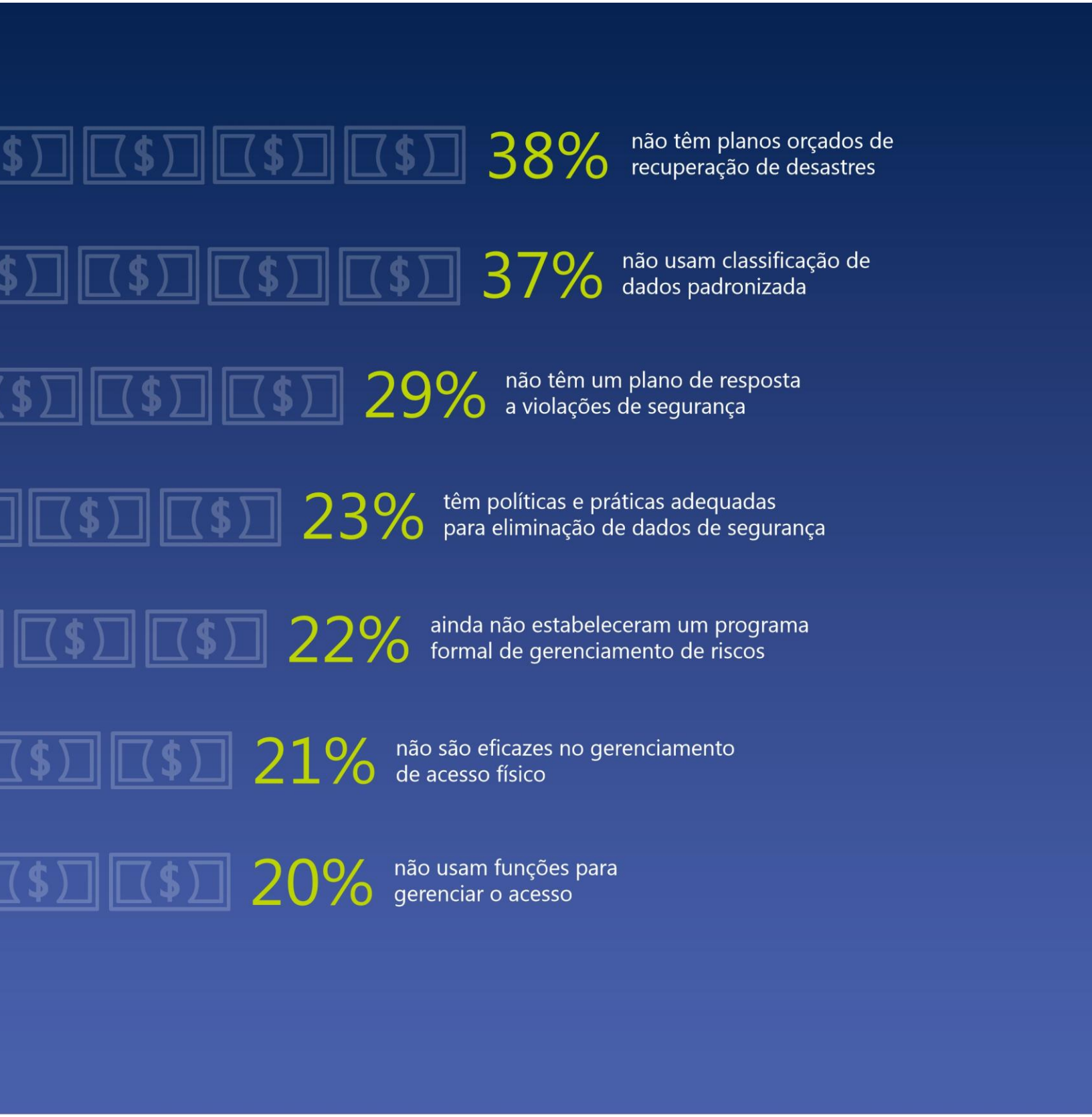

Tendências de Segurança em Serviços Financeiros

Principais conclusões e recomendações

Microsoft

Tendências de segurança no setor financeiro

Cenários de tecnologia da informação (TI) em organizações financeiras e no setor bancário corporativo no mundo estão mudando rapidamente, em parte por causa da constatação de que mais de 75% dos clientes estão dispostos a mudar para outra instituição financeira se ela oferecer melhor tecnologia.[1] Como resultado, organizações financeiras e bancárias estão trabalhando para oferecer aos usuários com visão tecnológica soluções que utilizem tecnologias mais recentes. Além disso, organizações bancárias e financeiras estão usando recursos avançados de mídia social para ajudar a aumentar sua participação no mercado. Esses fatores exigem muita atenção ao desenvolver recursos de TI e boa compreensão das principais regras financeiras, tais como a lei Sarbanes-Oxley (SOX); um estudo sugere que 30% a 50% das organizações financeiras estão gastando seus orçamentos de TI excedentes em conformidade regulatória.[2]

A computação em nuvem pode ajudar a melhorar os perfis de segurança das organizações financeiras, invertendo o ônus de garantir conformidade regulatória e minimizando riscos aos provedores de serviços de nuvem (CSPs). Embora a nuvem ofereça benefícios consideráveis, as organizações que adotam soluções baseadas em nuvem também podem se beneficiar de uma compreensão de relativa maturidade de suas próprias práticas de segurança.

