OPINIÃO

Como prevenir falhas antes que afetem a segurança e a produtividade

Rodrigo Cabral (*)

Hoje, manter operações seguras e eficientes exige mais do que reagir quando algo falha. É preciso antecipar.

A gestão inteligente de riscos transforma incertezas em oportunidades de desempenho. Quando os riscos são identificados e tratados de forma proativa, as equipes operam com mais confiança, o foco se intensifica e os processos fluem sem interrupções. Isso fortalece tanto a segurança quanto a continuidade operacional.

O primeiro passo é identificar vulnerabilidades com base em dados e no entendimento real das atividades críticas. No ambiente industrial, por exemplo, um levantamento da CNI divulgado em 2024 revela que 86% das indústrias brasileiras já adotam pelo menos uma técnica de manufatura mais moderna, um modelo de produção focado na redução de desperdícios e no aumento da eficiência.

No entanto, o estudo também chama atenção para a dificuldade de integrar essas metodologias a tecnologias como inteligência artificial, internet das coisas e big data, ferramentas que podem ampliar significativamente a produtividade e a segurança. Pois são nesses pontos que estão os maiores potenciais de mitigação de riscos.

Essa lacuna evidencia a importância de um ecossistema tecnológico integrado. Já estão disponíveis no mercado soluções que permitem automatizar fluxos de trabalho com base em eventos em tempo real. Um alarme acionado por sensores, câmeras ou sistemas de acesso pode automaticamente gerar alertas, bloquear entradas, escalar notificações e direcionar recursos de forma imediata, sem intervenção humana e com rastreabilidade.

Em paralelo, o uso de plataformas avançadas de vídeo proporciona visibilidade situacional com maior precisão. Ao gerenciar dispositivos de vídeo corporativo, como câmeras corporais e fixas, com ferramentas avançadas de detecção, marcação de eventos e compartilhamento seguro, é possível transformar vídeo em evidência acionável, acelerando investigações e protegendo pessoas e ativos.

Além disso, a comunicação eficiente é essencial para acelerar a resposta a qualquer anomalia. Sistemas troncalizados baseados em DMR (Digital Mobile Radio), oferecem uma infraestrutura robusta de rádio digital, com cobertura ampla, canais dedicados, priorização de chamadas e integração com dados e sensores. Ao contrário de soluções legadas e analógicas, esses sistemas garantem continuidade operacional mesmo em ambientes de alta criticidade, como indústrias, logística e utilities.

E quando falamos em comando e controle, consoles de despacho compatíveis com redes DMR permitem que operadores tenham total domínio da operação, recebam e enviem alertas, realizem conferência entre setores e acionem protocolos de emergência com um clique — tudo isso com redundância, gravação e interoperabilidade com outras plataformas, como voz sobre IP e aplicativos móveis.

Esse nível de integração também é aplicável ao setor de saúde. Em emergências hospitalares, por exemplo, a combinação entre sensores, inteligência operacional e comunicação instantânea permite acionar simultaneamente equipes médicas, ambulâncias, laboratórios e centrais de regulação, com acesso a informações clínicas, localização e disponibilidade de recursos em tempo real. Isso reduz falhas, acelera decisões e melhora a assistência prestada.

Gerenciar riscos de forma inteligente exige uma mudança cultural e estrutural. Isso significa substituir decisões baseadas em percepção por decisões baseadas em dados, tanto qualitativos quanto quantitativos. Ao analisar probabilidades, impactos e padrões recorrentes, os líderes conseguem priorizar riscos com mais precisão e agir antes que algo comprometa a operação.

Quando essa estratégia é integrada na cultura da organização, os resultados são visíveis: ambientes mais colaborativos, equipes mais bem preparadas e ferramentas que trabalham de forma coordenada para manter a segurança e a produtividade. A consequência é uma cadeia de ações positivas, menos incidentes, mais eficiência, menos custos emergenciais e mais foco na inovação.

A tecnologia, quando bem aplicada, transforma dados em decisões. E a gestão de riscos deixa de ser uma reação para se tornar uma vantagem competitiva, estratégica e, principalmente, segura para todos.

(*) Executive de pré-Vendas da Motorola Solutions para Brasil & SOLA.

"Não existirão mais radiologistas" – uma previsão equivocada

Geoffrey Hinton é uma figura proeminente no campo da inteligência artificial, tendo sido laureado com o Prêmio Nobel de Física de 2024 e com o Prêmio Turing de 2018 – esse último é frequentemente chamado de "Nobel da Computação".

Vivaldo José Breternitz (*)

Elnur_CANVA

Apesar de suas qualificações, em 2016, Hinton perdeu uma grande oportunidade de ficar calado, quando disse ser óbvio que num prazo que oscilava entre cinco e dez anos, não existiriam mais radiologistas, pois ferramentas de inteligência artificial, como os algoritmos de aprendizado profundo (deep learning), superariam os humanos na tarefa de interpretar imagens médicas.

Agora, os radiologistas, cujo trabalho vai além de interpretar imagens, são profissionais em falta – segundo a Association of American Medical Colleges, em 2033 faltarão naquele país cerca de 42 mil médicos, inclusive muitos radiologistas.

Ao falar sobre o assunto, o New York Times diz que a inteligência artificial é uma importante arma dos radiologistas, permitindo-lhes atuar muito mais eficientemente, inclusive detectando doenças anos antes do que acontece quando se usa métodos convencionais.

