



Vertigo3d\_CANVA

NOVA ERA

## BANCOS E INSTITUIÇÕES FINANCEIRAS DEVEM MODERNIZAR ABORDAGEM À SEGURANÇA FÍSICA

Muitos bancos de varejo e instituições financeiras ainda utilizam tecnologias de segurança física implementadas há mais de uma década. Embora esses sistemas legados ajudem a proteger os negócios até certo ponto, eles não conseguem acompanhar o novo cenário de ameaças da Era Digital.

As soluções legadas, embora antes eficazes, agora criam fragmentações que limitam o compartilhamento de informações e a escalabilidade. Esse desafio é agravado pelas crescentes ameaças cibernéticas, especialmente prevalentes no setor bancário", afirma José Rodrigues da Silva Neto, gerente de Vendas da Genetec para as verticais de Varejo e Finanças.

Com frequência, sistemas de monitoramento de vídeo, controle de acesso e de intrusão mais antigos, são soluções proprietárias e fechadas. Isso cria fragmentação na forma como são gerenciados e mantidos, bem como na maneira como as pessoas se conectam e compartilham informações.

Limitam também o quanto uma instituição pode escalar as operações, quais dispositivos pode escolher e a quais novas tecnologias terá acesso no futuro. "Em última análise, tudo isto contribui para maiores lacunas de segurança, processos demasiado complexos e dispendiosos e mais estresse para os operadores", diz o executivo da Genetec. Este cenário é expressivamente agravado pelas crescentes ameaças cibernéticas, especialmente prevalentes no setor bancário.

De acordo com o Relatório Estado da Segurança Física da Genetec, um número considerável de 50% dos profissionais do setor bancário e financeiros relataram ter sido alvo de cibercriminosos em 2023, em comparação com a taxa global de 31% em todas as indústrias pesquisadas. Para permanecerem competitivos, em conformidade e resilientes, os bancos e instituições financeiras precisam ser capazes de se adaptar.

"Com esta finalidade é fundamental investir em uma plataforma de segurança mais flexível e unificada, que pode ajudar a centralizar estratégias de mitigação de riscos e construir uma base mais forte e mais cibersegura. Além disso, adotar essa abordagem os manterá ágeis conforme surgem novas necessidades, além de abrir uma série de novas tecnologias de ponta, como aplicações na nuvem, analíticos de negócios e diversas soluções que automatizam e digitalizam processos desatualizados", explica Silva Neto.

Essas soluções mais recentes ajudam ainda mais os bancos e instituições financeiras a otimizar os dados de segurança física para obter informações comerciais valiosas. À medida que os bancos começam a buscar upgrade para sua infraestrutura de segurança física, saber o que procurar e priorizar durante a tomada de decisões pode levar a resultados mais bem-sucedidos. Arquitetura aberta, unificação, cibersegurança, automação de fluxo de trabalho e otimização de dados devem ser sempre prioridade máxima.

Nos bancos e instituições financeiras, as equipes de segurança física não estão focadas apenas em manter as pessoas seguras e proteger edifícios e ativos. Hoje, elas também tentam mitigar fraudes, combater



REVCO/IMAGEM CANVA

crimes cibernéticos, identificar ameaças internas e enfrentar a violência no local de trabalho.

Embora as agências bancárias e instituições financeiras compartilhem alguns desafios comuns, seus ambientes e necessidades únicos são muito diferentes. Os bancos de varejo gerenciam a segurança física em agências que podem variar de alguns sites em uma cidade pequena a centenas em todo o país. Independentemente da sua área de atuação, eles compartilham um objetivo de segurança comum: manter os colaboradores e ativos bancários seguros e, ao mesmo tempo, garantir uma experiência tranquila e conveniente para o cliente.

Para cumprir esses objetivos, cada site pode ter vários tipos de tecnologias implementadas. Isso pode incluir videomonitoramento, controle de acesso, intrusão, intercomunicação e outros sistemas de vários fornecedores. Outro fato é que muitas agências tendem a ficar presas a soluções mais antigas, proprietárias e independentes. Isso torna muito difícil para as equipes de segurança física verem o que está acontecendo em todos os locais, responder com eficácia às ameaças e cuidar da manutenção do sistema.

