OPINIÃO

Ransomware 2.0: por que hackers não querem só seus dados, mas também sua reputação?

José P. Leal Junior (*)

No submundo do crime cibernético, a reputação virou moeda de troca.

Os dados ainda são valiosos, mas deixaram de ser o alvo principal. Cada vez mais, os ataques de ransomware, um tipo de software malicioso que sequestra dados e exige pagamento para devolvê-los, evoluem para um modelo em que a verdadeira ameaça não é somente perder acesso às informações, mas ver esses dados serem expostos publicamente. Isso porque, hoje, o maior ativo de uma organização é a confiança que ela construiu com seus clientes, investidores e parceiros. E é exatamente isso que os hackers querem controlar.

Um fenômeno conhecido como ransomware 2.0. Nele, o foco deixa de ser o bloqueio de arquivos para o constrangimento público e a destruição da imagem corporativa. O novo jogo é psicológico, estratégico, e extremamente cruel. Ao prometer (e muitas vezes cumprir) a publicação de e-mails internos, segredos industriais ou dados sensíveis de clientes, os criminosos passam a controlar a narrativa pública, pressionando empresas a pagarem não pela restauração de sistemas, mas pelo silêncio.

De acordo com o Relatório de Tendências de Ransomware e Estratégias Proativas da Veeam 2025, o ransomware continua sendo a principal causa de interrupções e indisponibilidade em ambientes de TI. Apesar de uma leve queda no número de empresas afetadas, de 75% em 2023 para 69% em 2024, a ameaça permanece alta: sete em cada dez organizações sofreram ao menos um ataque no último ano. O mais preocupante, no entanto, é a baixa taxa de recuperação dos dados: apenas 10% das empresas conseguiram restaurar mais de 90% das informações comprometidas, enquanto 57% recuperaram menos da metade do que foi perdido.

Mesmo com 98% das empresas declarando possuir um plano de resposta a incidentes de ransomware, o relatório apontou lacunas importantes na estrutura desses planos. Menos da metade inclui práticas técnicas essenciais, como a verificação regular dos backups (44%) ou a existência de uma cadeia de comando definida para situações de crise (30%), elementos que podem fazer a diferença entre uma recuperação rápida e um colapso operacional.

Esses dados mostram que a confiança está sob ataque, tanto interna quanto externamente. Não se trata apenas de falhas técnicas, mas de um golpe que atinge a credibilidade das organizações. A estratégia por trás do ransomware 2.0 é simples, porém eficiente: causar um dano irreversível à reputação da vítima, muitas vezes com impactos mais duradouros do que a própria perda de dados.

Essa tática explora uma fraqueza humana e corporativa muitas vezes negligenciada: o medo da humilhação pública. Ao ameaçar divulgar informações sigilosas, os atacantes amplificam a pressão sobre executivos, tornando o dilema ético e estratégico ainda mais complexo. Pagar ou não pagar o resgate? Assumir o ataque publicamente ou tentar esconder? É nesse vácuo de pânico que os criminosos prosperam.

Por que essa mudança? Porque funciona. Hackers entenderam que expor falhas, escândalos internos ou brechas de compliance gera um efeito dominó: desvalorização de ações, perda de contratos, danos à moral da equipe e desconfiança do consumidor. E como vivemos em uma era em que tudo é público e imediato, a ameaça de um vazamento massivo se tornou mais eficaz do que qualquer código de encriptação.

Diante disso, a resposta não pode ser mais do mesmo. Firewalls (barreiras de proteção digital), backups e antivírus continuam essenciais, mas não são o bastante. As empresas precisam investir em uma nova camada de resiliência: a reputacional. Isso envolve ter planos de resposta a incidentes que incluam comunicação de crise, transparência com stakeholders (públicos estratégicos) e prontidão para atuar sob a pressão da imprensa. Muitas vezes, o que separa uma crise de reputação de uma oportunidade de fortalecimento institucional é a forma como a organização reage, e com que rapidez.

Também é fundamental evoluir do modelo reativo para o proativo. Isso significa adotar novos frameworks, fortalecer políticas de governança de dados, testar vulnerabilidades com frequência e, sobretudo, criar uma cultura de segurança transversal, que envolva desde o board até os estagiários. Afinal, uma senha fraca ou um clique distraído em um e-mail pode ser o início de um escândalo internacional.

