Contribution ID: **33** Type: **Lightning Talks (5 minutes)**

Why cybercrime is an evolution rather than a revolution

Wednesday, 10 April 2024 15:40 (5 minutes)

In the realm of cybersecurity, there is a pervasive belief that the threat landscape is in a perpetual state of flux, marked by constant innovation and evolution. This presentation challenges this prevailing narrative, offering a nuanced perspective that highlights the consistent characteristics inherent in cybercrime. Despite the emergence of new tactics and technologies, certain fundamental aspects of malicious activities remain remarkably stable.

By delving into the historical evolution of cyber threats, the presentation uncovers persistent motives and techniques that endure over time. It examines the foundational elements that transcend the surface-level changes. The aim is to shift the focus from the ephemeral nature of specific attack vectors to a deeper understanding of the unchanging core aspects of cybercrime and cyber-related threats more generally.

Recognizing these persistent aspects becomes paramount when considering emerging developments like Artificial Intelligence (AI). While anticipation of 'new'threats arises, a closer inspection reveals that the novelty often lies in the application rather than the underlying approach. By observing the historically evolved threat landscape, one can better anticipate its evolution, aiding in more effective preparation and response.

Within the higher education sector, the stakes are particularly high as institutions grapple with the delicate balance between open academic environments and the imperative to safeguard sensitive data. The unique challenges faced by universities and colleges stem from a confluence of factors, including the diverse and distributed nature of academic networks, the vast array of personal and research data, and the complex web of users ranging from students and faculty to administrative staff.

In addition to these challenges, the presentation recognizes the increasing prevalence of nation-state threats, especially in an increasingly complex geo-political climate. Unlike cybercriminals primarily motivated by financial gain, nation-state actors engage in cyber espionage, influence campaigns, and intellectual property theft. This dimension further complicates the cybersecurity landscape for higher education institutions, necessitating a multifaceted approach to defend against targeted attacks, without losing sight of the untargeted pervasive attacks conducted by cybercriminals.

In conclusion, the presentation encourages a balanced perspective on the cyber threat landscape—one that acknowledges the persistence of certain elements while recognizing the necessity of adapting to emerging risks, including the tactics employed by nation-state (sponsored) adversaries. For the higher education sector, where the implications of technological advancements are significant, understanding these consistent aspects becomes crucial, guiding informed decision-making and proactive defense strategies.

Primary author: VAN DER MEULEN, Nicole

Presenter: VAN DER MEULEN, Nicole

Session Classification: Lightning Talks

Track Classification: Lightning Talks