As tendências de segurança identificadas neste relatório são resultados de dados anônimos coletados de 12.000 participantes de uma pesquisa realizada durante o período de novembro de 2012 a fevereiro de 2014. As tendências são representativas de uma amostra mundial.

Para obter mais informações, incluindo resultados mundiais e as tabelas das quais os resultados foram criados, consulte www.microsoft.com/trustedcloud.

[1] *2014 Forecast: Tech Trends in Commercial Banking - (Previsão para 2014: Tendências tecnológicas no setor bancário comercial)* - www.channelpronetwork.com/article/Top-Cloud-Trends-in-the-SMB

[2] *Market Trends: Banking, Worldwide 2014* (PDF) www.luxoft.com/upload/iblock/36c/market_trends_banking_worldw_gartner.pdf

Principais conclusões

20% das organizações financeiras pesquisadas não usam controle de acesso baseado em função

As organizações financeiras que não usam funções executadas por funcionários (como administrador, usuário e convidado) para gerenciar o acesso podem permitir acesso ilegal a recursos e criar vulnerabilidades.

26% de todos os setores pesquisados no mundo não usam controle de acesso baseado em função, o que sugere que as organizações financeiras (em 20%) estão mais maduras a esse respeito.

Além disso, 38% das respostas indicam que as organizações financeiras estão registrando e fazendo auditoria do acesso do usuário com base em políticas e práticas adequadas.

Cerca de 20% das organizações financeiras não têm os mecanismos, as políticas ou os procedimentos para cancelar ou alterar acesso dos funcionários quando eles são desligados ou realocados, que é a mesma percentagem que a média mundial do setor.

O fator humano constitui uma das mais importantes contribuições para o sucesso de um plano de segurança das informações, mas também apresenta um dos maiores riscos. Funcionários mal-intencionados ou descontentes com acesso a ativos de informações importantes podem ser uma ameaça significativa à segurança e proteção desses ativos. Até mesmo pessoas sem má intenção podem constituir um perigo se não entenderem claramente suas responsabilidades de segurança das informações.

Recomendação

Restrinja o acesso por função e também por necessidade de saber. Restrinja o número de pessoas que podem conceder autorizações a um conjunto relativamente pequeno de membros confiáveis da equipe e controle as autorizações com sistema de tíquetes/acesso. Revise e atualize regularmente uma lista de pessoal autorizado.

Os principais CSPs normalmente realizam verificações em segundo plano regulares de pré e pós-contratação de seus funcionários.

21% das organizações financeiras pesquisadas não são eficazes no gerenciamento do acesso físico

Essa falta de capacidade de gerenciar acesso físico pode deixar os arquivos e ambientes de segurança vulneráveis, sem responsabilidades.

30% de todos os setores pesquisados no mundo não são eficazes no gerenciamento do acesso físico, o que sugere que as organizações financeiras (21%) estão mais maduras a esse respeito.

Manter o controle do acesso físico atualizado é um dos passos mais importantes que qualquer organização pode dar para proteger ativos de informações confidenciais. Se uma parte mal-intencionada obtiver acesso não autorizado às instalações que armazenam dados confidenciais, hardware e componentes de rede, os ativos de informações podem estar sujeitos a um risco significativo de divulgação, danos ou perdas.

Recomendação

Apenas pessoal autorizado deve ter acesso aos ambientes de dados e data center. Mecanismos comuns de segurança incluem portas protegidas por leitores biométricos ou crachás de identificação, pessoal da recepção que precisa identificar positivamente os funcionários e fornecedores autorizados e políticas que exigem acompanhantes e crachás para os visitantes autorizados.

CSPs normalmente conduzem operações em instalações de alta segurança protegidas por uma série de mecanismos que controlam o acesso a áreas confidenciais. Usar esse tipo de CSP pode ajudar a reduzir o custo do gerenciamento de data centers no local.

37% das organizações financeiras pesquisadas não usam classificação de dados padronizada

Essa conclusão sugere que informações confidenciais podem ser erroneamente classificadas ou nem ser classificadas.

42% de todos os setores pesquisados no mundo não usam classificação de dados padronizada, o que sugere que as organizações financeiras (em 37%) estão mais maduras no uso de classificação de dados.

Classificação de dados padronizada, que envolve associar cada ativo de dados a um conjunto de atributos padrão, pode ajudar uma organização a identificar os ativos que requerem tratamento especial para oferecer segurança e proteção de privacidade.