A Inteligência Artificial e a automação também atuam como aliadas importantes nesse cenário. Soluções baseadas em IA, por exemplo, já conseguem identificar padrões de comportamento suspeito, acelerar respostas e reduzir o tempo de mitigação. Mas a tecnologia, por si só, não resolve o problema se a cultura da empresa continuar vulnerável à manipulação emocional promovida pelos atacantes.

Por fim, é hora de enxergar a cibersegurança como parte da estratégia de marca. Em um mundo hiperconectado, proteger dados é proteger reputações, e reputações são, muitas vezes, mais valiosas do que qualquer ativo financeiro. O ransomware 2.0 é o espelho de uma nova era, em que a guerra digital é travada também no campo da confiança.

O desafio é grande, mas as oportunidades de aprendizado e transformação também são imensas para aqueles que decidirem investir em resiliência e inovação.

Você está preparado para proteger não só seus sistemas, mas sua imagem?

(*) Country manager da Veeam no Brasil.

Um pouco de água na fervura da inteligência artificial

Nos próximos anos, 50% das organizações que haviam planejado substituir suas equipes de atendimento ao cliente por ferramentas de inteligência artificial deverão reverter essa decisão.

Vivaldo José Breternitz (*)

Elnur_CANVA

Segundo uma pesquisa recente da consultoria americana Gartner, os objetivos inicialmente traçados eram ambiciosos demais - e, no fim das contas, inatingíveis. A transição para um modelo empresarial centrado em inteligência artificial está se revelando muito mais complexa do que se imaginava.

Em março passado, a Gartner entrevistou 163 líderes da área de atendimento e suporte ao cliente. Quase todos os respondentes (95%) afirmaram que pretendem manter seus colaboradores humanos enquanto avaliam qual o papel que as tecnologias de IA podem realisticamente desempenhar dentro de suas organizações.

Kathy Ross, diretora sênior de análise da Gartner, destacou que, embora a IA tenha potencial para transformar o atendimento ao cliente, ela não é uma solução milagrosa. A interação humana ainda é essencial em muitas situações — sobretudo quando o consumidor chega ao final de uma jornada frustrante e precisa de ajuda para resolver problemas com um produto ou serviço recém-adquirido que não funciona como deveria.

A visão atual da Gartner é clara: os serviços de IA devem complementar — e não substituir — a atuação humana. "À medida que o cenário do atendimento ao cliente continua a evoluir, integrar a IA às capacidades humanas é essencial", declarou a empresa.

Apesar dessa mudança de perspectiva, algumas empresas de grande porte seguem em frente com planos de demitir milhares de profissionais da área para substituí-los por tecnologias baseadas em IA generativa. No entanto, segundo Brian Weber, vice-presidente de análise da Gartner, muitas dessas iniciativas não estão correndo como o esperado — por diversos motivos.

Executivos têm abraçado a IA com a expectativa de obter economias expressivas, mas frequentemente subestimam os custos reais envolvidos na implementação e manutenção dessas soluções. A IA generativa, observa Weber, "pode gerar um custo total de operação tão elevado que acaba anulando qualquer economia prevista".

"As pessoas só querem falar com outras pessoas ao telefone", afirma Weber. Para ele, cresce o receio entre os consumidores de que a IA bloqueie o acesso ao suporte humano. De fato, segundo a pesquisa, 51% dos clientes dizem confiar nos atendentes humanos para resolver seus problemas, enquanto apenas 7% depositam maior confiança na IA.

Centros de atendimento exclusivamente baseados em inteligência artificial, conclui Weber, ainda são tecnicamente e financeiramente inviáveis — e, do ponto de vista do cliente, indesejáveis – parece ser uma opinião sensata, contrariando o hype que tem envolvido IA.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor e consultor – vjnitz@gmail.com.

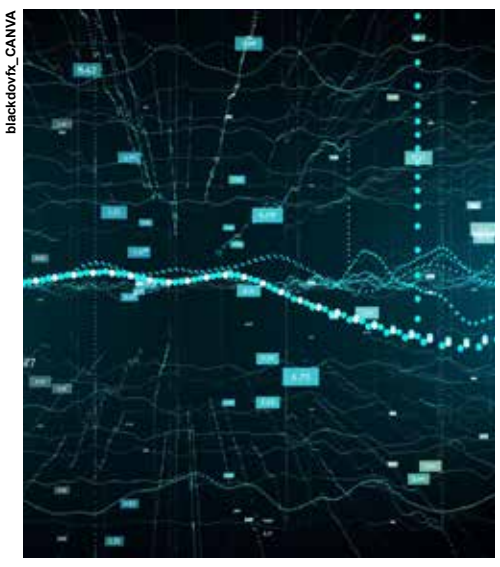
Dados são o novo petróleo da era da IA

Na atual revolução digital, uma verdade se torna cada vez mais evidente: o verdadeiro poder na era da Inteligência Artificial não está apenas nos algoritmos sofisticados, mas no controle dos dados que os alimentam. Esta percepção, que ecoa as análises de especialistas do setor, aponta para uma realidade que muitas organizações ainda não compreenderam completamente.

