DOCUMENTO SORE SEGURANÇA

Serviços em Cloud
Segurança para PaperCut MF

Segurança de dados na nuvem desde o início

Proteger dados importantes é uma busca secular.

Em 1586, um nobre inglês chamado Anthony Babington começou a enviar mensagens à presa Maria, Rainha da Escócia. O conteúdo da correspondência girava em torno de uma conspiração para assassinar a Rainha Elizabeth e instalar Maria no trono da Inglaterra. Babington usou uma série de técnicas para manter suas mensagens o mais secretas possível, já que a traição era bastante desaprovada.

No mundo cibernético de hoje, nos referiríamos à sua abordagem como segurança em camadas. Primeiro, ele criptografou as mensagens, depois as escondeu nas rolhas dos barris de cerveja e depois as transportou através de uma rede de cúmplices de confiança. Infelizmente para Babington, ele usou uma cifra fraca e sua rede também foi comprometida. Em poucos meses, ele pagou o preço mais alto pela falta de segurança dos dados.

Na PaperCut prestamos atenção especial a vários aspectos da segurança de dados, e isso está presente em tudo o que construímos. Você também pode querer ler o whitepaper Protegendo seu sistema de impressão.

Negócio arriscado

Proteger um ativo valioso sempre apresenta algum risco inerente. Normalmente, o objetivo da segurança de dados é reduzir o risco ao nível mais baixo aceitável e, ao mesmo tempo, manter os objetivos de negócios e conter os custos. Portanto, devemos sempre ter em mente estes três itens: risco, objetivos e custo.

Poderíamos criar um plano de segurança de dados com risco absolutamente zero, tornando os dados inacessíveis a qualquer pessoa, mas isso provavelmente não atenderia aos objetivos de negócios ou teria um custo exorbitante.

Os dados eletrónicos introduzem alguns riscos adicionais a considerar. Antigamente, para roubar um ativo, os ladrões tinham que roubá-lo fisicamente. Agora, com os dados eletrônicos, eles podem simplesmente fazer uma cópia e, na maioria dos casos, a cópia é tão valiosa quanto o original. E pior ainda, muitas vezes há poucas evidências de que a cópia foi tirada, então você nem sabe que foi roubado.

IEm 1980, houve uma série de roubos de aeronaves comerciais nos EUA. Por acaso, o caso foi resolvido no dia 14 de maio em Atlanta, na Geórgia, quando um porta-malas de carga se abriu durante o carregamento. A tripulação descobriu um clandestino escondido dentro do porta-malas com um pouco de comida e um tanque de oxigênio. Acontece que ele rastejava para fora do porta-malas no meio do vôo, pegava todos os objetos de valor que pudesse e depois os levava de volta para o porta-malas com ele. Compare esse roubo físico de objetos de valor com o roubo de dados eletrônicos - chamaríamos suas ações de ataque clássico do tipo Man in the Middle e roubo de dados em trânsito.

Felizmente, o roubo de itens físicos tornou o roubo aéreo rapidamente evidente, mas com ativos digitais, o roubo geralmente passa despercebido por um período de tempo.

Identificar adequadamente seus objetivos de negócios para segurança de dados pode levar algum tempo. Os objetivos precisam incluir requisitos legais (por exemplo, GDPR, HIPAA), eficiência operacional para coisas como planejamento de continuidade de negócios e cadeia de suprimentos, e itens básicos como quem requer acesso aos dados e com que rapidez. Poderíamos cobrir alguns desses objetivos colocando todos os dados da empresa em um servidor web público, sem criptografia. Pode ser altamente eficiente para os negócios, mas pode ser desastroso para a reputação, confidencialidade e integridade. Portanto, seus objetivos de negócios também precisam abranger esses aspectos.

Ativos eletrônicos como informações de saúde protegidas (PHI), informações de identificação pessoal (PII), dados de cartão de crédito, propriedade intelectual e outros devem ser protegidos de forma a minimizar o risco de perda, exposição ou cópia.

