Como a governança robusta de TI protege operações e dados estratégicos

O setor de varejo, cada vez mais digital e dependente de tecnologia, tornou-se um dos alvos preferenciais dos cibercriminosos

Luciano Costa (*)

Quase 25% de todos os ciberataques no mundo hoje tem como alvo empresas de varejo. Estima-se que 80% dos varejistas globais sofreram ataques no último ano – muitos enfrentando múltiplos incidentes, como infecção por malware em sites, tentativas de transações fraudulentas e violações em gateways de pagamento.

Os impactos financeiros também escalam: o custo médio de uma violação de dados no varejo atingiu cerca de US$ 3,91 milhões em 2024, um aumento de 18% em relação ao ano anterior. Além do prejuízo financeiro direto, esses incidentes abalam a confiança dos consumidores – 62% dos clientes afirmam não confiar na segurança de seus dados nas empresas de varejo.

anyaberkut_CANVA

Principais riscos: dados, disponibilidade e fraudes

Diversas ameaças cibernéticas impactam o varejo digital moderno, sendo as mais críticas o vazamento de dados sensíveis, indisponibilidade de sistemas, ataques de negação de serviço (DDoS) e fraudes online. Os vazamentos expõem informações confidenciais de clientes, podendo resultar em perda de confiança, penalidades regulatórias e danos à reputação das marcas. A indisponibilidade causada por falhas ou ataques, como o ransomware, paralisa sistemas essenciais, prejudica vendas e pode gerar grandes prejuízos financeiros.

Ataques DDoS, especialmente críticos durante campanhas como Black Friday, derrubam sites ao sobrecarregar servidores com tráfego malicioso, causando perda imediata de vendas e danos à imagem da empresa. Fraudes digitais, como uso de cartões roubados e interceptação de pagamentos, exploram falhas no processo e são difíceis de prevenir devido à velocidade e à ausência de padrões claros. Esses riscos muitas vezes se combinam, reforçando a necessidade de uma abordagem estruturada e holística em segurança digital para mitigar impactos ao negócio.

Governança de TI estruturada: a chave para mitigação de riscos

Para enfrentar as ameaças crescentes, os varejistas digitais precisam adotar uma governança de TI robusta e bem estruturada, baseada em boas práticas e em compliance.

Isso inclui desde planejar antecipadamente respostas a diferentes cenários de ataque, até implantar arquitetura de TI redundante e planos de continuidade de negócios. Com governança, a empresa consegue antecipar ameaças e preparar respostas, em vez de reagir de forma caótica após o dano.

Por exemplo, equipes de segurança bem treinadas e protocolos definidos podem conter um ataque de ransomware antes que ele se espalhe, ou isolar um sistema afetado para manter o restante das operações funcionando. Essa postura proativa reduz drasticamente tanto a frequência quanto o impacto dos incidentes.

Uma governança de TI robusta no varejo digital deve estar fundamentada em pilares essenciais, como políticas claras de segurança que definam protocolos detalhados, auditorias periódicas e capacitação contínua dos colaboradores. Somada a isso, é crucial implementar uma gestão rigorosa de acessos, adotando o princípio do menor privilégio e ferramentas avançadas de autenticação, minimizando vulnerabilidades internas e prevenindo usos indevidos.

Complementando essas práticas, é essencial automatizar processos críticos como atualizações de segurança, monitoramento contínuo e backups frequentes, reduzindo erros humanos e acelerando respostas.

Em síntese, à medida que o varejo se torna mais digital e os criminosos cibernéticos mais audazes, investir em governança de TI sólida e em práticas rigorosas de segurança deixou de ser opcional – é um imperativo estratégico para a sobrevivência e sucesso no setor.

Uma governança bem estruturada, apoiada pelas melhores práticas de mercado e pela aderência a normas de compliance, mitiga os riscos cibernéticos e aumenta a resiliência operacional das empresas varejistas. Isso significa proteger os dados críticos e sistemas essenciais contra ameaças, mas também garantir que, mesmo diante de um incidente, a empresa consiga manter suas operações ou se recuperar rapidamente.

O resultado é duplo: preservar a continuidade do negócio e manter a confiança dos clientes em um ambiente de compras digitais seguras. Em um cenário de ameaças em constante evolução, a capacidade de antecipar-se aos riscos e responder de forma eficaz pode definir quais organizações do varejo conseguirão prosperar na era digital de forma segura e sustentável.

(*) Cofundador da Setrion Software e Milldesk.

Como o comportamento humano ameaça a segurança cibernética

O ataque cibernético que chacoalhou o país, em julho de 2025, acendeu um alerta quanto à proteção contra as ameaças cibernéticas. Vale recordar que o ataque que afetou pelo menos seis importantes instituições financeiras do Brasil, incluindo o Banco Central, tinha como alvo uma empresa de tecnologia, responsável por prestar serviços de transferência e segurança para as transações via PIX.

