Empresas & Negócios

Matéria de capa

Melpomenem_CANVA

LOJAS VIRTUAIS

COMO PREVENIR ATAQUES E GOLPES NAS VENDAS DE FINAL DE ANO

Já imaginou ver todo o planejamento traçado para as vendas de final de ano ser estagnado devido à indisponibilidade do e-commerce? Infelizmente esse não é um cenário improvável para empresas que ainda não contam com uma estratégia de segurança bem definida para a sua loja virtual. Isso porque, os ataques hackers estão em ascensão.

Mario Gama (*)

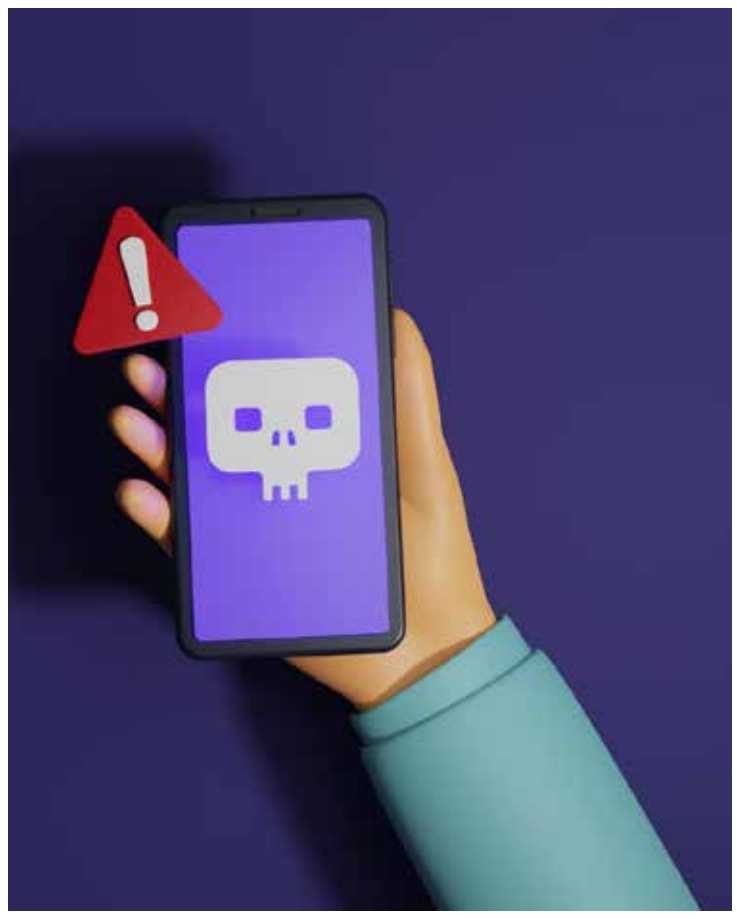
Para se ter uma ideia, um relatório da NetScout sobre ameaças DDoS – que impedem que os usuários consigam acessar o site devido a uma sobrecarga proposital de solicitações – aponta que o Brasil registrou mais de 372 mil ataques DDoS no primeiro semestre de 2024, um aumento de 4,3% em relação ao segundo semestre de 2023. Esse movimento de mercado, indica a necessidade das empresas aprofundarem suas discussões relacionadas à tecnologia e cibersegurança.

IA para bem e para o mal – A Inteligência Artificial (IA) tem se mostrado promissora em muitas áreas e pessoas mal intencionadas já começaram a explorá-la. De acordo com a pesquisa "The State of Cybersecurity in LATAM 2024", cerca de 55% das empresas brasileiras sofreram com ataques cibernéticos alimentados por IA em 2023.

Entre as aplicações destaca-se a deepfake, que adultera conteúdos tornando-os realistas, sendo amplamente utilizada para forjar cadastros e fazer compras ilícitas. Além disso, outro ataque que tem se aperfeiçoado com o apoio da IA são os e-mails fraudulentos, que cada vez mais têm se apresentado como seguro às vítimas.

