Cibersegurança em IoT: o que os recentes ataques a infraestruturas conectadas ensinam sobre vulnerabilidades críticas

José Roberto Rodrigues (*)

A possibilidade de monitorar e controlar equipamentos a distância trouxe ganhos de eficiência para empresas de diferentes portes e setores, sobretudo no segmento industrial. A tecnologia IoT (Internet das Coisas) consolidou-se como um dos pilares da Indústria 4.0, transformando parques fabris tradicionais em ambientes inteligentes e integrados.

Essa convergência de máquinas, sensores, robôs e sistemas de software industriais à internet permite a coleta, o compartilhamento e a análise de dados em tempo real diretamente do chão de fábrica, tornando essas operações mais eficientes e produtivas. Os ganhos vão da manutenção preditiva, que reduz paradas não planejadas, à otimização operacional, com menos desperdícios, gargalos logísticos e consumo de recursos. Isso gera economia e contribui para uma operação mais sustentável.

No entanto, esses ganhos ficam em risco quando o avanço operacional não é acompanhado por uma arquitetura de segurança adequada. Com a Inteligência Artificial e a expansão da nuvem, esses riscos também ganham escala. Ao conectar esse ecossistema de infraestrutura digital à internet, é preciso estabelecer controles rigorosos. Uma falha na cadeia de fornecimento de tecnologia pode comprometer o investimento e a continuidade da operação.

Vulnerabilidade crítica

Uma invasão a sistemas de refrigeração afetou redes varejistas em sete países, menos de um mês após um evento similar na França. Os casos expõem a vulnerabilidade digital da cadeia de abastecimento alimentar da Europa.

O ataque hacker que atingiu redes de varejo na França, como Carrefour, Intermarché, Coopérative U e Monoprix, no começo de outubro, causando prejuízos financeiros estimados em dezenas de milhões de euros e afetando cerca de 700 lojas, mostrou os riscos para a infraestrutura de TI. O episódio, que mirou sistemas de refrigeração industrial e colocou em risco a conservação de alimentos, deixou evidente como falhas na proteção de dispositivos conectados podem ultrapassar o ambiente digital e comprometer operações físicas. Recentemente, uma nova onda de ataques cibernéticos a redes de supermercados em diferentes países europeus voltou a expor a vulnerabilidade digital da cadeia de abastecimento alimentar. Os incidentes reforçam a necessidade de rever a governança e a maturidade da segurança de dispositivos IoT.

Nos dois episódios, os sistemas de refrigeração estiveram entre os alvos, evidenciando os riscos associados à exposição de equipamentos industriais conectados à internet. Dispositivos com configurações inadequadas, credenciais vulneráveis ou softwares desatualizados podem se transformar em portas de entrada para invasores. Mesmo quando os fabricantes disponibilizam correções de segurança (patches), a proteção depende de uma gestão contínua de atualizações, acessos e monitoramento. Quando essa responsabilidade é negligenciada, uma vulnerabilidade aparentemente restrita a um equipamento pode gerar consequências em toda a operação.

A dimensão desse risco acompanha a expansão acelerada dos perímetros digitais. Segundo dados do IoT Security Statistics, da Ordr, fornecedora de soluções de segurança, estima-se que já existam mais de 21 bilhões de dispositivos conectados globalmente, com projeção de alcançar 39 bilhões até 2030. A consultoria também aponta uma média de 820 mil ataques diários a dispositivos IoT em 2026 – um salto de 46% em relação ao período anterior —, sinalizando que mais da metade desses ativos possui vulnerabilidades críticas exploráveis. São números que ajudam a entender o desafio enfrentado pelas organizações em proteger seus ambientes conectados.

Cibersegurança em Tecnologia Operacional (TO)

Embora a discussão sobre cibersegurança industrial não seja nova, o caso francês reforça a necessidade de uma atuação preventiva do mercado de TI. A higiene cibernética básica inclui avaliar e aplicar atualizações de firmware e software de IoT assim que disponibilizadas pelos fabricantes, considerando os requisitos de continuidade da operação. Do ponto de vista de arquitetura de rede e infraestrutura de TI, dispositivos críticos jamais devem ser expostos diretamente à internet pública. O acesso remoto a esses ambientes precisa ser controlado, trafegando por redes virtuais privadas (VPNs) seguras, com autenticação multifator (MFA).

A segregação de redes — separando o ambiente de Tecnologia Operacional (TO) da rede corporativa ou do Wi-Fi de clientes — é outra prática essencial de arquitetura que pode mitigar os riscos desse tipo de ataque. Essa separação ajuda a impedir que o comprometimento da rede de escritórios alcance o maquinário físico das lojas. Além disso, o monitoramento preventivo e o uso de soluções analíticas em tempo real para detectar comportamentos anômalos (como o acionamento de um ciclo de aquecimento em freezers industriais na madrugada) ajudam a proteger a continuidade da operação.

