AÇÕES CONFIÁVEIS

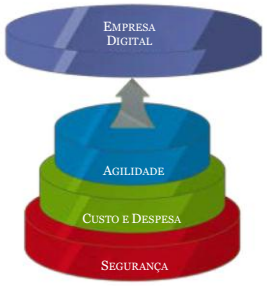
O setor bancário com flexibilidade e capacidade de resposta

"A principal preocupação dos nossos clientes é se podemos fazer negócios com eles em segurança. Se não conseguirmos mostrar que somos inteligentes o suficiente para sermos confiáveis, eles irão embora e não voltarão."

CEO de uma organização internacional de bancos, fevereiro de 2018

Segurança e proteção. Esse é o principal assunto quando se fala do mercado digital com as organizações. Nesse universo, não há setor mais sensível do que os grupos financeiros comerciais que fazem negócios pela Internet. Quando os clientes não estão protegidos contra vulnerabilidades de dados, organizações financeiras de produtos e serviços arriscam expor completamente a base monetária que viabiliza esse negócio.

Para uma organização de serviços financeiros comerciais prosperar como uma empresa longeva e saudável, é essencial que ela seja capaz de demonstrar competência na proteção das informações dos clientes.

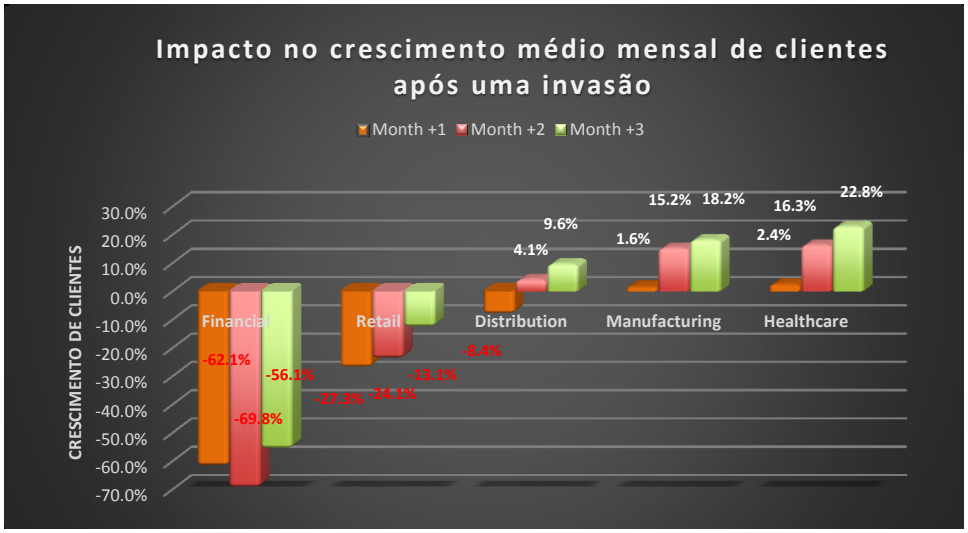


BASE DO MERCADO DIGITAL

Agilidade e flexibilidade são importantes para competir no mercado digital, mas é fundamental que todas as transações realizadas por uma organização sejam seguras e protegidas, especialmente na área de serviços financeiros. A perda da confiança após uma importante violação é uma facada no coração de uma organização.

Em um estudo recente da Solitaire Interglobal Ltd. (SIL), foi analisado o efeito na base de clientes de uma organização de diversos setores. A rapidez e a força da resposta adversa dos clientes a violações em prestadores de serviços financeiros são muito maiores e mais frágeis do que em qualquer outra área.

Os clientes precisam confiar que a organização protege as informações que coleta deles e que usa para conduzir os negócios. A falha nessa área corrói a reputação de uma organização mais rapidamente do que qualquer outro fator. Isso transparece como uma traição de um acordo não declarado entre comprador e vendedor.



A recuperação dos clientes financeiros ao nível anterior à violação pode levar até 19,5 meses. Mesmo o tempo médio informado de 7,5 meses é extremamente caro para uma organização financeira comercial.

Se uma organização depende de novos clientes, o custo para conquistar um novo cliente aumenta em média 1,32 em comparação com o que era antes da invasão. Qualquer expansão de mercado terá que lidar com o restabelecimento da reputação para que os novos clientes se sintam confiantes o suficiente para se envolver com a empresa. Para isso, a vulnerabilidade demonstrada e a falha de segurança precisam ser superadas.

Se uma organização tenta recuperar os clientes que a abandonaram, os custos informados por organizações financeiras maduras são 18,6 vezes maiores do que o inicial de aquisição da empresa. Para uma organização financeira que ainda não é madura (em atividade há mais de cinco anos e com uma retenção de clientes anual normal superior a 80%), as chances de ela existir como entidade autônoma e viável em um ano são de apenas 34,2%.

Em outras palavras, ser hackeado é extremamente ruim para os negócios. Especialmente para organizações financeiras.

A viabilidade da organização financeira também é extremamente sensível ao número de violações e como esses eventos são tratados. Em alguns casos, as organizações tentaram esconder o fato de que houve uma invasão significativa. As reações emocionais dos clientes afetados são diretamente atribuíveis à rapidez e à facilidade com que a empresa reage à violação.

