BDO USA

ARTICLE

September 22, 2023

AI-Powered Cyber Attacks: Understanding and Mitigating the Risks

The threat of AI-powered cyber attacks is growing explosively alongside the recent adoption of new Artificial Intelligence (AI) technology. Hackers are increasingly using AI to launch sophisticated attacks that are difficult to detect and defend against, even launching “dark” services like FraudGPT and WormGPT. It is important for organizations to understand the risks and take steps to mitigate them.

How Do AI-Powered Cyber Attacks Work?

AI-powered cyber attacks use machine learning to analyze a human or machine target and find techniques most likely to help compromise an organization. This could be generating an email based on your people’s social media profile or using small bits of information to predict the most likely vulnerabilities in a target system and launch an attack. These attacks can be highly targeted

and can bypass traditional cybersecurity solutions that are not equipped to detect them. Yesterday's advice - like paying attention to mis-spelling and poor grammar in an email that helped detect human-oriented attacks, or high amounts of bad traffic in a machine-generated scan - are techniques of the past.

One of the key risks of AI-powered cyber attacks is their ability to learn and adapt to new defenses. Traditional cybersecurity solutions often rely on known patterns and signatures to detect and block attacks. However, AI-powered attacks can learn from these defenses and find new ways to bypass them. This means that organizations must continuously monitor and adapt their defenses to stay ahead of these evolving threats.

Learn more in our recent post, 4 Cybersecurity Considerations for AI Deployment

Another risk of AI-powered cyber attacks is their potential to cause widespread damage. These attacks can target critical infrastructure, such as power grids and transportation systems, and disrupt entire economies. They can also steal sensitive data, such as financial information and intellectual property, which can have long-lasting consequences for organizations and individuals.

How to Mitigate the Risks of AI-Powered Cyber Attacks

To mitigate the risks of AI-powered cyber attacks, organizations must take a multi-faceted approach. This includes:

Implementing AI-powered cybersecurity solutions

As AI-powered cyber attacks become more sophisticated, traditional cybersecurity solutions are no longer sufficient. Organizations must implement AI-powered solutions that can detect and respond to these evolving threats. It sounds like something that two years ago would have been science fiction, however with the right technology and tuning, your defenses can learn what is likely to be "good" activity and help protect against bad actors.

Conducting regular security assessments

Organizations must conduct regular security assessments to identify vulnerabilities in their systems and networks. This includes penetration testing and vulnerability scanning to identify weaknesses that could be exploited by hackers.

Training employees on cybersecurity best practices

Employees are often the weakest link in an organization's cybersecurity defenses. User response actions like an email click, or ignoring an alert of a genuine attack thinking it false are still part of many of today's incident investigations. Organizations must provide regular training on cybersecurity best practices, such as how to identify phishing emails and how to create strong passwords. Professionals in security roles need well-organized information to make good decisions about how to respond to signs of attack in the business.

Developing an incident response plan

Organizations must develop an incident response plan that outlines the steps to be taken in the event of a cyber attack. This includes identifying key personnel, establishing communication channels, and having a plan in place to restore systems and data. The time to develop such a plan is not during the attack – it's during regular operation of the business, so if the worst happens, your business remains resilient.

Collaborating with cybersecurity experts

Finally, organizations must collaborate with cybersecurity experts to stay up to date on the latest threats and defenses. This includes attending industry conferences and working with trusted partners to develop customized cybersecurity solutions.

The AI-Enhanced Attack Age is Here, Get Started

AI-powered cyber attacks pose a significant threat to organizations of all sizes. Thoughts like “my business is too small to be a target” are no longer true. These attacks are highly targeted, can bypass traditional cybersecurity defenses, and can cause widespread damage. Organizations can mitigate the risks and stay a step ahead of cyber criminals by implementing AI-powered cybersecurity solutions, conducting regular security assessments, training employees on best practices, developing an incident response plan, and collaborating with cybersecurity experts. As cybersecurity providers, it is our responsibility to help our clients understand these risks and develop customized solutions to protect against them.