Visão integrada de segurança

O acesso remoto e a conectividade em nuvem são essenciais para a competitividade das empresas. Eliminá-los em nome da segurança é retroceder no avanço tecnológico. Para mim, o objetivo da governança deve ser garantir que essa conectividade não comprometa a continuidade dos negócios. Adotar abordagens modernas de segurança baseadas no conceito de Zero Trust, por exemplo, é um dos caminhos para controlar os acessos aos ativos corporativos e reduzir sua exposição a ataques.

Essa realidade exige uma atuação conjunta entre as equipes de Tecnologia da Informação (TI), tradicionalmente responsáveis pela proteção de dados, e as equipes de Tecnologia Operacional (TO), focadas na operação física. Tratar essas áreas de forma isolada cria pontos cegos na segurança.

Com o avanço da Indústria 4.0, a cibersegurança da IoT precisa ser considerada desde o início da implementação de hardware. Deve fazer parte do desenho da solução, incluindo a escolha dos equipamentos, a política de atualizações, a gestão de identidades e acessos privilegiados e os planos de contingência. Entendo que essa responsabilidade envolve toda a cadeia de TI, incluindo a gestão de terceiros – fornecedores, prestadores de serviços, clientes e parceiros de negócios.

Conectividade, infraestrutura e segurança precisam caminhar lado a lado para garantir eficiência e disponibilidade nas operações. À medida que dispositivos digitais passam a comandar ativos físicos, proteger os acessos, monitorar comportamentos e limitar os efeitos de possíveis invasões também passa a fazer parte da continuidade dos negócios.

(*) Country manager & alliances manager LATAM da Adistec, uma das principais distribuidoras de valor agregado em soluções de TI do Brasil e América Latina.

Consórcio ganha força em diferentes cenários da economia e pressiona modernização tecnológica das administradoras

Mesmo em cenários de juros altos ou baixos, modalidade segue gerando demanda; Topaz já implantou seu novo ERP nos primeiros clientes e projeta ampliar a adoção da solução em 2027

O mercado brasileiro de consórcios mantém sua trajetória de crescimento, mesmo em cenários de instabilidade econômica. Com o crédito mais caro, o modelo ganha espaço como alternativa para consumidores que querem adquirir bens sem as taxas de juros de outras formas de financiamento. Quando os juros caem e a economia melhora, o consórcio também se beneficia do aumento da renda disponível e passa a ser considerado uma opção de planejamento financeiro.



kutubQ_CANVA

Essa resiliência se reflete na aquisição de bens. Dados apresentados pela Associação Brasileira de Administradoras de Consórcios (ABAC) mostram que cerca de um em cada três veículos leves vendidos no país é adquirido por meio de consórcio, proporção que chega a uma em cada duas motocicletas. No entanto, também aumenta a concorrência entre administradoras para oferecer jornadas mais eficientes, seguras e acessíveis aos consumidores.

"O consórcio consegue passar por diferentes momentos da economia porque atende a uma necessidade que permanece: a vontade de adquirir um bem e planejar essa conquista. Em um cenário de crédito mais caro, ele ganha ainda mais relevância, mas, quando os juros estão baixos, também continua competitivo como instrumento de planejamento", afirma Jorge Iglesias, CEO da Topaz, uma das maiores empresas de tecnologia especializada em soluções financeiras digitais do mundo e parte do Grupo Stefanini.

O crescimento do mercado traz uma questão para as administradoras: a pressão por eficiência. Nos últimos meses, a Topaz tem percebido uma preocupação ainda maior do setor com temas como proteção contra fraudes, qualidade da venda, análise de crédito e entrada de documentos, além da busca por mais agilidade nos processos de contemplação e faturamento dos bens. Na avaliação da empresa, isso reforça a necessidade de contar com uma tecnologia capaz de acompanhar o aumento da demanda sem se tornar um limitador da operação.

"As administradoras estão mais criteriosas em relação ao que entregam ao cliente, ao vendedor e às próprias equipes. Ao mesmo tempo em que o mercado cresce, aumenta a concorrência. Isso exige mais qualidade, segurança e eficiência dos fornecedores de tecnologia", diz Iglesias.

É nesse contexto que a Topaz vem ampliando sua atuação no segmento e lançou neste ano, após três anos de desenvolvimento, o ERP especificamente para o mercado de consórcios, já em implantação nos primeiros clientes. A empresa segue para uma sequência de novas implementações e já negocia novos projetos para 2027. A plataforma foi desenvolvida com uma arquitetura mais moderna e não monolítica, com infraestrutura em nuvem e recursos voltados à integração e à digitalização da jornada das administradoras. Segundo estimativas da Topaz, os primeiros clientes já reportam economia de 50% ou mais nos custos de infraestrutura, em comparação com ambientes mais tradicionais.

"Estamos vendo, na prática, que modernizar o ERP pode ter impacto não apenas na experiência do cliente, mas também na eficiência da própria operação. Uma arquitetura mais atual permite escalar, integrar novos canais e reduzir a dependência de estruturas legadas que podem se tornar gargalos para o crescimento", destaca o CEO da Topaz.

