Add credit and caption

Europe is setting the global standard to securing

Industry 4.0 signifies an accelerated shift towards advanced capabilities, technologies, connectivity, and automation. Artificial Intelligence (AI), particularly the newest generation of AI – Generative AI – has played a significant role, if not a leading role in driving this acceleration. It has, and will continue to create new business models, and undoubtedly new industries altogether. The opportunity is real, and world-leading innovators are harnessing rapidly evolving AI tools to generate value. Gartner predicts that in under three years, Generative AI will produce 10 percent of all data – that's tens of trillions of gigabytes.

Gen AI technology and security concerns

While there is extensive discussion around the capabilities and the possibilities of Generative AI, along with its potential to revolutionise the way we work, the security risks surrounding the technology are being discussed with similar vigour. Abuse or misuse of AI is increasingly on the minds of consumers, businesses, and governments.

With the AI revolution moving at speed, it has brought forth significant challenges that CISOs must consider in their adoption plans. The emergence of AI has significantly reduced the complexity involved in carrying out malicious activities, such as gaining an understanding of complex and intricate architectures, applications, systems, and tools.

For example, activities like conducting port or application scanning to identify vulnerabilities, and then strategically planning attack chains to exploit those entry points, have been simplified. Now, attackers can simply use natural language queries to execute common attacks like phishing, XSS, or DDOS, making the need for extensive technical skills, understanding, or experience less critical than ever before to "do bad stuff".

Consequently, it's no surprise that the frequency and impact of successful ransomware attacks have nearly doubled in 2023 compared to the same period last year.

AI-Driven threats the next frontier in Cybersecurity

Meanwhile, as existing threats accelerate, we are seeing new and innovative threats such as prompt injection attacks ,being regularly introduced. As end-users are also putting business-sensitive data knowingly or unknowingly into AI-based services, it's placing additional demand on their already strapped security teams' requirements. Our friends across IT Security teams are now also required to place additional efforts into supporting, controlling, and governing the use of these services.

As usual in our industry, attackers are leading the charge, finding new ways to leverage AI technologies and capabilities, as security teams diligently work to identify, protect, detect, respond, and recover to those threats. Increasing the costs or decreasing the ROI of successful attacks for the "bad guys" – described well by Mark Simos of Microsoft – is a key mitigating factor in winning cyber defence battles. When businesses can get themselves in front of their already known, common, and low-cost but high-value attacks, they are doing themselves a favour.

Over the next decade, we will also experience a new generation of attacks not just *with*, but also *against* AI systems. Attackers will look to manipulate the tooling, mechanisms, code, and infrastructure delivering the AI work, to influence the classifiers that systems use to bias models and control outputs. As we've seen with advanced Phishing sites, adversaries will be able create malicious models that will be indistinguishable from the real or expected models, which in foreseeable scenarios can be catastrophic. Understanding the breadth and depth of various AI & ML tools being used within the business and ensuring implementation is being carried out following regulation is essential. Meanwhile, being resilient in ensuring their defence against those "unexpected" threats coming in, should be a prioritized focus for decision makers going forward.

The roads taken to secure AI

While there are many known and unknown security concerns to consider regarding the use of AI, we can see progress from innovators, businesses, and governments in their efforts to facilitate the progress of its development, at the same time gaining broader understanding of the potential risks of the capabilities.

The White House announced new investments in AI research and forthcoming public assessments and policies, and the UK Government is playing an active role in positioning itself as a leader in global AI safety regulation. However, it's the European Union that is setting the global standard to regulate artificial intelligence with its AI Act, initially proposed in 2021 and expected to be approved for legislation by end of this year, or at latest in early 2024. The AI Act will establish comprehensive regulations for artificial intelligence technologies, emphasizing transparency and fundamental rights protection in the European Union.

The EU has also established the Digital Services Act (DSA), which has gone into force November 2022, and will be governed for compliance by the start of 2024. This legislation will bring with it a separate set of rules focusing on regulating online platforms and

addressing illegal content to safeguard people from harmful online activities and content. The DSA is encouraging European organizations to prepare now to keep up with the rapid development of Generative AI.

I'm sure many of you reading this blog, will recall the investments and associated pain needed to understand and address GDPR compliance. Both the AI Act and DSA bring a significant and varying set of controls in which companies and governments are expected to comply, and there are significant financial penalties related to breaking these rules.

With the rapid change and explosive growth of AI integrations across the IT landscape, business and security leaders need to be comfortable in their understanding of these new requirements. Additionally, they will also need to ensure their executive and board leadership understands and is enabled to prioritize the expected actions their businesses need to take.

EU's bold vision for secure AI leadership

The way the EU is approaching AI will define the future world in which we live. To help build a resilient Europe for the Digital Decade, people and businesses should enjoy the benefits of AI while feeling safe and protected. The European AI Strategy aims to make the EU a world-leader for AI, to ensure AI is human-centric, sustainable, and trustworthy in the pursuit to empower citizens and businesses to unleash their potential.

Fostering excellence in AI will strengthen Europe's potential to compete globally, and the EU will achieve this by enabling the development and uptake of AI in the EU. This will make it the place where AI thrives from the lab to the market; ensuring that it works for people and remains a force for good in society, while also building strategic leadership in high-impact industry sectors.

Businesses using Generative AI will have to follow transparency requirements including disclosing that the content was generated by AI, designing the model to prevent it from generating illegal content and publishing summaries of copyrighted data used for training. This will be a momentous change for Europe, and the rest of the world will follow.