Cinco dicas para empresas se protegerem de roubo de dados na internet

Segundo COO da BugHunt, dados mais visados para roubo variam entre informações financeiras, pessoais, empresariais e até mesmo genéticas


Hallshadow_CANVA

Atualmente, é cada vez mais comum que empresas e pessoas sejam alvos de roubo de dados. Isso acontece devido à alta dos ciberataques que, em 2024, atingiu um patamar estratosférico. Segundo um estudo realizado pela FortiGuard Labs, o número de tentativas de ciberataques no Brasil alcançou a marca de 356 bilhões, ressaltando a necessidade de maiores investimentos em cibersegurança.

De acordo com Bruno Telles, COO da BugHunt, empresa brasileira de cibersegurança pioneira em Bug Bounty na América Latina, o roubo de dados se trata da aquisição não autorizada de informações confidenciais ou sensíveis de terceiros, com a intenção de explorar essas informações indevidamente, para ganho pessoal ou por propósitos maliciosos, impossibilitando o acesso das empresas ou dos donos desses dados.

"Existem muitas formas de roubo de dados. O phishing é uma das mais comuns e envolve o envio de e-mails, mensagens falsas e até ligações fraudulentas para enganar as vítimas e levá-las a clicar em links maliciosos", explica o especialista. "O malware e ransomware também são muito recorrentes e consistem, respectivamente, na infecção de dispositivos por vírus e no bloqueio de arquivos ou sistemas, exigindo pagamento para restaurar o acesso. Muitas vezes, os ataques também acontecem por meio da invasão de softwares desatualizados e vulneráveis ou por brechas abertas por usuários de redes de Wi-Fi inseguras, já que as informações podem ser interceptadas por invasores que monitoram o tráfego", completa.

Segundo o especialista, os dados mais visados para roubo mudam conforme os objetivos dos cibercriminosos, variando entre informações financeiras, pessoais, de saúde, empresariais, escolares e até mesmo genéticas. "Os dados roubados podem ser usados para diversas finalidades, incluindo fraude financeira, roubo de identidade, extorsão, chantagem ou espionagem corporativa", alerta.

O COO da BugHunt ainda reforça que existem diversas formas de invadir um sistema para a coleta indevida das informações. "Não existe uma fórmula certa para ocorrer um roubo de dados, depende muito da porta de entrada que o cibercriminoso vai utilizar para invadir os sistemas. Isso pode incluir exploração de vulnerabilidades, práticas de segurança inadequadas ou enganação de usuários", complementa.

Diante desse cenário, o especialista em segurança da informação listou cinco passos para empresas se protegerem de roubos de dados na internet.

- **Fortalecer cultura de segurança -** Para Telles, é essencial promover uma cultura de segurança da informação dentro das empresas, e isso inclui a gestão e educação dos colaboradores sobre condutas de cibersegurança. "É importante educar funcionários sobre práticas seguras por meio de treinamentos e workshops. Desta forma, eles conseguirão identificar ataques phishing e anormalidades nas comunicações, além de reforçar a importância de relatar atividades suspeitas", explica.

- **Investir em ferramentas para segurança** - Investir em recursos de defesa é extremamente recomendável para criar uma primeira barreira de proteção para os dados das empresas. "Ferramentas como firewalls, antivírus, Data Loss Prevention, entre outras, funcionam como uma barreira essencial para evitar a infecção dos sistemas por malware e outros tipos de ataques cibernéticos", esclarece o executivo.

- **Realizar políticas de controle de acesso -** Implementar políticas de controle de acesso garante que apenas funcionários autorizados tenham acesso aos dados sensíveis. "É importante utilizar autenticação de dois fatores e passkeys sempre que possível", lembra Telles.

- **Executar testes de segurança** - O especialista reforça que é fundamental testar os sistemas de forma proativa para que se identifique falhas na segurança antes de um ataque real. "O ideal é realizar testes de segurança constantemente, como Pentest e Bug Bounty. Desta forma, é possível identificar e corrigir potenciais vulnerabilidades em sistemas e infraestrutura antes de serem exploradas por cibercriminosos", comenta.

- **Criar um plano de resposta a incidentes -** Outra recomendação do COO da BugHunt é desenvolver um plano de resposta a incidentes de segurança realista e bem estruturado, considerando todas as possibilidades de invasão. "Desta forma, é possível assegurar uma ação mais rápida e eficaz em casos de violação de segurança", conclui.

Adoção de multi-cloud cresce e impulsiona inovação e governança nas empresas

O futuro da transformação digital está na adoção de arquiteturas multi-cloud, que permitem às empresas integrar diferentes provedores e escolher a melhor solução para cada desafio. Essa tendência já é realidade: segundo a Gartner, até 2027 mais de 90% das grandes empresas terão estratégias multi-cloud, enquanto a IDC projeta que o mercado global supere US$ 135 bilhões no mesmo período. No Brasil, dados da ISG mostram que mais de 70% das grandes companhias já utilizam o modelo para equilibrar custo, performance e governança.

Éric Machado, CEO da Revna Tecnologia e especialista em gestão de TI e Supply Chain, ressalta que a transformação vai além da tecnologia. "Multi-cloud é a expressão máxima da liberdade digital. Ela oferece às empresas a possibilidade de montar sua arquitetura como um mosaico inteligente, colocando cada aplicação, banco de dados ou workload no ambiente mais adequado em termos de performance, custo e segurança. Essa orquestração reduz riscos, amplia governança e acelera a inovação", afirma.

