Inteligência Artificial Generativa: Crescimento Explosivo e Desafios de Se

Data: 2025-09-19 05:16:00

Autor: Inteligência Against Invaders

Redazione RHC:**19 Setembro 2025 07:14**

Por Umberto Pirovano, Gerente Sênior de Soluções Técnicas da Palo Alto Networks

A Inteligência Artificial Generativa (GenAI) está redefinindo a tecnologia e o cenário de negócios em um ritmo surpreendente. De acordo com o relatório da Palo Alto Networks “The State of Generative AI in 2025”, espera-se que o tráfego GenAI aumente mais de 890% em 2024. Esse crescimento explosivo pode ser atribuído ao amadurecimento dos modelos de IA, ao aumento da automação dos negócios e ao aumento da implantação, impulsionado por retornos de produtividade cada vez mais evidentes. O aumento da adoção e do uso marca uma mudança definitiva: o GenAI não é mais uma novidade, mas uma utilidade essencial.

De acordo com Pesquisa do Observatório de Inteligência Artificial da Universidade Politécnica de Milão, em 2024, a GenAI impulsionou o mercado de inteligência artificial na Itália: 43% dos gastos com esse tipo de solução foram exclusivamente em projetos GenAI ou híbridos, que também incluíam IA tradicional.

No entanto, essa rápida expansão traz consigo desafios significativos, principalmente em relação à segurança de dados. Os incidentes de prevenção de perda de dados (DLP) relacionados à GenAI mais que dobraram: até 2025, o número médio mensal aumentou 2,5 vezes, agora respondendo por 14% de todos os incidentes de dados. Os aplicativos GenAI amplificam um vetor crescente de perda de informações, pois o uso não autorizado ou descuidado pode levar a vazamentos de propriedade intelectual, problemas de conformidade regulatória e violações.

As empresas detectaram uma média de 66 aplicativos GenAI em uso, 10% dos quais foram classificados como de alto risco. O uso generalizado de ferramentas não autorizadas, a falta de políticas claras de IA e a pressão para adotar rapidamente essa tecnologia – sem controles de segurança adequados – podem expor as empresas a riscos significativos.

A maioria das transações GenAI (83,8%) vem de quatro casos de uso principais: assistentes de redação, agentes de conversação, pesquisa corporativa e plataformas de desenvolvedor. Essas ferramentas são populares entre os funcionários porque executam diretamente tarefas diárias e repetitivas. Os assistentes de redação, por exemplo, apoiam os usuários nas várias etapas da escrita, desde a redação de e-mails até a geração de postagens e a criação de relatórios. Os agentes de conversação, por outro lado, oferecem respostas instantâneas e em linguagem natural a uma ampla gama de perguntas, tornando-os úteis para atendimento ao cliente, aprendizado e produtividade.

É claro que as tecnologias GenAI já estão tendo um impacto positivo em várias áreas, conforme destacado no relatório do Gartner "*Informe sua estratégia de IA generativa com exemplos de casos de provedores de saúde*No setor de saúde, por exemplo, documentação clínica automatizada, suporte à decisão clínica e caminhos personalizados de atendimento ao paciente estão entre as áreas que podem ser citadas.

Mesmo na Itália, setores cruciais como petróleo e gás estão experimentando um impacto significativo. Os setores de gás, serviços financeiros, seguros e saúde, que gerenciam e armazenam dados e informações altamente confidenciais, estão integrando o GenAI em suas operações para otimizar operações, agilizar processos e aumentar a eficiência e a produtividade. No entanto, seu uso representa um risco inerente, dado o potencial de os usuários inserirem informações confidenciais, expondo-as a roubo ou exfiltração. De fato, apesar de ter aplicativos controlados e protegidos por sua empresa, nem todos os funcionários os utilizam, confiando em aplicativos de terceiros, talvez percebidos como mais eficientes, convenientes ou simplesmente mais fáceis de usar.

Em virtude de seus recursos avançados de análise preditiva, a inteligência artificial também representa um pilar fundamental da prevenção. Ao processar dados históricos e informações em tempo real, os sistemas de IA são capazes de prever e sinalizar possíveis problemas antes que eles possam levar a consequências negativas. Por exemplo, no contexto financeiro, isso se traduz na capacidade de detectar transações fraudulentas, mitigando perdas econômicas; na área da saúde, a IA pode ajudar a salvar vidas, prevendo os resultados dos pacientes e sugerindo medidas preventivas apropriadas.

Desafios e riscos do GenAI

A inteligência artificial é uma tecnologia emergente que está atraindo considerável interesse. No entanto, é crucial estar ciente dos possíveis desafios e complexidades que isso acarreta. Com um número crescente de empresas experimentando aplicativos GenAI de terceiros, é importante entender completamente o cenário de risco:

- **Falta de visibilidade do uso da IA:** A "IA oculta" torna difícil para as equipes de segurança monitorar e controlar como as ferramentas GenAI estão sendo usadas em toda a empresa.
- **Não autenticadoAcesso Organizado e Exposição de Dados:** Dificuldade em restringir o acesso às ferramentas GenAI por meio de contas pessoais ou detectar (e bloquear) quando os usuários carregam dados confidenciais.
- **Interações de IA inseguras:** Modelos de IA "desbloqueados" ou manipulados podem responder com links maliciosos e malware, ou permitir seu uso para fins não intencionais.
- **Proliferação de plug-ins, copilotos e agentes de IA:** Ecossistemas complexos de IA com plug-ins de navegador, agentes de IA, bots e copilotos criam uma "entrada lateral" frequentemente negligenciada, aumentando as vulnerabilidades.

Em conclusão, embora o GenAI ofereça oportunidades sem precedentes de inovação e eficiência, é imperativo que as empresas adotem uma abordagem proativa e estratégica para o gerenciamento de riscos. A conscientização, o treinamento do usuário e a implementação de políticas robustas e medidas concretas de segurança são etapas essenciais para explorar plenamente o potencial do GenAI e proteger seu ativo mais valioso: os dados.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli