How Generative AI Will Impact Supply Chain Cyber Security

Haydn Brooks, CEO, Risk Ledger

Since its introduction in late 2022, OpenAI's Large Language Model (LLM), ChatGPT, swiftly became the most popular app of all time, with the highest growing user base in history. ChatGPT and other generative AI tools are already impacting nearly every industry and profession. In some cases, adoption is an informed choice to introduce LLMs into business workflows. However, often the adoption is indirect and less controlled as suppliers (especially SaaS providers) have already integrated LLMs into their systems and services at breakneck speed, imposing the change on organisations using their software.

Generative AI is a double-edged sword. On the one hand, it will help security teams by adding its advanced data analysis power to enhance threat intelligence and analysis, early detection, incident response, smart authentication, among other activities, while also reducing the resource burdens on teams. Via APIs and plugins, these tools are already being introduced into security software such as threat intelligence tools, Security Information and Event Management (SIEM), Intrusion Detection or Vulnerability Management systems. They also allow users to remain proactive in their security efforts by adding a logical layer to protect organisations' data, for example by learning what's 'normal' in their organisation-specific environments.

On the other hand, threat actors, too, are making increased use of the power of these new tools, not least for designing and refining malware that is harder to detect as well as for enhancing their phishing techniques. Specifically, generative AI will make spoofing even harder to detect by allowing threat actors to create communications that are much more personalised, and by taking advantage of deep fakes, both in audio and visual form. To take just one example, threat actors are now able to simply identify an existing online video or audio file of a company's CEO, utilise generative AI applications to create an audio message cloning the voice of the CEO, and then use this to launch a social engineering attack against unexpecting company employees.

Generative AI applications also bear many security risks to the confidentiality, integrity and availability (CIA triad) of organisations' data. Like any other tools, generative AI and LLMs can be compromised, for example via prompt injection attacks, data poisoning, denial of service attacks, or inference attacks. But they can also pose risks to organisations based on their proclivity for 'hallucinations' and generating false information.

Last but in no way least, there is a risk of employees feeding sensitive proprietary or customer data into these tools, exposing this data to potential unauthorised access. Since AI tools often resemble black boxes, users can also not be sure how the data they input into these tools is being handled. On average, enterprise employees are entering confidential business data into ChatGPT 199 times per week, thus exposing these organisations, and their customers, to both security and privacy risks.

The majority of security professionals attribute the significant overall increase in cyber attacks since 2023 not least to the emergence and widespread adoption of generative AI, with 82% worried about how generative AI "might enable additional cyberattacks". However, despite over half (53%) of organisations acknowledging generative AI as a risk, just over a third (38%) have so far taken steps to mitigate against it.

The biggest threat to organisations emanating from generative AI, however, will come in the form of third party and wider supply chain risk. Since many business critical third party vendors and especially SaaS providers have already been integrating generative AI into their own products and services at scale, even organisations that decide not to directly adopt the new AI tools into their own workflows, are still exposed to the risk that these tools if their suppliers have done so. It is these supply chain risks that organisations will find the hardest to grapple with in the months and years to come, and which will necessitate updating existing methods for third party risk management.

This will include assessing third-parties' responsible usage of LLMs. Specifically, organisations will have to:

- Identify service providers, SaaS platforms, or future integrations that involve LLMs.
- Categorise them based on risk and importance to your organisation.
- Understand where data is shared by the third party with any AI integrations and take risk-based decisions based on defined security criteria.
- Establishing whether third parties also have an AI risk management framework in place.
- Include generative AI-related security control questions in all future risk assessments of third parties.

Find out more about the supply chain security implications and how to mitigate the risks emanating from third parties integrating generative AI applications at breakneck speed in the Risk Ledger's upcoming series of article on the subject. Sign-up to receive our newsletter to receive the articles directly to your inbox.