Recomendação

As organizações precisam garantir que os armazenamentos de dados, que contêm os dados do cliente, sejam classificados como ativos confidenciais que requerem um nível elevado de segurança.

Os CSPs normalmente classificam os dados e outros ativos de acordo com políticas bem definidas, que determinam um conjunto padrão de atributos de segurança e privacidade, entre outros.

23% das organizações financeiras pesquisadas têm políticas e práticas adequadas para proteger eliminação de dados

Além disso, em mais de 14% das organizações bancárias, espera-se que os funcionários, individualmente, desempenhem funções de backup e retenção de documentos, sem uma política ou procedimento formal, que pode potencialmente levar a violações de retenção de dados.

31% de todos os setores pesquisados no mundo têm políticas e práticas adequadas para proteger a eliminação de dados, o que sugere que as organizações financeiras (em 23%) estão menos maduras em relação a isso.

Uma política eficaz de eliminação de dados fornece orientações sobre como e onde eliminar dados de modo seguro e protegido e ajuda a fornecer aos usuários as ferramentas necessárias para cumprir a política.

Recomendação

As organizações devem ter um plano de backup e recuperação de dados que defina uma abordagem de backup e recuperação dados em caso de necessidade. Um plano típico de backup e recuperação de dados atribui responsabilidades claras ao pessoal específico e define os objetivos de backup e recuperação. Além disso, políticas fortes que regulam a eliminação adequada de registros eletrônicos e em papel podem ajudar a impedir que dados confidenciais sejam divulgados sem autorização.

Os CSPs geralmente mantêm uma estrutura de backup e recuperação de dados consistente com as práticas do setor. Além disso, dados eletrônicos armazenados em provedores de nuvens estão normalmente sujeitos a fortes políticas de eliminação de dados, que se originam de programas de classificação de dados e requerem que a mídia descartada seja destruída ou transformada conforme descrito pelo programa de recuperação e retenção de dados.

22% das organizações financeiras pesquisadas ainda não estabeleceram um programa formal de gerenciamento de riscos

Além disso, os mesmos 22% mais provavelmente só realizam avaliação de risco quando ocorre um incidente.

27% de todos os setores pesquisados no mundo não estabeleceram um programa formal de gerenciamento de riscos, o que sugere que as organizações financeiras (em 22%) estão mais maduras a esse respeito.

Realizar avaliações de risco regularmente pode ajudar uma organização a acompanhar como os dados confidenciais são armazenados e transmitidos entre aplicativos, bancos de dados, servidores e redes. A avaliação de riscos ajuda a conformidade com períodos de retenção definidos e requisitos de eliminação no fim da vida útil, além de ajudar a proteger os dados contra o uso não autorizado, acesso, perda, destruição e falsificação.

Recomendação

As organizações devem ter um plano de segurança de informações. Tais planos são mais eficazes quando integrados a uma estrutura maior de gerenciamento de risco de informações.

CSPs geralmente realizam avaliações de risco regulares que avaliam ameaças à confidencialidade, integridade e disponibilidade de dados e outros ativos sob seu controle; eles costumam usar estruturas de gerenciamento de riscos de informações gerenciadas centralmente.

29% das organizações financeiras pesquisadas não têm um plano de resposta a violações de segurança

Essa conclusão pode indicar que os mesmos 29% das organizações nunca realizaram um teste de cenário de pior caso e só agem quando são solicitados a fazê-lo.

40% de todos os setores pesquisados no mundo não têm um plano de resposta a violações de segurança, o que sugere que as organizações financeiras (em 29%) estão mais maduras a esse respeito.

Quando ocorre um incidente de segurança, relatórios adequados e oportunos podem significar a diferença entre conter os danos e a sofrer uma violação maior ou perda de ativos de informações importantes.

Recomendação

Para uma resposta eficaz a incidentes, é importante comunicar que eventos de segurança das informações precisam ser comunicados às partes imediatamente e claramente.

Os CSPs geralmente exigem que seus funcionários informem sobre quaisquer incidentes de segurança, pontos fracos e defeitos imediatamente usando procedimentos bem documentados e testados.

38% das organizações financeiras pesquisadas não têm planos orçados de recuperação de desastres

Um plano de recuperação de desastres define a abordagem e as etapas que uma organização adotará para retomar as operações em condições adversas, como desastres naturais, ataques ou agitação.

35% de todos os setores pesquisados no mundo não têm planos orçados de recuperação de desastres, o que sugere que as organizações financeiras (em 38%) estão menos maduras a esse respeito.

Recomendação

Um plano de recuperação de desastres deve ser criado atribuindo claras responsabilidades ao pessoal específico; definir os objetivos da recuperação; delinear os padrões para notificação, encaminhamento e desaceleração, além de oferecer treinamento a todas as partes interessadas.

Os CSPs geralmente mantêm estruturas de recuperação de desastres que sejam consistentes com práticas dos setores.