A estratégia empresarial moderna deve se construir em torno do que podemos chamar de "soberania de dados". É fundamental estabelecer um princípio claro: dados são ativos estratégicos que devem ser gerenciados com responsabilidade e transparência. Não basta simplesmente implementar IA - é preciso uma arquitetura de dados resiliente, ética e alinhada aos objetivos de longo prazo das organizações.

Apesar dos impressionantes US$110 bilhões investidos em startups de IA em 2024, segundo dados da Dealroom, a discussão não deve ter foco apenas na tecnologia. A inteligência artificial é, sem dúvida, uma força transformadora, mas sua eficácia depende intrinsecamente da qualidade, governança e inteligência aplicada aos dados. As grandes empresas de tecnologia entenderam há anos que quem detém os dados, detém o futuro. Não é coincidência que invistam bilhões em

blackdovfx_CANVA



infraestrutura de dados - estão construindo os alicerces da próxima revolução digital.

A nova corrida do ouro digital

O diferencial competitivo de mercado será definido por quem conseguir acessar, controlar e gerar insights a partir dos dados. Quem dominar os dados, assim como a tecnologia, terá capacidade de liderar mercados, influenciar decisões e moldar o futuro digital.

Esta é a nova corrida do ouro da era digital, onde a riqueza não está enterrada no solo, mas dispersa em cada interação, cada clique, cada transação que geramos diariamente. As organizações que compreenderem essa dinâmica e se posicionarem adequadamente terão vantagem competitiva significativa.

Soberania de dados como estratégia

Os próximos anos serão marcados por uma intensa disputa pelo controle informacional, exigindo novas abordagens para governança e transparência. A liderança na era da IA não será definida apenas pelo conhecimento tecnológico, mas pela capacidade de gerenciar dados de forma ética e estratégica.

É fundamental que a discussão sobre IA inclua a gestão de dados como pilar central, considerando seu impacto em comportamentos, decisões e até mesmo crenças. Esta perspectiva holística sobre dados e inteligência artificial representa não apenas uma oportunidade de negócio, mas uma responsabilidade social que não pode ser ignorada.

A revolução que vivemos hoje exige uma nova mentalidade: aquela que reconhece nos dados não apenas números e estatísticas, mas o combustível que moverá a próxima fase da evolução tecnológica e social.

(Fonte: João Paulo Miranda é CEO da Objective).

News @TI

ricardosouza@netjen.com.br

Thomson Reuters lança seu primeiro Agente de IA – CoCounsel para tributário

@A Thomson Reuters lançou sua primeira IA Agêntica, começando com o CoCounsel para profissionais fiscais, tributários, de auditoria e contabilidade. A plataforma Agêntica da Thomson Reuters está em desenvolvimento há mais de um ano, acelerada pela aquisição da Materia, a startup de copilot IA especializada em sistemas agênticos para tributos e contabilidade. Sua base já está ativa em produtos usados por algumas das maiores empresas de contabilidade dos Estados Unidos. Esses novos sistemas estão sendo incorporados em plataformas legais, fiscais, de risco e de conformidade - todos adaptados a ambientes de alto risco onde precisão e confiança não são negociáveis (https://www.thomsonreuters.com.br/pt.html).

Farmácias Digitais leva expertise em IA para otimizar varejo no Desenvolva Day Delivery

@O Farmácias Digitais, ecossistema completo de soluções para o varejo farmacêutico, participa do Desenvolva Day Delivery, que acontece em Uberaba (MG), em 26 de junho (quinta-feira), a partir das 9h. O evento, focado em imersão prática para donos e gestores de farmácias, é uma plataforma fundamental para discutir os avanços e desafios do delivery farmacêutico no Brasil. A presença do Farmácias Digitais neste encontro reforça o compromisso da empresa em impulsionar a transformação digital do setor, oferecendo ferramentas e conhecimentos que promovam mais eficiência, praticidade e confiabilidade aos estabelecimentos (https://cursos.desenvolvaconsultoria.com.br/desenvolva-day-delivery-uberaba/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.