A preocupação com esses ataques vai além da possível quebra de confiança institucional e da reputação das organizações, visto que as invasões têm se mostrado cada vez mais frequentes e sofisticadas. Para se ter uma ideia, uma pesquisa realizada pela Grant Thornton, empresa de consultoria e auditoria, e pela Opice Blum Advogados, empresa especializada em direito digital, revela que 79% das empresas no Brasil se sentem expostas a ataques cibernéticos. Nesse contexto, é natural que nos perguntemos: o que pode facilitar invasões como a que ocorreu recentemente e como proteger empresas e instituições financeiras de ataques como esses?

Ao longo da minha carreira na área de cibersegurança, liderando processos em grandes corporações, pude perceber que o passo número 1 é a análise de risco, que consiste em pensar em todas as possibilidades e o impacto de cada ameaça. Neste sentido, proteger as redes de empresas e grandes instituições de ataques comuns como phishing, pagamento por privilégios para funcionários ou terceiros, ransomware e deepfakes, por exemplo, exige uma série de precauções que devem ser seguidas. Porém, além de estar atentos a essas técnicas, atualmente tem sido necessário focar em uma que vem ganhando notoriedade, principalmente após esse caso de invasão a instituições brasileiras: a engenharia social.

Isso porque esse tipo de abordagem se baseia em uma forma de ataque que engana, manipula ou explora a confiança de uma pessoa que trabalha em serviços de dados para que ela, de forma voluntária - exceto no caso de pagamento por privilégios -, repasse a senha de plataformas restritas para desconhecidos, de maneira que se possa acessar informações ou realizar transações bancárias livremente, como foi o caso noticiado recentemente. No segundo semestre de 2024, um dos métodos da engenharia social, o vishing (combinação das palavras "voice" e "phishing" – que aplica golpes por meio de ligações telefônicas), teve um crescimento de 442% em todo o mundo, em qualquer âmbito, de acordo com o Relatório Global de Ameaças 2025, desenvolvido pela empresa especializada em segurança cibernética CrowdStrike. Nessas ocasiões, um ponto chama a atenção: a confiança em seres humanos como a última camada de proteção.

O estudo realizado pelo Fórum Econômico Mundial aponta que 95% dos problemas de cibersegurança são causados por erro humano. Isso reforça um argumento muito comentado pelos especialistas na área, que é o fato de o fator humano ser um elo fraco em situações como o ataque que ocorreu no Brasil. Essa discussão não ventila a possibilidade de substituição da figura humana, mas atenta para o que pode ser feito para que esses profissionais assumam uma postura mais confiável diante desses possíveis ataques.

Para que as empresas se sintam mais seguras com os seus dados, alguns dos principais tópicos a serem abordados são a conscientização e a capacitação dos profissionais para que situações de risco sejam evitadas. Com isso, os funcionários poderão compreender de forma mais clara que desempenham um papel essencial na proteção da empresa para a qual estão trabalhando e se sintam verdadeiramente preparados para enfrentar qualquer tipo de golpe. Além disso, o monitoramento dos acessos e dos dados da corporação são fundamentais para evitar incidentes que comprometam informações restritas.

Mitigar esse problema requer um grande desafio e um olhar especialmente voltado às pessoas. No entanto, para que funcionários e gestores estejam sintonizados no caminho de uma empresa mais segura é fundamental, principalmente, que haja ética e conscientização da responsabilidade que cada profissional tem neste setor. Sendo assim, é possível que casos, como o que vimos recentemente no Brasil, sejam cada vez menos frequentes.

(Fonte: Daniel Aragão é head de Cyber Security da NEC na América Latina).

Modernização de Infraestrutura com IA

Alex Pereira (*)

A infraestrutura de TI tradicional tem se mostrado limitada diante dos desafios atuais enfrentados por organizações de todos os setores, não apenas negócios nativamente digitais. Estamos em uma era em que resiliência, observabilidade, automação e inteligência adaptativa são mandatórias. Incorporar Inteligência Artificial ao núcleo da infraestrutura não é mais apenas uma vantagem competitiva, é um catalisador poderoso para alcançar um novo patamar de eficiência, adaptabilidade e proteção em ambientes cada vez mais complexos.

Da virtualização para a infraestrutura cognitiva

Virtualização foi um passo, automação via scripts foi outro, agora, estamos avançando para a era da infraestrutura cognitiva, onde soluções baseadas em Inteligência Artificial e Machine Learning já conseguem analisar grandes volumes de telemetria, comportamento e sinais de risco, sugerindo ou até mesmo, em alguns casos, aplicando ações corretivas em tempo real. De redes autônomas a ambientes AIOps e plataformas de segurança automatizada, a tomada de decisão orientada por dados está deixando de ser conceito e se tornando prática operacional em ambientes modernos.

Essa mudança é tão estrutural quanto a introdução da nuvem pública há uma década. A diferença agora é que não se trata apenas de tecnologia de sustentação, mas de capacidade estratégica para continuidade, economia operacional e vantagem competitiva.