A adoção do modelo também está alinhada às principais tendências globais. A McKinsey aponta que o avanço da inteligência artificial generativa acelera a busca por arquiteturas híbridas e multi-cloud, enquanto a Flexera mostra que 89% das organizações colocam segurança e compliance como seus maiores desafios, mas reconhecem o modelo como indispensável para resiliência e inovação. O movimento recente de integração entre Oracle e Microsoft, que permite rodar workloads críticos em ambas as nuvens, reforça como até os gigantes globais se adaptam a essa demanda.

Para Éric Machado, o verdadeiro diferencial do multi-cloud é dar autonomia às empresas para crescer sem amarras. Segundo ele, não são apenas os sistemas que fazem a diferença, mas principalmente as pessoas capazes de arquitetar e orquestrar todo o processo. "Projetos de transformação só geram impacto real quando líderes e times trabalham em colaboração, com propósito e disciplina", afirma.

Na visão do executivo, a conexão entre AWS, Google, Microsoft, Oracle e outros em um ecossistema único e híbrido mostra que a tecnologia pode ser liberdade e competitividade ao mesmo tempo. "Independentemente da aplicação que você rode, seja ERP da própria Oracle, SAP, TOTVS ou qualquer outro sistema, é possível orquestrar a integração de tudo em um ambiente cloud, rico em diversidade e diferenciais, montado sob medida com o que cada fabricante de software tem de melhor para cada cliente. Sem amarras", finaliza Éric.

A Cadeia de Valor como alicerce estratégico na arquitetura organizacional moderna

Tito Borges (*)

No atual cenário de transformação digital e evolução constante do mercado, a construção de uma estratégia organizacional eficaz exige mais do que apenas visão de futuro: requer estruturas sólidas, integradas e adaptáveis

Nesse contexto, a Cadeia de Valor emerge como uma ferramenta essencial, permitindo que as organizações identifiquem, analisem e otimizem seus recursos, ao mesmo tempo em que organizam suas atividades-chave com foco na geração de vantagem competitiva.

Ao mapear todas as etapas da criação e entrega de produtos ou serviços, a Cadeia de Valor permite identificar oportunidades para reduzir custos, melhorar a eficiência e alinhar esforços estratégicos. Mais que uma ferramenta de análise, é um guia prático para conectar as ações da empresa à sua proposta de valor e às demandas do mercado. Essa lógica também orienta a arquitetura organizacional, permitindo estruturar processos, papéis e recursos de forma eficiente, com governança e fluxos bem definidos para maximizar resultados e integração entre áreas.

Na era digital, adaptar a arquitetura organizacional para torná-la mais ágil e responsiva é essencial. Estruturas menos hierárquicas, equipes multidisciplinares e a digitalização de processos promovem inovação, aceleram decisões e aumentam a eficiência. Nesse contexto, a arquitetura de carreiras também ganha destaque ao oferecer trajetórias claras de desenvolvimento, alinhadas às transformações do mercado. Essa abordagem fortalece o engajamento, valoriza a contribuição individual e contribui para atrair e reter talentos em um ambiente cada vez mais competitivo.

Entretanto, estruturar carreiras em um contexto de inovação acelerada representa um desafio considerável. A obsolescência rápida das competências técnicas exige uma atualização constante por parte dos profissionais, além da necessidade de desenvolver habilidades comportamentais que favoreçam a adaptabilidade. Nesse cenário, as organizações devem oferecer trajetórias flexíveis que integrem o desenvolvimento técnico e humano, além de sistemas de avaliação que reconheçam o esforço contínuo de aprendizado e inovação.

As novas tecnologias são fundamentais para tornar as organizações mais eficientes e adaptáveis. Ferramentas digitais e soluções baseadas em dados ampliam a visibilidade dos processos, otimizam recursos e reduzem custos, promovendo estruturas mais dinâmicas. No contexto da Cadeia de Valor, tecnologias como ERP, Business Intelligence, sistemas de governança e plataformas colaborativas fortalecem a integração entre áreas, apoiam decisões estratégicas e aumentam a agilidade na entrega de resultados.

Entretanto, para que essas inovações se consolidem de maneira sustentável, é essencial equilibrá-las com a cultura organizacional. A tecnologia deve ser incorporada de forma humanizada, respeitando os valores, a história e o capital humano da empresa. Líderes e gestores têm um papel fundamental nesse processo, conduzindo as transformações com empatia, promovendo capacitações e garantindo que a mudança tecnológica complemente — e não substitua — a identidade organizacional.

Por fim, vale destacar a importância crescente da cultura orientada a dados (data driven). Adotar essa mentalidade não é apenas uma tendência, mas uma necessidade estratégica. Ao fundamentar decisões em análises precisas, as organizações aumentam sua capacidade de antecipar cenários, personalizar estratégias e inovar com responsabilidade. Essa abordagem fortalece a transparência, estimula a melhoria contínua e conecta todos os níveis da organização aos seus objetivos estratégicos, promovendo crescimento sustentável e relevância em um mercado cada vez mais digital e competitivo.

(*) Associado ABRH-MG e Gerente de Arquitetura Organizacional e Remuneração da FIEMG.