OPINIÃO

O dia depois do ataque hacker: saiba o que priorizar na empresa

Ramon Ribeiro (*)

A ocorrência de um incidente de segurança que resulte em uma invasão hacker é, sem dúvida, um dos maiores pesadelos para qualquer empresa hoje.

Além do impacto imediato nos negócios, há implicações legais e de reputação que podem perdurar por meses ou até anos. No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabelece uma série de requisitos que as empresas devem seguir após a ocorrência de tais incidentes.

De acordo com um relatório recente da Federasul – Federação de Entidades Empresariais do Rio Grande do Sul -, mais de 40% das empresas brasileiras já foram alvo de algum tipo de ataque cibernético. No entanto, muitas dessas empresas ainda enfrentam dificuldades para cumprir os requisitos legais estabelecidos pela LGPD. Dados da Autoridade Nacional de Proteção de Dados (ANPD) revelam que apenas cerca de 30% das empresas invadidas declararam oficialmente a ocorrência do incidente. Essa discrepância pode ser atribuída a diversos fatores, incluindo a falta de conscientização, a complexidade dos processos de conformidade e o medo de repercussões negativas na reputação da empresa.

O dia após o incidente: primeiros passos

Após a confirmação de uma invasão hacker, a primeira medida é conter o incidente para evitar a sua propagação. Isso inclui isolar os sistemas afetados, interromper o acesso não autorizado e implementar medidas de controle de danos.

Em paralelo, é importante montar uma equipe de resposta a incidentes, que deve incluir especialistas em segurança da informação, profissionais de TI, advogados e consultores de comunicação. Essa equipe será a responsável por uma série de tomadas de decisões – principalmente as que envolvem a continuidade do negócio nos dias seguintes.

Em termos de conformidade com a LGPD, é preciso documentar todas as ações tomadas durante a resposta ao incidente. Essa documentação servirá como evidência de que a empresa agiu de acordo com os requisitos legais e poderá ser utilizada em eventuais auditorias ou investigações pela ANPD.

Nos primeiros dias, a equipe de resposta deve realizar uma análise forense detalhada para identificar a origem da invasão, o método utilizado pelos hackers e o alcance do comprometimento. Este processo é vital não apenas para compreender os aspectos técnicos do ataque, mas também para coletar evidências que serão necessárias para reportar o incidente às autoridades competentes e também à seguradora – caso a empresa tenha realizado um seguro cibernético.

Há aqui um aspecto muito importante: a análise forense também serve para determinar se os atacantes ainda estão dentro da rede da empresa – uma situação que, infelizmente, é muito comum, ainda mais se após o incidente a empresa estiver sofrendo algum tipo de chantagem financeira mediante a liberação de dados que os criminosos tenham eventualmente roubado.

Além disso, a LGPD, em seu artigo 48, exige que o controlador de dados comunique à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados afetados acerca da ocorrência de um incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Esta comunicação deve ser feita em prazo razoável, conforme regulamentação específica da ANPD, e deve incluir informações sobre a natureza dos dados afetados, os titulares envolvidos, as medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Com base nessa exigência legal, é essencial, logo após a análise inicial, preparar um relatório detalhado que inclua todas as informações mencionadas pela LGPD. Nisso, a análise forense também ajuda a determinar se houve extração e roubo de dados – na extensão que os criminosos eventualmente estejam alegando.

Este relatório deve ser revisado por profissionais de conformidade e pelos advogados da empresa antes de ser submetido à ANPD. A legislação também determina que a empresa faça a comunicação clara e transparente aos titulares dos dados afetados, explicando o ocorrido, as medidas tomadas e os passos seguintes para assegurar a proteção dos dados pessoais.

A transparência e a comunicação eficaz, aliás, são pilares fundamentais durante a gestão de um incidente de segurança. A gestão deve manter uma comunicação constante com as equipes internas e externas, garantindo que todas as partes envolvidas estejam informadas sobre o progresso das ações e as próximas etapas.

Avaliação das políticas de segurança é ação necessária

Paralelamente à comunicação com as partes interessadas, a empresa deve iniciar um processo de avaliação e revisão de suas políticas e práticas de segurança. Isso inclui a reavaliação de todos os controles de segurança, acessos, credenciais com alto nível de acesso, bem como a implementação de medidas adicionais para prevenir futuros incidentes.

Em paralelo à revisão e análise de sistemas e processos afetados, a empresa deve focar, também, na recuperação dos sistemas e na restauração das suas operações. Isso envolve a limpeza de todos os sistemas afetados, a aplicação de patches de segurança, a restauração de backups e a revalidação dos controles de acesso. É essencial garantir que os sistemas estejam completamente seguros antes de serem colocados de volta em operação.

