CYBERSECURITY

2023 Cybersecurity Year in Review: Notable Facts and Policies

FEBRUARY 2, 2024

Despite significant investments in cybersecurity infrastructure and new technologies, cyber threats are still rising. Several hacking incidents, such as the MOVEit, 23andMe, and MGM Resorts hacks, marked the year 2023. We also saw the launch of the Biden-Harris administration's National Cybersecurity Strategy and the National Cyber Workforce and Education Strategy (NCWES) to address current and future cyber threats. Another important development was the rise of Artificial Intelligence, which is already changing the cyber threat landscape.

Unfortunately, ransomware attacks broke new records in 2023. Among the notable victims were MGM Resorts, Caesar Entertainment, the City of Dallas, and the U.S. Marshals Service. Sixty-nine zero-day vulnerabilities were discovered in 2023 alone, the second-highest number ever recorded. LockBit, Clop, and BlackCat were the most active groups responsible for hundreds of high-profile ransomware attacks. Such groups have been using advanced hacking tools and complex methods in their attacks. According to a survey by CyberRisk Alliance Business Intelligence, 71% of the participating organizations reported that the increasing sophistication of ransomware groups is their top concern, followed by AI-powered attacks.

2023 witnessed significant advancements in AI technology. The introduction of ChatGPT and other advanced AI tools has raised speculation all around the globe about its impact on our lives. Many people have valid concerns about potential job loss due to AI. The cybersecurity industry currently suffers from a workforce shortage. AI has I has the potential to address this gap in the short term, giving the industry more time to train and hire new employees. Recent estimates show that there are around 600,000 unfilled cybersecurity jobs in the U.S. alone. This shortage can be alleviated in the short term by incorporating AI in cybersecurity. It

doesn’t mean that AI should replace human expertise. Cybersecurity professionals are essential in many organizations and will most likely continue to play a crucial role.

As a subfield of Artificial Intelligence (AI), Machine Learning (ML) has been a part of cybersecurity for a long time. We use AI to advance and facilitate various cybersecurity tasks, from vulnerability scanning to digital forensic analysis and anomaly detection. ML is an integral element in many security tools, such as IDS and IPS systems, firewalls, antimalware solutions, SIEM and EDR tools, and Identity and Access Management services. With ML, we can monitor large volumes of data packets traveling through or leaving a network and detect anomalies by generating and utilizing a baseline at a speed that is beyond human capability.

Another important application of AI is in the area of threat intelligence. It helps us to identify and share the tactics, techniques, and procedures (TTPs) of threat actors. By utilizing AI and knowledge of TTPs, we can more effectively deal with a broad range of cyber threats. This emerging technology also enhances monitoring and incident response capabilities. Nowadays, AI is deployed in various cybersecurity areas, making it an essential component of computer and network protection.

It’s a fact that AI technology can also be employed for harmful purposes. AI is not only utilized by cybersecurity professionals but also by cybercriminals. Most cyberattacks are based on social engineering, and hackers take advantage of AI to create more sophisticated schemes. They can generate audio or video content to impersonate someone else using AI. Moreover, AI can be employed to develop improved algorithms for cracking passwords. Artificial intelligence (AI) has opened new doors for us, but it also poses new threats that we need to be mindful of and ready to handle. Despite its drawbacks, AI has more advantages, and it can help us advance the technologies we use to secure our digital assets. We should embrace AI in cybersecurity and apply it to improve the detection and response mechanisms.

The Biden administration released the National Cybersecurity Strategy in March 2023. The report acknowledges the rise of AI as an emerging trend and its potential risks. The document also recognized several other threats and the administration’s game plan to address cyber risks. The strategy befittingly emphasized the importance of protecting critical infrastructure

from cyberattacks. Critical infrastructures are crucial for public welfare, and their disruption can threaten national security. Past cyberattacks targeting critical infrastructure have caused significant damage. The administration aims to ensure that the country is prepared for complex cyberattacks that could impact critical infrastructure.

The strategy represents a significant step towards reducing the risks associated with insecure applications. The administration's goal is to shift the responsibility for cybersecurity away from individuals, organizations, and local governments, and place it on vendors. Currently, vendors are generally protected from liability claims related to vulnerabilities through licensing agreements. Eliminating this legal protection would compel companies to improve the security of their products.

We have observed numerous advancements in the field of cybersecurity in 2023 that can give us an insight into what we can expect in 2024. The current trends suggest that ransomware attacks are likely to increase in 2024. Additionally, we will continue to discuss and speculate about AI and its potential impact on cybersecurity.

Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.