se de que sua organização adota as normas de segurança atuais de seu setor**. Certas normas, tais como a HIPAA e ITAR, bem como as regulamentações da FDA foram concebidas para otimizar a segurança dos tipos das informações mais críticas em setores específicos. Para obter uma segurança eficaz, você e seu provedor de infraestrutura em nuvem precisam atender aos padrões de segurança mais relevantes para o seu setor. A robustez da cadeia de segurança só dura até chegar ao seu elo mais fraco. Os padrões de segurança também evoluem ao longo do tempo e fornecem uma referência que ajuda a avaliar se as práticas e os procedimentos de segurança de sua organização são suficientes para manter os riscos ao mínimo em um determinado momento.
- **Considere um serviço de validação da conformidade**. Consultores terceirizados que se especializam em avaliar a conformidade regulamentar e de segurança podem fornecer um parâmetro útil e imparcial para garantir que seus esforços de segurança estejam colocando sua organização na direção certa.
- **Certifique-se de que todos os seus fornecedores de nuvem adotem os padrões de segurança mais recentes**. A tecnologia em nuvem está facilitando às empresas a adoção de diversos serviços baseados em nuvem para diferentes funções –– automação de vendas, ERP, gerenciamento de ativos, folhas de pagamento e muito mais. É essencial que todos os fornecedores de serviços em nuvem adotem as normas de segurança pertinentes ao seu setor e entendam os requisitos de segurança específicos de sua empresa.

Ao buscar, sempre que possível, conformidade com as normas aceitas, você pode reduzir a exposição de sua organização aos riscos e estar preparado para resolver problemas rapidamente e a um custo mínimo.

Resumo

Revise as normas

Ao manter-se em conformidade com as normas de segurança, tais como a ISO/IEC 27001: 2013 e NIST 800-53, e manter-se atualizado com as recomendações mais recentes dessas normas, você reduz o risco de um ataque cibernético problemático.

Saiba mais sobre a Infor Cloud em infor.com/cloud

Compartilhar:

Infor América Latina, www.infor.com

INF-1475040-pt-BR-0219-1