Localização

Um fator chave na sua decisão de proteger os dados eletrônicos é onde localizar os dados armazenados. Normalmente, isso significa escolher hospedado localmente (ou seja, no local) ou na nuvem. No entanto, a decisão não é tão clara como costumava ser, principalmente devido aos avanços significativos na segurança da nuvem. Vamos dividir a decisão de localização dos dados em cinco objetivos.

Custo

Os data centers hospedados localmente têm custos iniciais e operacionais significativamente mais altos do que os data centers em nuvem privada (ou seja, infraestrutura como serviço*). Você precisará de servidores, discos, licenças, equipamentos de rede, energia elétrica, sistemas de refrigeração e uma equipe de TI incrível para gerenciar, manter e atualizar tudo isso. Um data center em nuvem privada, por outro lado, tem um custo de entrada muito baixo, mas você pagará por praticamente cada quilobyte de disco e ciclo de processador que usar. Você também arcará com a maior parte dos custos de licença, gerenciamento e atualização de software. Sim, isso também pode aumentar com o tempo, mas chega um ponto de equilíbrio (geralmente medido em anos) em que a nuvem privada tem um custo total de propriedade mais alto. Outros custos a serem considerados e equilibrados em relação aos objetivos de negócios incluem escalabilidade, conformidade legal e fluxo de caixa.

Nota: Os serviços PaperCut MF Cloud estão incluídos como parte de sua licença quando você tem manutenção e suporte ativos.

Segurança

Este costumava ser um golpe certeiro para data centers hospedados localmente, mas isso foi "há muito tempo" (australiano por "alguns anos"). Um data center hospedado localmente oferece controle total sobre onde e como proteger os dados. Para algumas organizações, esse controle não é negociável para determinados dados que manipulam. Um dos motivos é cumprir os regulamentos de proteção de dados (por exemplo, GDPR, HIPAA, FERPA). A conformidade com os regulamentos nem sempre pode ser verificada por terceiros que têm acesso aos dados na nuvem pública.

Os dados hospedados localmente só vão para onde você manda e só são acessíveis a pessoas e sistemas que você autoriza, a menos que você os armazene em um disco ou os coloque em uma rede. Porque se alguém puder acessar os dados, poderá roubá-los. Considere algumas estatísticas sobre violações de dados:

- Mais de 20% das violações em 2021 usam credenciais roubadas (Verizon, 2022 Data Breach
- Relatório de Investigações)
- 93% dos malwares inseridos por e-mail'
- Os ataques à cadeia de abastecimento aumentaram mais de 600% em 20213
- 27% das violações são resultado de erro humano, 25% de falhas no sistema e 48% são ataques maliciosos (muitos dos quais eram "insiders")

A maioria das organizações que hospedam seus próprios dados não consegue mais acompanhar o aumento da quantidade e da sofisticação das ameaças. Muito poucos estão preparados para se defender contra vulnerabilidades de chips de hardware, explorações de dia zero, ataques multivetoriais ou malware polimórfico. Estamos no ponto em que a maioria dos provedores de nuvem dedicados oferecem maior segurança do que os auto-hospedados. No entanto, ainda existem preocupações significativas com a segurança dos dados na nuvem, sendo que a maioria delas se enquadra na categoria de como a nuvem é usada. Por exemplo, milhões de registros de dados foram expostos nos últimos anos devido a buckets do Amazon S3 mal configurados. Alerta de spoiler: se você não configurar a autenticação e a criptografia, outras pessoas poderão ver seus dados.
Mais uma área onde as violações são relatadas como “acesso online” acontece na cadeia de abastecimento. Essas violações podem acontecer a terceiros que desempenham um papel nas suas operações comerciais e que têm acesso aos seus dados. A maioria das organizações não possui procedimentos adequados de verificação de terceiros. A sua responsabilidade pela proteção de dados inclui aqueles com quem você compartilha esses dados.

Uma escola que fornece informações aos alunos a terceiros que preparam as suas refeições é tão vulnerável como o elo mais fraco da cadeia de abastecimento. Um hospital que compartilha dados de pacientes com um cobrador de contas médicas terceirizado é vulnerável e responsável por violações de PHI. Antes de confiar suas responsabilidades de proteção de dados a um provedor de nuvem, certifique-se de que ele garanta a segurança de todos os terceiros.