LOGICALIS
Architects of Change

PORQUE É QUE A CIBERSEGURANÇA TEM DE SER UMA PRIORIDADE MÁXIMA PARA OS EXECUTIVOS C-LEVEL

O trabalho remoto, pelo menos em regime parcial, veio para ficar. Gigantes do mundo da tecnologia, como Facebook, Shopify, e Twitter, indicaram que irão permitir aos seus colaboradores trabalhar a partir de casa mesmo quando for considerado seguro voltar ao escritório.
Estas mudanças estão a revelar-se populares, e muitos colaboradores aceitam bem a ideia e gostariam de continuar a trabalhar a partir de casa. De facto, há muitos aspetos positivos, tanto para os colaboradores como para as empresas, no novo modelo de trabalho híbrido, tais como a diminuição das deslocações e a capacidade das organizações contratarem a partir de uma base de candidatos mais ampla, sem restrições geográficas.
Mas também há desvantagens. Uma das questões fundamentais em torno do trabalho remoto e híbrido envolve a cibersegurança, uma vez que alguns colaboradores podem ser mais propensos a correr riscos em casa do que no escritório. Estas mudanças podem tornar as empresas vulneráveis a riscos de cibersegurança e conformidade, e um ciberataque pode ter enormes custos e implicações financeiras para uma organização.
Com o trabalho remoto como parte da"normalidade", tanto agora como no futuro, as empresas precisam de dar prioridade à cibersegurança dos colaboradores remotos. Muitas empresas já estabeleceram conectividade e fluxos de trabalho à distância para cumprir objetivos empresariais durante o último ano; o requisito agora é avaliar a segurança e garantir que não estão a ser alvos fáceis para os cibercriminosos.

CONSEQUÊNCIAS DOS CIBERATAQUES

Um estudo da Malwarebytes descobriu que, desde o início da pandemia, as violações de segurança, em 20% dos inquiridos, resultaram de trabalhadores remotos. Os ciberataques podem ter um impacto prejudicial em toda a organização, e a sua prevenção tem de ser uma prioridade empresarial.
As consequências mais óbvias de não ter essa prioridade são financeiras, especialmente se uma violação de segurança envolver transferências eletrónicas fraudulentas. Contudo, os seus efeitos podem chegar muito mais longe. Mesmo que dinheiro não esteja diretamente envolvido, o ataque pode, ainda assim, ter um impacto fiscal negativo nos resultados financeiros de uma empresa. Há custos de resposta e de recuperação, um custo de investigação, a dificuldade da perda de receitas, despesas legais e de relações públicas, entre outros fatores.
Um ciberataque também pode resultar em perda de produtividade. A tecnologia lenta, ou uma interrupção da tecnologia, significa que a força de trabalho não pode aceder a aplicações e sistemas cruciais para as empresas. A menor produtividade e o aumento dos custos que daí resultam podem destabilizar a continuidade empresarial e mesmo abrandar o futuro crescimento da empresa.
Uma força de trabalho desprotegida também coloca em risco os dados críticos dos seus clientes. Consumidores e empresas querem interagir com organizações que tratam os seus dados com cuidado e segurança. No ano passado, assistiu-se a casos de pirataria de grandes dimensões, que envolveram o Twitter, o Zoom, e várias organizações de saúde. Considerando o importante papel do Zoom em manter as empresas a trabalhar durante a pandemia, o seu hacking, em abril de 2020, e consequente perda de 500.000 palavras-passe de clientes, foi sentido em todo o ecossistema empresarial.
A confiança é, deste modo, uma componente vital. Embora as violações de dados tenham, atualmente, uma consequência real para as organizações, nos termos do Regulamento Geral de Proteção de Dados e de outras legislações associadas por todo o mundo, a confiança, e a sua perda, são mais difíceis de quantificar com precisão. Perder a confiança dos clientes tem um efeito prejudicial na reputação da marca, e voltar a conquistá-la pode ser um desafio.

ADOTAR UMA ABORDAGEM HOLÍSTICA

Providenciar segurança à força de trabalho, de forma holística, incluindo às pessoas que lidam diariamente com clientes e dados de clientes, pode proteger as empresas de danos à sua reputação a longo prazo.
Manter os colaboradores híbridos seguros, onde quer que estejam, é agora uma componente essencial para garantir o futuro sucesso empresarial. As empresas devem procurar implementar uma estratégia de segurança holística que não só inclua produtos e serviços, mas que também aproveite a experiência da sua equipa de segurança e reconheça que a segurança é um processo contínuo. Assim como os cibercriminosos nunca deixarão de aperfeiçoar os seus métodos de ataque, as ferramentas para os combater devem, também, evoluir continuamente.
Utilizando uma abordagem holística, é possível desenvolver, implementar e manter uma postura de segurança eficaz que incorpora toda uma infraestrutura de IT e promove a tecnologia existente.
Uma estratégia de segurança holística deve ser resiliente, adaptável e fácil de gerir. Os passos para criar uma abordagem de segurança abrangente variam consoante as necessidades da empresa, mas devem incluir:

- **Determinar os riscos dentro da sua organização:** Compreender a sua vulnerabilidade ao ataque é fundamental para adotar o framework correto.
- **Criar um ecossistema arquitetado e fortemente integrado:** Muitos destes podem, atualmente, ser automatizados para combater o ataque antes deste ocorrer.
- **Reconhecer os ataques:** Conhecer as várias fases de um ataque de ransomware irá ajudá-lo a determinar a melhor forma de proteger a sua empresa.
- **Alinhar a estratégia de segurança com as operações:** Para uma estratégia de segurança bem desenvolvida, a coordenação com as operações comerciais é essencial para proteger os assets certos e preparar a empresa para o futuro.
- **Escalar para o futuro:** Promover os serviços geridos para inovar continuamente e em escala.

Sem uma força de trabalho protegida, as empresas podem correr o risco de causar danos a longo prazo ao seu negócio. Contudo, com uma força de trabalho securizada, beneficiam de seguro contra danos e perdas, e oferecem um serviço mais robusto aos seus clientes e colaboradores.