Ética e Integridade

Denise Debiasi

Bi2 PARTNERS

Quando auditorias e consultorias falham

wildpixel_CANVA

Pode perceber que atrás de todo grande escândalo corporativo sempre há a atuação questionável das empresas de auditoria e consultoria, algumas de renome internacional. Isso acontece tanto no Brasil quanto no exterior. O público e a mídia sempre se perguntam quando explodem casos de fraudes contábeis com o poder de abalar as estruturas do mercado: como auditores e consultores não conseguiram ver que havia coisas muito erradas nas contas e nos planos de gestão das companhias?

O questionamento é pertinente pois a função das auditorias é justamente atestar a idoneidade das informações financeiras dos clientes. E a tarefa das consultorias é auxiliar na administração saudável de quem as contrata.

Vejamos o que se passou na Americanas, o exemplo mais bombástico de cambalacho financeiro dos últimos anos no Brasil. A companhia varejista contratou uma grande companhia para auditar suas contas entre 2016 e 2019. Os auditores encontraram várias inconsistências contábeis, notificaram a alta administração da varejista sobre os problemas detectados e emitiram um comunicado para os acionistas. Sem receber quaisquer respostas do cliente por quase um mês, a companhia auditora teve o contrato de prestação de serviço inexplicavelmente rescindido. A alegação para o destrato foi uma mera razão comercial.

Outra empresa foi contratada no lugar para avaliar as contas da Americanas a partir de então. E para a nova empresa de auditoria, uma multinacional de fama internacional, não foi detectada nenhuma anomalia financeira que pudesse preocupar acionistas, diretores, fornecedores, clientes e bancos. Com o parecer favorável das contas da varejista, o mercado dormiu tranquilamente por mais três anos. Até que o novo presidente da Americanas encontrasse a fraude algumas semanas após assumir o cargo. Aí a bomba explodiu!

As perguntas que fazemos são: por que alguns auditores notaram os erros financeiros do cliente e outros não? Por que a auditoria que comunicou as falhas contábeis à alta direção teve o contrato rescindido? E o que ganhou a empresa de auditoria que não cumpriu sua obrigação de denunciar os crimes que a varejista estava praticando por anos?

As respostas para tais questões devem fazer parte do trabalho da área de compliance das empresas de consultoria e auditoria mundo afora. Afinal, o que se passou na Americanas é o mesmo enredo de quase todas as fraudes financeiras recentes. Ou a crise da companhia brasileira é muito diferente do drama vivenciado quase que simultaneamente pela FTX?! Acredito que não. Olhando mais para trás, como as empresas de consultoria e auditoria deixaram passar outras falhas bisonhas nos balanços da WorldCom, Banco Nacional, Merck, Parmalat, Enron Corporation, EBX, Tyco e BRB?

Se as auditorias existem para zelar pela autenticidade das informações financeiras do mercado capitalista, quem é que zela pela credibilidade das empresas de auditoria? Essa é uma boa questão que precisamos fazer e exigir respostas de autoridades.

Saiba quem é a nossa Colunista:

Denise Debiasi é CEO da Bi2 Partners, reconhecida pela expertise e reputação de seus profissionais nas áreas de investigações globais e inteligência estratégica, governança e finanças corporativas, conformidade com leis nacionais e internacionais de combate à corrupção, antissuborno e antilavagem de dinheiro, arbitragem e suporte a litígios, entre outros serviços de primeira importância em mercados emergentes.

Empresas & Negócios

www.netjen.com.br

Colaboradores felizes e clientes satisfeitos: entenda como as experiências estão conectadas

A relação que a empresa estabelece com seus colaboradores é fundamental para que a experiência do cliente seja inesquecível; o CEO da Dialog, Hugo Godinho, comenta sobre os benefícios de investir em Customer Experience

No cerne de uma estratégia de sucesso voltada para o cliente, está o que chamamos de Customer Experience – um componente vital para as marcas que se preocupam em fortalecer suas imagens no mercado. Entretanto, antes de investir nessa jornada de experiência do consumidor, é fundamental que as empresas reconheçam que o primeiro passo precisa ser dado dentro da própria organização.

Nesse contexto, a Comunicação Interna desempenha um papel essencial, contribuindo para que colaboradores felizes deixem clientes satisfeitos. Construir experiências cada vez mais positivas no ambiente de trabalho é um dos compromissos que grandes empresas têm assumido nos últimos anos. Afinal, de acordo com dados da Willis Towers Watson, esse tema é uma prioridade para 90% das organizações. Isso ocorre porque falar sobre experiência é falar, também, sobre resultado.

gradyreese_CANVA

Números divulgados por Josh Bersin mostram que organizações que se destacam em Employee Experience têm 2,2 vezes mais chances de exceder metas financeiras, 2,4 vezes mais chances de agradar os clientes e 5,1 vezes mais chances de engajar e reter os profissionais. Ou seja, no final, quando a experiência do colaborador é positiva, ela é refletida na qualidade do trabalho que ele executa.

Para Hugo Godinho, CEO da Dialog, HRTech que lidera o setor de CI com foco em engajamento no Brasil, a experiência do colaborador e a do cliente são dois lados da mesma moeda. "Colaboradores motivados, informados e engajados são a base para um atendimento excepcional ao cliente. A influência da comunicação no ambiente de trabalho transcende os limites da empresa, determinando não apenas como as mensagens são recebidas, mas também como será a experiência nas interações com o público geral", explica.

