Forcepoint reveals cybersecurity predictions for 2019

Cyber experts and research teams warn of risks to critical infrastructure and national intelligence, threats to biometric identification and over-reliance on AI in cybersecurity.

Source: pixabay.com

Global cybersecurity leader Forcepoint launched its 2019 Forcepoint Cybersecurity Predictions Report, with security specialists, behavioural intelligence researchers and data scientists providing guidance on the sophisticated threats facing organisations in the months to come.

The report examines seven areas where risks will increase in 2019, with Forcepoint experts taking a deep dive into technology trends and the motivation behind cyber-attacks, so that business and government leaders and their security teams can better prepare to face the new wave of threats.

Enterprises and governments are facing a hyper-converged world where connected systems put not only critical data and intellectual property but also the physical safety at risk. The report explores these areas and concludes that when people can collaborate in a trusted manner, leveraging data creatively and freely through technology, businesses can securely innovate to create value.

“The cybersecurity industry and attackers expend efforts in a never-ending cycle of breach, react, and circumvent—a true cat-and-mouse game,” said Raffael Marty, vice president of research and intelligence, Forcepoint.

“We need to escape this game. Researching these predictions forces us to step back and see the overall forest among the millions of trees. Cybersecurity professionals and business leaders need to adapt to changes based on the risk they represent, allowing them to free the good while still stopping the bad.”

Grappling with digital transformation and trust

The 2019 Forcepoint Cybersecurity Predictions report explores the impact of businesses putting their trust in cloud providers on faith, the impact of end-user trust in securing personal data using biometrics and the potential impact of cascading of trust throughout a supply chain.

In a survey of Forcepoint customers, 94% identified security when moving to the cloud as an important issue. Fifty-eight percent are actively looking for trust-worthy providers with a strong reputation for security and 31% are limiting the amount of data placed in the cloud due to security concerns.

“One way to increase trust and gain control is through behavioural modelling of users or, more specifically, their digital identities, to understand the reasons behind their activity,” Marty continued. “Understanding how a user acts on the network and within applications can identify behavioural anomalies that help inform risk-adaptive responses.”

Areas of risk

Forcepoint predictions include areas of risk in 2019.

Highlights of this year’s report include:

- ### Driven to the Edge

  Consumers exhausted by breaches and abuse of their personal data have led organisations to introduce new privacy safeguards in the services they provide. Edge computing offers consumers more control of their data by keeping it on their smartphone or laptop. But solutions today must overcome a lack of consumer trust that data will not be leaked to the cloud if they are to succeed.

- ### A collision course to Cyber Cold War

  Espionage has always presented a way for nation-states to acquire new technology but as opportunities for legitimate access dwindle because of the increase in trade protections, people on the other side of embargoes will have real incentive to acquire it by nefarious means. How will organisations keep intellectual property out of the hands of nation-state-sponsored hackers?

- ### The Winter of AI

  If AI is about reproducing cognition, does cybersecurity AI really exist? How will attackers capitalise on a slowdown of AI funding? When we trust in algorithms and analytics to successfully pilot automobiles, provide insight into healthcare decisions and alert security professionals to potential data loss incidents, how far should that trust go? Will vendor claims around AI effectiveness hold up against the reality of sophisticated cyberattacks?

- ### A Counterfeit Reflection

  As phishing attacks persist, hacker tricks such as “SIM Swaps” undermine the effectiveness of some two-factor

authentication (2FA) methods such as text messaging. Biometrics offer additional security by using data more unique to each end-user, but newfound vulnerabilities in facial recognition software lead experts to put faith into behavioural biometrics.

Download the 2019 Forcepoint Cybersecurity Predictions Report.