Observabilidade inteligente: De logs a insights preditivos

Em arquiteturas modernas, observabilidade não é mais sobre monitorar CPU ou uptime. É sobre capturar e correlacionar eventos em tempo real de milhares de fontes (APIs, containers, endpoints, redes etc.), aplicando modelos de IA que detectam anomalias contextuais, como o comportamento irregular de um microsserviço sob carga específica. Por exemplo, em ambientes de última geração, soluções como Dynatrace ou Datadog detectam um aumento anômalo na latência de uma API crítica, identificam automaticamente a causa raiz, como sobrecarga no banco de dados, e executam uma mitigação automatizada, redirecionando o tráfego para uma réplica saudável. Tudo isso ocorre em segundos, sem intervenção humana, com alertas acionados para o time de engenharia em tempo real.

Automação autônoma e autosserviço com IA Generativa

A automação clássica depende de fluxos predefinidos. O novo paradigma é a orquestração inteligente com IA, onde a infraestrutura entende intenções declarativas, sugere remediações, valida segurança e executa com rastreabilidade.

Hoje, soluções como Harness.io, StackStorm com LLMs e plataformas GitOps já permitem automações declarativas com inteligência contextual. Ainda que o paradigma de um copiloto de infraestrutura 100% autônomo esteja em evolução, os avanços recentes mostram que estamos nos aproximando rapidamente de um modelo onde intenções declarativas como "Aumentar resiliência da aplicação X" poderão ser interpretadas e executadas com supervisão reduzida, rastreabilidade e governança.

De acordo com um estudo recente da Deloitte, organizações que avançaram além da fase inicial de testes em automação inteligente, relataram uma economia média de custos de 32%.

Segurança proativa e resiliência dinâmica

A infraestrutura moderna precisa ser ciber-resiliente por design, com IA monitorando padrões de acesso, eventos de sistema e comportamento lateral, integrando com threat intelligence e respondendo em segundos.

A segurança moderna vai além de firewalls e antivírus. É sobre antecipar, detectar e responder rapidamente às ameaças antes que se tornem incidentes. Plataformas como o Vydar são fundamentais neste novo modelo, ao fornecerem inteligência contínua sobre ameaças externas, incluindo phishing, vazamentos, sites falsos e ameaças na dark web, que muitas vezes são os vetores de entrada dos ataques.

Uma vez que o perímetro é comprometido, entra em cena o desafio da movimentação lateral, quando o atacante já está dentro da rede e tenta escalar privilégios, acessar sistemas sensíveis e persistir sem ser detectado. Aqui, entram soluções como CrowdStrike Falcon, Microsoft Defender for Endpoint, Darktrace ou Vectra AI, que utilizam IA e modelos comportamentais para identificar padrões suspeitos dentro da rede. Por exemplo, um modelo de ML percebe um padrão de movimentação lateral semelhante a ataques anteriores no honeypot. Ele isola automaticamente o segmento afetado, bloqueia o token de acesso, notifica a equipe e ativa playbooks automatizados para investigação. Essa combinação de visão externa (com soluções como o Vydar) e resposta interna inteligente (com EDR/NDR baseados em IA) é o novo pilar da cibersegurança resiliente.

FinOps com IA: Otimização em tempo real

Em ambientes multicloud, o uso ineficiente de recursos pode gerar perdas significativas. Modelos de IA podem prever picos de demanda, simular cenários de escalabilidade e até sugerir reservas ou conversões de instâncias com base em uso histórico.

A gestão de custos em nuvem evoluiu de painéis passivos para mecanismos inteligentes que não apenas monitoram, mas sugerem otimizações proativas. Ferramentas como Kubecost, CloudZero, ou Azure Cost Management já identificam workloads com potencial de migração para instâncias spot, estimam economia e apontam ações. Por exemplo, a ferramenta identifica que um workload de Kubernetes com tráfego previsível poderia migrar temporariamente para instâncias spot com autoscaling, com economia estimada de até 26%. A execução ainda exige validação e orquestração humana, mas o potencial de impacto já é mensurável. O próximo passo, e algumas empresas já desenvolvem internamente, é a IA executar essas otimizações automaticamente, dentro de políticas de resiliência e segurança.

Como Começar?

1. **Mapeie vulnerabilidades invisíveis:** Quais partes da sua infraestrutura operam sem visibilidade em tempo real? Identifique gargalos onde a tomada de decisão ainda depende de esforço humano contínuo.
2. **Escolha um caso de alto impacto:** Comece pequeno, mas estratégico. Pode ser a automação de resposta a incidentes, otimização de custos com IA ou integração de inteligência de ameaças externas.
3. **Implemente com supervisão e aprendizado:** Estabeleça um ciclo onde a IA age com base em políticas definidas, com supervisão humana, refinando a atuação com feedback iterativo.
4. **Transforme mindset e processos:** Adotar IA na infraestrutura exige mais que tecnologia, exige uma nova mentalidade. Crie um ambiente onde operação e inovação caminham juntas, com cultura de dados, aprendizado contínuo e colaboração entre TI e negócio.

Para concluir, a modernização de infraestrutura com IA não é apenas um upgrade técnico, é um movimento estratégico, inevitável e transformador. Empresas que tratam IA como pilar da infraestrutura se posicionam com resiliência, velocidade e inteligência de decisão muito superiores. Quem liderar esse movimento agora terá uma vantagem assimétrica em um mundo onde tempo, dados e contexto definem sobrevivência e liderança.

(*) - Gerente de Operações de Logística