Diante dessa realidade, a Comunicação Interna é uma importante aliada. O potencial estratégico dessa área precisa acompanhar por completo a jornada do colaborador nas empresas. Isso significa não apenas ser responsável pelo compartilhamento de informações relevantes, mas também atuar de forma proativa no fortalecimento da cultura organizacional. Quando falamos em experiência do colaborador, precisamos saber que ela reflete a forma como a empresa se conecta e se comunica com ele.

Segundo a Gallagher, 82% dos profissionais acreditam que a Comunicação Interna é um dos principais impulsionadores da experiência do colaborador na organização. Dessa forma, se a empresa não investe em CI, dificilmente garantirá uma experiência satisfatória – tanto para o público interno quanto para o externo, que são os clientes e consumidores.

Ataques à cadeia de suprimentos são foco de cibercriminosos

Especialistas da companhia destacam os principais tipos de ataques.

Os ataques cibernéticos se transformaram em uma das maiores ameaças da atualidade, e um dos focos mais emergentes e alarmantes nesse contexto são os ataques à cadeia de suprimentos. Esses eventos têm como objetivo aproveitar fragilidades nas operações de abastecimento e entrega de produtos e serviços de uma organização, que frequentemente envolvem múltiplos stakeholders, como fornecedores, fabricantes, distribuidores e varejistas.

O termo "cadeia de suprimentos" refere-se ao conjunto de processos e atividades relacionados à produção, transporte, armazenamento e entrega de produtos ou serviços ao cliente final. Na era da informação digital, essa cadeia é frequentemente suportada por sistemas informatizados que, se comprometidos, podem levar a interrupções significativas, perdas financeiras e danos à reputação das organizações.

Em 2020 e 2021, exemplos significativos de ataques ocorreram e viraram destaque. O primeiro episódio aconteceu em uma empresa de software de gestão de rede, que foi comprometida por atacantes que inseriram um backdoor em uma de suas atualizações de software. Assim, quando empresas e agências governamentais em todo mundo instalaram a atualização comprometida, os atacantes ganharam acesso às suas redes. Já o segundo, ocorrido em 2021, teve como foco uma empresa de software de gestão de TI. Os atacantes exploraram uma vulnerabilidade em seu software VSA e implantaram ransomware em redes de clientes que usavam o produto.

"Provedores de Serviços Gerenciados (MSPs) frequentemente se tornam alvos em ataques desse tipo, devido ao amplo acesso que possuem às redes de seus clientes. Quando um MSP é comprometido, os invasores podem facilmente expandir sua presença nas redes dos clientes", afirma Caique Barqueta, Especialista em Inteligência de Ameaças da ISH Tecnologia.

Essa estratégia é usada pelos atacantes para estender seu domínio e obter acesso a redes que seriam desafiadoras de invadir de outra forma. Mesmo que uma empresa possua sólidas medidas de segurança, se um de seus fornecedores for vulnerável, ele se tornará o ponto de entrada. Uma vez dentro da rede do fornecedor, os criminosos podem aproveitar essa relação de confiança para infiltrar-se na rede principal.

Os tipos de ataques à cadeia de suprimentos têm aprimorado sua complexidade e evoluído ao longo do tempo. Os mais frequentes são:

• Ataques de software: Comprometendo o software legítimo durante o processo de desenvolvimento ou atualização, os atacantes inserem códigos maliciosos para que quando instalados ou atualizados no software da organização-alvo, a empresa fique vulnerável a ameaças.

Syda Productions_CANVA

- **Ataques de hardware:** Os atacantes modificam ou inserem componentes existentes de hardware durante o processo de transporte ou manufatura. Com isso, pode permitir que eles espionem, modifiquem ou interrompam as operações que utilizam esse hardware.

- **Ataques via provedores de serviço:** Os invasores ao comprometerem os Provedores de Serviço Gerenciados (MSPs), desbloqueiam acesso a redes e sistemas de seus clientes, podendo usar esse acesso para atacar os clientes do MSP.

- **Ataques por infiltração de fornecedor:** Muitas vezes organizações dão acesso a suas redes para fornecedores confiáveis para fins de manutenção, suporte ou outros serviços. Atacantes podem comprometer esses fornecedores e usar esse acesso legítimo para entrar nas redes das organizações-alvo.

- **Ataques de insiders maliciosos:** Insiders podem ser funcionários, ex-funcionários, parceiros... que com o conhecimento adquirido podem acessar e comprometer a organização. Esses ataques são motivados por ganhos financeiros, vingança ou outras razões.

- **Espionagem da cadeia de suprimentos:** Os atacantes, ao invés de comprometerem diretamente uma organização, espionam as comunicações entre fornecedores, buscando informações sensíveis ou pontos de acesso potenciais.

"Estes ataques escancaram a importância de olhar para a segurança de forma mais ampla, não se limitando apenas ao que uma organização faz internamente, mas também considerando todas as pessoas e empresas com as quais ela se relaciona. Manter a cadeia de suprimentos segura é essencial para garantir a proteção geral da organização", conclui Barqueta.