Entre os recursos que vêm recebendo maior atenção do mercado está a funcionalidade de múltiplas cotas, que permite à administradora simular uma venda envolvendo diferentes cotas e utilizar inteligência artificial para construir cenários de probabilidade de contemplação, considerando variáveis como lance e valor atualizado das parcelas e sendo flexível para os fluxos operacionais de acordo com o produto e regras. A Topaz também destaca a evolução das estratégias de distribuição por meio de marcas parceiras e modelos white label, que permitem às administradoras ampliar a oferta de consórcios por diferentes canais e marcas.

A evolução tecnológica também responde a uma mudança no comportamento do consumidor. Para a Topaz, as administradoras terão de ampliar o acesso às informações e permitir que clientes escolham diferentes canais para realizar simulações, vendas e atendimentos - desde aplicativos e WhatsApp a parceiros e escritórios de revenda. Para isso, uma infraestrutura baseada em APIs organizadas e seguras passa a ser cada vez mais relevante. Em sistemas legados, a necessidade de abrir chamados com o fornecedor para acessar informações ou desenvolver novas integrações pode aumentar o tempo de resposta. Para uma administradora que precisa lançar campanhas, produtos ou novos canais em escala, a tecnologia não pode se transformar em um limitador e, consequentemente, em um gargalo para a expansão do negócio.

"O consumidor quer mais informação e mais liberdade para escolher como se relacionar com a administradora. Para acompanhar esse movimento, a tecnologia passa a dar velocidade ao negócio. Em 2027, essa deve ser uma das principais agendas das administradoras: modernizar sua infraestrutura para sustentar o crescimento das vendas", conclui Iglesias, CEO da Topaz.

Pesquisa mostra que quase 40% dos leitores trocam anúncios por acesso a notícias

Levantamento mostra que apenas 8% dos leitores priorizam assinaturas e aponta novos caminhos para a sustentabilidade da mídia no Brasil. Uma nova pesquisa sobre o comportamento do consumidor brasileiro revela que 39% dos leitores preferem assistir a um anúncio curto a pagar por uma assinatura - escolhida por apenas 8% - para ter acesso a reportagens restritas por paywall. Os dados apontam para uma oportunidade urgente: a adoção de modelos híbridos baseados em publicidade como caminho para garantir a sustentabilidade financeira do jornalismo digital.

O estudo, encomendado pela Fusify, empresa de tecnologia em publicidade digital que faz parte do ecossistema da Membrana Media, surge em um momento em que a indústria de notícias no Brasil se adapta a mudanças significativas na forma como o público acessa e consome informação. De acordo com o Digital News Report 2026, do Instituto Reuters, apenas 15% dos brasileiros atualmente pagam por notícias online, uma queda de cinco pontos percentuais em relação a 2023. O relatório também destaca o papel crescente das redes sociais e de ferramentas baseadas em IA no consumo de notícias.

O AdWall, da Membrana, oferece uma alternativa ao acesso exclusivo por assinatura, impulsionado pela demanda publicitária da Fusify. Quando os leitores se deparam com um conteúdo restrito, eles podem optar por interagir com uma experiência publicitária curta (vídeo, banner ou animação) em troca da liberação do artigo. Isso permite que os veículos gerem receita publicitária com leitores que não estariam dispostos a pagar por uma assinatura, ao mesmo tempo em que oferece aos anunciantes a oportunidade de alcançar públicos em ambientes editoriais consolidados.

"Em um país onde apenas 15% dos leitores pagam por conteúdo online, os paywalls tradicionais acabam, inadvertidamente, excluindo a grande maioria da população do acesso ao jornalismo de qualidade. A questão para os veículos já não é simplesmente se os leitores vão pagar por notícias, mas sim como construir modelos sustentáveis que reflitam a maneira como as pessoas realmente consomem conteúdo digital. Nossa pesquisa sugere que há demanda por alternativas ao modelo 'pague ou saia'. O AdWall é uma forma de ponte para essa lacuna, permitindo monetizar audiências que talvez não assinassem, ao mesmo tempo em que dá aos anunciantes acesso a leitores engajados", explica Daniela Benoit, Head de Vendas da Fusify Brasil.

O levantamento, realizado com 814 brasileiros com 18 anos ou mais em todas as regiões do país, também destaca os riscos associados aos bloqueios rígidos de conteúdo: ao se deparar com um paywall, 27% dos brasileiros procuram a mesma informação em sites de notícias gratuitos, enquanto 15% recorrem a plataformas de redes sociais (como Instagram e TikTok) ou aplicativos de mensagem (como o WhatsApp).

Essa migração para fontes não verificadas é particularmente crítica durante períodos eleitorais, quando o acesso a informações de confiança é fundamental. Para os veículos, isso cria uma oportunidade de reter mais leitores dentro de seus próprios ambientes digitais, em vez de perdê-los após um bloqueio estrito.

Em vez de substituir os modelos de assinatura, a proposta do AdWall é complementar as abordagens existentes no jornalismo digital e contribuir para uma discussão mais ampla sobre receita sustentável e acesso a conteúdos confiáveis.

Metodologia: A pesquisa foi realizada em outubro de 2026 com 814 brasileiros de 18 anos ou mais, residentes em todas as regiões do país. Os dados foram coletados por meio de um questionário online aplicado via plataforma Toluna Insights.