Esse problema é agravado por todas as fusões e aquisições que acontecem no setor bancário. "Quando os bancos se unem, as tecnologias existentes nas diversas agências nem sempre podem ser facilmente ligadas. E sem ter uma maneira de gerenciar e controlar centralmente esses sistemas, cresce a fragmentação e as lacunas na segurança. Equipamentos legados de segurança física também podem manter as organizações bancárias presas ao passado.

As tecnologias mais antigas não conseguem empregar escala de forma eficaz para satisfazer às crescentes exigências dos bancos progressistas. Além disso, estes sistemas desatualizados não foram concebidos para ajudar os bancos se adaptarem à evolução dos padrões de proteção de dados e de privacidade", comenta Silva Neto. Há também uma oportunidade perdida de utilizar estes sistemas de segurança para compreender melhor a experiência do cliente nas agências.

As soluções de segurança física coletam muitas informações e as tecnologias mais antigas simplesmente não possuem as ferramentas analíticas para transformar esses dados em insights de negócios valiosos. De acordo com o executivo da Genetec, as demais instituições financeiras geralmente precisam proteger um site corporativo de grandes dimensões ou alguns escritórios, geralmente em centros movimentados de cidades ou áreas suburbanas.

Milhares de colaboradores, visitantes e prestadores de serviços passam por suas portas e, para mantê-los seguros, equipes de segurança física monitoram diversos tipos de sistemas. Isso pode incluir videomonitoramento, controle de acesso, intrusão, intercomunicação, analíticos de vídeo, incêndio e segurança e vários outros sistemas prediais.

Embora tenham acesso a toda esta tecnologia e informação, nada está ligado. Isto significa que quando surgem incidentes, os operadores precisam alternar de um sistema para outro para descobrir o que está acontecendo antes de resolver o problema e isso não é fácil quando se tem de gerenciar um grande volume de credenciais com tecnologias antigas que não possuem a automação necessária.

Afinal, exigirá que se vasculhe pastas para encontrar procedimentos operacionais padrão (SOPs) e que se confie em planilhas para rastrear credenciais incapazes de atender aos padrões modernos. "À medida que as instituições financeiras digitalizam as operações, precisam de tecnologia de segurança física que acompanhe o ritmo", detalha Silva Neto.

Por este motivo, quando as instituições do setor financeiro começam a procurar uma nova solução de segurança física, há muito a considerar. Embora bancos, financeiras e seguradoras tenham critérios diferentes nas suas listas de prioridades existem aspectos fundamentais a serem considerados em um projeto bem-sucedido de segurança. O primeiro deles é escolher soluções de arquitetura aberta em vez de hardware e software proprietários.

"Padronize com um sistema flexível que permita dimensionar as operações de segurança e adicionar novas tecnologias de ponta e dispositivos conectados à nuvem conforme a necessidade, ressalta Silva Neto. Em seguida integre vídeo, controle de acesso, intrusão e outros sistemas em uma plataforma de segurança unificada, conectando todos os sistemas e sites a um centro de operações de segurança e empregue recursos móveis para monitoramento e resposta remota.

Outro aspecto importante é consolidar os esforços de cibersegurança e privacidade usando uma única plataforma, usando defesas cibernéticas integradas e recursos de privacidade para mitigar riscos potenciais e aproveitar implementações na nuvem ou híbridas para agilizar atualizações e práticas recomendadas de segurança cibernética. "Priorize também a automação para aprimorar a resposta a incidentes e o trabalho investigativo.

Experimente novos módulos, recursos e soluções avançadas para digitalizar processos, reduzir custos e capacitar seus operadores de novas maneiras. É essencial investir em uma plataforma com recursos integrados que ajudam a otimizar os dados, assim é possível obter insights valiosos para melhorar a experiência do cliente, monitorar o uso e a ocupação das instalações e aprimorar as iniciativas de automação predial", destaca o executivo da Genetec.

Para permanecerem competitivos, em compliance e resilientes, os bancos de varejo e instituições financeiras precisam modernizar sua abordagem à segurança física, mudando para uma plataforma de segurança flexível e unificada, que possa centralizar estratégias de mitigação de riscos e construir uma base mais forte e mais cibersegura. - Fonte e mais informações: (www.genetec.com/br).



JOES CANVA