Uma vez que os sistemas estejam novamente operacionais, é preciso conduzir uma revisão pós-incidente para identificar lições aprendidas e áreas de melhoria. Esta revisão deve envolver todas as partes relevantes e resultar em um relatório final que destaque as causas do incidente, as medidas tomadas, os impactos e as recomendações para melhorar a postura de segurança da empresa no futuro.

Além das ações técnicas e organizacionais, a gestão de um incidente de segurança requer uma abordagem proativa em relação à governança e à cultura de segurança. Isso inclui a implementação de um programa contínuo de melhorias em segurança cibernética e a promoção de uma cultura corporativa que valorize a segurança e a privacidade.

A reação a um incidente de segurança exige um conjunto de ações coordenadas e bem planejadas, alinhadas às exigências da LGPD. Desde a contenção inicial e a comunicação com as partes interessadas até a recuperação dos sistemas e a revisão pós-incidente, cada passo é essencial para minimizar os impactos negativos e garantir a conformidade legal. Mais do que isso, é preciso olhar de frente as falhas e corrigi-las – acima de tudo, um incidente deve levar a estratégia de cibersegurança da empresa a um novo patamar.

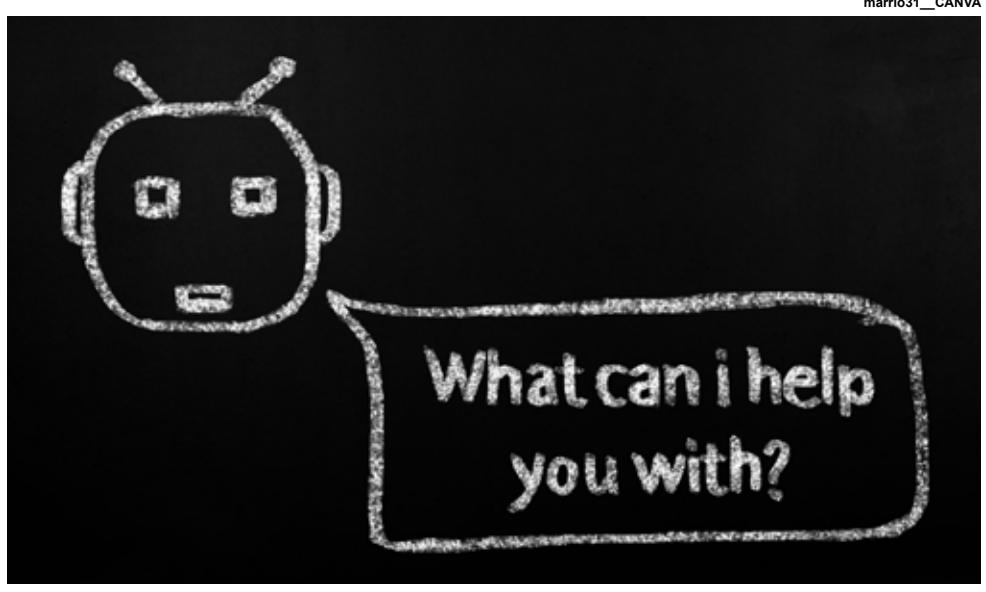
(*) CTO da Solo Iron.

ChatGPT é o 7º site mais visitado do mundo

Desde seu lançamento, em fins de 2022, o ChatGPT segue crescendo de forma meteórica.

Vivaldo José Breternitz (*)

marrio31__CANVA



De acordo com pesquisas da Similarweb, uma empresa israelense de tecnologia da informação, o site é o sétimo mais visitado de todo o mundo, recebendo cerca de quatro bilhões de visitas a cada mês.

Em primeiro lugar entre os sites mais visitados está o Google, seguido por YouTube, Facebook, Instagram, X e WhatsApp. Em um ano, o número de visitas ao ChatGPT cresceu 137%. De todo o tráfego gerado na internet, 1,86% é direcionado para o site.

Esse crescimento levou os pesquisadores a fazer observações mais aprofundadas sobre o ChatGPT. Por exemplo, nos Estados Unidos, os principais fornecedores de notícias, como a Reuters, receberam um número limitado de visitas provenientes do ChatGPT e isso, para a Similarweb, significa que os usuários, uma vez recebidas as informações da inteligência artificial, param, confiando nas informações que receberam, sem clicar nas fontes sugeridas no final das respostas.

Essa é uma tendência preocupante se considerarmos as "alucinações" que a inteligência artificial generativa ainda enfrenta, gerando respostas erradas.