Na Mayo Clinic, segundo o jornal, onde o número de radiologistas aumentou 55% desde quando Hinton fez sua infeliz previsão, o departamento de radiologia cresceu e passou a incluir uma equipe de 40 cientistas de inteligência artificial, pesquisadores, analistas e engenheiros que desenvolveram mais de 250 modelos de inteligência artificial para uso em radiologia, incluindo analisadores de tecidos e preditores de doenças.

A Mayo Clinic Platform, é uma iniciativa da Mayo Clinic focada em saúde digital e a distância, que visa posicionar a instituição como líder global nesses campos, usando inteligência artificial e outros dispositivos. Seu presidente, John Halamka disse que "daqui a cinco anos, será negligência médica não usar inteligência artificial".

Falando sobre sua infeliz previsão alguns anos depois, Hinton disse que se referira mais especificamente à tarefa de interpretação de imagens, e não à totalidade das responsabilidades de um radiologista.

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

Uso de apps de mensagens no trabalho acende alerta

A adoção de aplicativos de mensagens instantâneas, como WhatsApp e Telegram, transformou a comunicação no ambiente profissional, oferecendo agilidade e facilitando a interação entre equipes e com clientes. No Brasil, 95% das empresas utilizam o WhatsApp no dia a dia, de acordo com um levantamento realizado pelo International Data Corporation (IDC). No entanto, a conveniência dessas plataformas acompanha riscos relacionados à proteção de dados, que demandam atenção e gerenciamento por parte das organizações para prevenir exposição de informações e incidentes cibernéticos.

Para Rodrigo Rocha, gerente de arquitetura de soluções da CG One, empresa de tecnologia focada em segurança da informação, proteção de redes e gerenciamento integrado de riscos, o uso desses aplicativos no ambiente corporativo traz muitas vantagens, mas também oferece perigos. "Assim como no uso pessoal, essas ferramentas são porta de entrada para tentativas de golpe, e a divulgação indevida de dados confidenciais, de forma intencional ou não, é uma preocupação central para as organizações", afirma.

Apesar de contarem com a criptografia de ponta a ponta, recurso padrão em muitas dessas plataformas, a proteção em aplicativos de mensagens instantâneas é limitada. Isso porque essa tecnologia protege o conteúdo das mensagens contra interceptação por terceiros durante a transmissão, mas não impede o envio ou recebimento de links maliciosos, arquivos infectados ou o compartilhamento indevido de dados por parte dos usuários.

Kaspars_Grinvalds_CANVA

"Se um link ou arquivo malicioso for enviado por meio desses aplicativos, ele chegará ao destinatário e poderá comprometer o dispositivo", analisa Rocha. O especialista acrescenta que, por isso, não se deve assumir que essas ferramentas são totalmente seguras apenas pela criptografia.

Estratégias para evitar problemas

Diante deste cenário, a simples proibição do uso desses canais pode se mostrar ineficaz ou gerar problemas operacionais. A alternativa recomendada envolve a implementação de uma abordagem multifacetada. "Isso inclui estabelecer políticas internas claras sobre o uso corporativo dos aplicativos de mensagens, definindo o que pode ou não ser compartilhado", explica Rocha.

Para o especialista, a conscientização e o treinamento contínuo dos colaboradores sobre práticas seguras de comunicação digital e a identificação de ameaças, como mensagens de remetentes desconhecidos ou com conteúdo suspeito, são componentes fundamentais para garantir a segurança das operações.

Paralelamente, o mercado oferece alternativas tecnológicas desenhadas para adicionar camadas extras de proteção ao uso corporativo de aplicativos de mensagens. "Hoje existem soluções que se integram ao contexto empresarial desses apps e podem monitorar as comunicações para fins de auditoria e conformidade, analisar o conteúdo em busca de informações sensíveis e até bloquear o envio de dados confidenciais, operando sem comprometer a privacidade dos funcionários", explica.

Prevenção como a chave

Investir em medidas de controle e prevenção é uma ação estratégica para as empresas. Os custos associados a uma quebra de confidencialidade de dados, que podem incluir prejuízos financeiros diretos, danos à reputação e implicações legais (como as relacionadas à LGPD), superam o investimento necessário para implementar defesas adequadas.

"Se ferramentas de comunicação tipo WhatsApp forem usadas como uma ferramenta oficial de comunicação, é muito importante as empresas implementarem soluções de monitoramento e bloqueio de vazamento de dados. As consequências de uma ocorrência desse tipo são muito mais custosas do que investir na prevenção," conclui Rocha.

News @TI

ricardosouza@netjen.com.br

50 vagas em São Paulo com foco em cibersegurança e inovação digital

@A Redbelt Security, consultoria brasileira especializada em segurança da informação, está com 50 novas vagas abertas para profissionais de tecnologia em São Paulo, distribuídas entre os níveis júnior, pleno e sênior. As oportunidades contemplam diferentes modalidades de trabalho (presencial, híbrido e remoto) e abrangem áreas estratégicas como vendas, marketing e centro de operações de segurança (SOC). A consultoria destaca que grande parte das vagas é destinada a profissionais de Blue e Red Team, duas especialidades em alta demanda no mercado de cibersegurança atual. Blue Team são equipes responsáveis pela defesa e monitoramento contínuo de sistemas, detectando e respondendo a ameaças em tempo real. Já os integrantes do Red Team atuam como "hackers éticos", simulando ataques reais para identificar vulnerabilidades antes que sejam exploradas por criminosos (https://redbeltsecurity.gupy.io/).

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.