No entanto, ao mesmo passo que existe esse uso inadequado, profissionais especializados em cibersegurança também têm empregado a IA na identificação automatizada e inteligente da própria deepfake e dos comportamentos anormais dos usuários, assim como na agilidade na resolução de problemas e melhor tempo de resposta a um ataque, que sem o rastreamento ágil poderia levar dias para ser solucionado.

Um estudo da Microsoft, inclusive, aponta que o time de segurança chega a ser 39% mais rápido em atividades como sumarizar um incidente, se comparado a um time sem os recursos de IA. Isso mostra um ganho expressivo em velocidade e desempenho para um time que, definitivamente, precisa agir muito rápido.



Lerbank-bbk22_CANVA

Boas práticas para garantir boas vendas – Considerando todo esse cenário atual do Brasil, vários são os tipos de ataques e golpes que podem afetar uma loja virtual. Não apenas o sistema, mas também funcionários e clientes podem estar suscetíveis. Isso ocorre, pois as motivações de ações fraudulentas variam, em seus mais diferentes níveis de tipos e complexidades.

Nesse contexto, as pessoas mal intencionadas podem querer indisponibilizar o site para inibir as vendas, ter algum tipo de controle do negócio, obter dados de clientes, ou promover um desconto, em interesse próprio, por exemplo. Assim, a conscientização de clientes, funcionários e parceiros se torna imprescindível e urgente.

Afinal, de nada adianta todo o investimento em tecnologia para garantir segurança nas transações enquanto as pessoas compartilham seu acesso com um terceiro por ter sido ludibriada de forma criminosa.

Por isso, é fundamental indicar com clareza quais são os canais de vendas oficiais e alertar sobre possíveis golpes. Em paralelo, fazer o adequado mapeamento de permissões e acessos, além de oferecer autenticação em mais de um fator, é necessário.

No mais, toda a infraestrutura tecnológica tem que estar muito bem estruturada, envolvendo uma avaliação prévia da estimativa de carga que se espera no período de alta demanda, os planos de crescimento e a atualização do ambiente, para inibir que se torne vulnerável. No que se refere especificamente à segurança, também é preciso um plano completo de acompanhamento de vulnerabilidades, bem como testes de resposta a incidentes e de invasão.

Nos períodos de maior demanda, mais do que a preocupação com o time de vendas, é preciso reunir as equipes de infraestrutura, cibersegurança e prevenção de fraudes para executar o planejamento previamente desenhado, monitorando em tempo real as requisições e o comportamento dos usuários, mapeando gatilhos suspeitos e o que está gerando de carga no ambiente, além de identificar possíveis golpes e tentativas de ataque.

Por fim, mas não menos importante: tenha um backup e procedimentos de recuperação testados e treinador pelo time. Esta é a salvaguarda de segurança que toda empresa precisa ter, para que em casos de incidente o sistema seja restaurado. Esse é um ponto importante, pois a maioria dos grupos de ransomware tentam danificar o backup também.

Melpomenem_CANVA

Investir em infraestrutura de TI e em processos maduros de cibersegurança é o caminho – Dado que as oportunidades avançam na mesma velocidade que golpes e ataques, o mercado tem demandado especialização em infraestrutura de TI e cibersegurança.

Para tanto, empresas especializadas tem se mostrado grandes aliadas nessa jornada de evolução digital das lojas virtuais, liderando projetos robustos de estruturação do ambiente, acompanhamento de adversidades e tomadas de ação ágeis e assertivas.

Além de garantir a manutenção dos negócios, também é possível estimular sua ascensão, acelerando não só as vendas de final de ano, mas estimulando um diálogo maduro e necessário sobre o papel da tecnologia e da cibersegurança no varejo digital.

(*) É Cybersecurity Practice Leader Latin America & Caribe da SoftwareOne, provedora global (https://www.softwareone.com/pt-br).