O público do ChatGPT é composto por 54,41% de homens e 45,59% de mulheres, enquanto a faixa etária mais numerosa é a de 25 a 34 anos. Os principais temas das solicitações dizem respeito a videogames e acessórios tecnológicos.

São números impressionantes, mostrando a presença cada vez maior da inteligência artificial em nossa vida diária, de vez que concorrentes como Gemini, DeepSeek e outros também vem registrando forte crescimento.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

Agentes de IA para transformar fluxos de trabalho em CRM, RH e TI

JUST_sUPER

A ServiceNow (NYSE: NOW), plataforma de IA para transformação empresarial, anunciou hoje o lançamento da plataforma Yokohama, expandindo seus agentes de IA em CRM, RH, TI e outras áreas para aprimorar fluxos de trabalho e impulsionar o impacto operacional. As novas funcionalidades incluem agentes pré-configurados, projetados para oferecer produtividade e previsibilidade desde o primeiro dia, além de ferramentas para criação, integração e gerenciamento completo do ciclo de vida dos agentes de IA.

Dado que dados alimentam a IA, a ServiceNow também anunciou a expansão do Knowledge Graph, com avanços no Common Service Data Model (CSDM), permitindo uma maior conectividade entre fontes de dados e melhorando a eficiência dos agentes de IA.

De acordo com o Gartner, até 2028, 40% dos CIOs exigirão "Agentes Guardiões" para monitorar e conter autonomamente os resultados das ações de IA destacando a necessidade de uma abordagem coordenada para a implementação de IA em larga escala. Com o Yokohama Release, a ServiceNow se posiciona como a torre de controle dos agentes de IA empresariais, eliminando desafios como fragmentação de dados, lacunas de governança e dificuldades de desempenho em tempo real.

Diferente de outras soluções de IA isoladas, os agentes de IA da ServiceNow operam em uma única plataforma integrada, garantindo conectividade em tempo real por meio do Workflow Data Fabric. Isso permite que empresas gerenciem milhares de agentes de IA em CRM, TI, RH, finanças e outras áreas, garantindo visibilidade e controle centralizados.

"Agentic AI é a nova fronteira. Líderes empresariais não estão mais apenas experimentando IA; eles estão exigindo soluções que proporcionem produtividade em escala," disse Amit Zavery, presidente, CPO e COO da ServiceNow. "Nosso framework líder de IA agentic atende a essa demanda ao oferecer previsibilidade e eficiência desde o início. Ao combinar IA agentic, data fabric e automação de fluxos de trabalho em uma única plataforma, facilitamos a integração da IA nos processos empresariais, permitindo que organizações mensurem e impulsionem resultados de negócios de forma mais rápida, inteligente e em escala."

News @TI

ricardosouza@netjen.com.br

Proteção do Microsoft 365 integrada para provedores de serviços gerenciados

@A Acronis, líder global em cibersegurança e proteção de dados, anunciou hoje o lançamento do Acronis Ultimate 365, uma solução abrangente de proteção do Microsoft 365 para provedores de serviços gerenciados (MSPs). Com o Ultimate 365, os MSPs podem gerenciar a segurança cibernética, backup e conformidade com uma plataforma nativamente integrada, multi-inquilino, para ajudar a aumentar a eficiência, reduzir a carga de trabalho dos técnicos, maximizar a lucratividade e simplificar o gerenciamento de clientes. O Acronis Ultimate 365 promete oferecer aos MSPs proteção completa do Microsoft 365, aceleração do tempo para a obtenção de receita e gerenciamento escalável e eficiente (https://www.acronis.com/en-us/blog/POSTs/introducing-acronis-ultimate-365-complete-proteção-for-microsoft-365/).

RecargaPay transforma celular em maquininha

@O RecargaPay, super app de pagamentos com mais de 10 milhões de clientes no Brasil, anuncia o lançamento da tecnologia Tap To Phone, funcionalidade que permite receber pagamentos por aproximação em celulares que possuem a tecnologia Near Field Communication (NFC). A solução, desenvolvida em parceria com a Visa, é livre de mensalidade e chega para transformar a maneira como os brasileiros realizam suas cobranças, sejam eles Pessoa Jurídica (PJ) ou Pessoa Física (PF). Chamada pelo app de Tap to Pay, a ferramenta oferece taxas competitivas e bônus no saldo das vendas, agregando mais praticidade e conveniência ao dia a dia de prestadores de serviços e donos de pequenos negócios, já que dispensa a necessidade de maquininhas para receber por cartão (@recargapay).

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.