> *"A confiança cibernética é crucial para as finanças. A consistência entre segurança e ameaça é um fator fundamental na reputação e na confiança do cliente."*
>
> Stéphane Nappo, diretora global de Segurança da Informação e assessora do conselho da IBFS, Paris, França

A perda da integridade dos dados e da proteção das informações dos clientes pode acontecer, não importa o rigor da segurança definida por uma organização. A maioria dos clientes entende isso, portanto, uma invasão no sistema de segurança não é necessariamente o grande problema. No entanto, o sentimento de traição e erosão da confiança é ampliado quando uma organização não reage a uma violação com firmeza e postura. Assumir os problemas é uma forma de humanizar uma organização, mas essa solução não funciona para todas as empresas. Definir uma postura em relação a segurança e invasões é, portanto, um componente essencial das políticas e dos procedimentos de uma empresa.

Sem prontidão, não há como amenizar a reação dos clientes quando uma invasão acontece. Os clientes que se sentem traídos por uma empresa têm muito menos probabilidade de voltar a essa organização. Em um estudo com mais de 175 mil organizações, mais de 78% dos clientes se recusavam a voltar após uma violação se a organização não assumisse o evento imediatamente. Mais de 79% esperavam que a organização atacada explicasse precisamente o que estava fazendo para remediar a vulnerabilidade e reparar qualquer dano que tivesse sido feito.

Tentar encobrir o incidente foi visto por mais de 95% dos clientes respondendo às perguntas como um desrespeito a eles como indivíduos. Ou, como um participante anotou: "Por que eu faria negócios com uma empresa que mostrou que não me vê como pessoa? Por que eu faria qualquer coisa com alguém que não me valorizasse?"

Quanto vale a viabilidade de uma organização? Qual seria o impacto da perda da maior parte dos clientes atuais no resultado final? Esta é a compensação realista para o incômodo e a despesa da segurança cibernética. Se os clientes não confiarem em uma organização, eles não farão negócios com ela.

Isso resulta em uma queda imediata e de longo prazo nas receitas. Isso também agrava ainda mais a reputação já prejudicada do negócio. Dependendo de uma série de fatores de remediação, esses clientes podem nunca retornar. Se o fizerem, será somente após um gasto significativo com serviços, equipamentos e pessoal para restabelecer uma posição confiável e atrair os clientes de volta.

SOLUÇÕES LINUXONE PARA BANCOS

Uma maneira de lidar com esse risco é criar uma base que tenha uma segurança demonstrável de alto nível. Isso faz com que a escolha da plataforma vá além do custo imediato, exigindo que as empresas examinem todo o risco e a exposição que o *negócio cibernético* traz com suas promessas lucrativas.

O IBM LinuxONE é um componente significativo na construção de uma base para a transformação. Ele aborda as principais áreas de sucesso no novo mercado de segurança, resiliência e desempenho que permitem que as organizações respondam com agilidade aos desafios que aparecem todos os dias no ciberespaço.

Os custos direcionados são afetados positivamente pela solução LinuxONE. Minimizar as despesas com menos pessoal necessário e um custo de propriedade significativamente menor é extremamente benéfico. As diferenças nessa área são significativas, com *economia de* TCO *de até 80%* e *redução nos níveis de equipe de até 60%* ou mais.

Segurança é onde a solução LinuxONE faz a maior diferença. É muito menos provável que os hackers consigam violar as proteções necessárias para o inventário digital quando a cibersegurança básica tem um ponto de partida mais rigoroso. Na verdade, as implementações do LinuxONE mostram *menos de 0,01%* de invasões de segurança bem-sucedidas por 1000 aplicações implantadas do que outras arquiteturas.

O custo mais baixo para proteger a reputação de uma organização e o impacto na receita é tão significativo que pode fazer a diferença entre uma organização ser viável ou não. A proteção contra invasões se traduz facilmente em mais confiança dos clientes, o que, por sua vez, leva a receitas mais altas e mais fidelidade do cliente.

No volátil mundo dos negócios cibernéticos, a confiança nas organizações que detêm o controle básico das finanças é a mais sensível e frágil. Proteger essa confiança supera outras preocupações como velocidade e flexibilidade, já que a velocidade para uma empresa incapaz de proteger e reter os clientes é irrelevante.

SOLITAIRE INTERGLOBAL LTD.

A Solitaire Interglobal Ltd. (SIL) vem coletando dados sobre a evolução do mercado e o comportamento de produção há mais de 40 anos. Dando suporte a mais de 6 mil clientes e executando mais de 100 milhões de modelos preditivos a cada ano, a SIL também conduziu o Global Security nos últimos 22 anos. Esse serviço de associação permitiu que a SIL construísse um repositório que ultrapassa 550 PB de dados em um nível muito granular. Esses dados são extraídos a cada hora para encontrar tendências, fazer comparações e determinar limites que ajudam as organizações a serem bem-sucedidas.

ATRIBUIÇÕES E ISENÇÕES DE RESPONSABILIDADE

Este documento foi desenvolvido com o financiamento da IBM. Apesar de o documento poder usar material disponível público de vários fornecedores, inclusive da IBM, ele não necessariamente reflete as posições desses fornecedores sobre os assuntos tratados neste documento.

42018942BRPT