Don’t Let Cybersecurity Exploits Threaten Your Customer Experience

CenturyLink Technology Hong Kong Limited

Cybersecurity today is a critical business enabler. Without the right approach to managing risks, organizations will be handicapped when it comes to delivering great customer experiences. Here is how enterprises can start tackling risks proactively if they want to secure their customers’ trust.

As the age of the customer dawns upon us, customer experience is becoming the new competitive advantage. According to McKinsey, projects that successfully optimized customer experience typically saw revenue growth of five to 10 percent.

With this in mind, more than 4 in 10 organizations in Asia Pacific which 451 researches surveyed last year cited customer experience as a top driver of their digital transformation efforts. Some of those efforts include improving customer service, developing innovative products and services, and deploying new digital engagement technologies.

In light of offering good user experiences, enterprises need to ensure that they manage cybersecurity risks well. One security breach might be enough to negatively impact customer satisfaction or worse, lose customer trust. Just last week, a Singapore Airlines’ customer blamed the airline’s weak security system for the loss of her frequent flyer miles, and said that she might switch her airline loyalty program after the incident. Similarly, the recent cyberattack that caused the personal data of 380,000 Hong Kong Broadband Network customers to be leaked could have cost the telco customer loyalty since a study revealed that 70 percent of consumers would stop doing business with an enterprise that fall victim to data breaches.

The Constantly Evolving Threat Landscape in Asia Pacific

As countries increasingly upgrade their communication infrastructure to better cater to the constant connectivity demanded by consumers, the move also opens more doors to cyber threats. Our 2018 Threat Report found that countries with strong communication infrastructure unknowingly supplied bandwidth for Internet of Things (IoT) distributed denial-of-service (DDoS) attacks. Interestingly, those countries were also the largest victims, based on attack command volume. For instance, China not only hosted the second highest number of botnets globally – with 454,000 botnets hosted daily on average – but was also the second most hit by DDoS across the world in 2017.

What this suggests is that as cities progress to become smart cities, which leverages connected IoT devices such as sensors, smart phones, smart equipment and smart applications to serve citizens, they are inadvertently putting themselves in a vulnerable position. Take electricity providers for example. As they digitize their power grids to improve reliability, availability and efficiency of the grid, they are also increasing their chances of being attacked by malware such as Stuxnet if they do not have strong defenses in place. Likewise, as the healthcare sector embraces connected devices such as drug administration devices and remote monitoring devices to deliver better patient care, those smart devices could put patient data and physical safety at risk if they are hacked.

To prevent such incidents, some governments such as Singapore have created cybersecurity laws that require companies – especially those offering essential services such as healthcare, banking and energy – to strengthen their cybersecurity posture and share cybersecurity information to help others prevent cyberattacks more effectively.

As technology advances, malware becomes increasingly sophisticated, common and resilient too. By taking advantage of insecure IoT devices, both Gafgyt and Mirai malware allow cybercriminals to execute a variety of attacks. Our CenturyLink Threat Research Labs also reported that there were 562 unique Gagfyt command and control servers (C2s) and 339 Mirai C2s last year, with the longest uptime being 117 days and 83 days respectively.

Despite efforts to grow the cybersecurity industry, there is still a lack of cybersecurity talents. 6 in 10 organizations in the Asia Pacific stated that they did not have enough cybersecurity employees last year, and nearly half of them attributed it to the shortage of qualified personnel. This growing cybersecurity skills gap should be a cause for concern as it impedes an organization’s ability to detect and quickly respond to cyberattacks, putting them in a vulnerable position.

Security As an Enabler of Customer Experience

Given the state of cybersecurity today, organizations need to take a proactive and holistic security approach in protecting their company to avoid becoming victims of cyberattacks. Furthermore, with the growing emphasis on customer experience for business success, cybersecurity has evolved beyond “just an IT” function to be a critical component of seamless services for customer satisfaction.

Enterprises Can Do Their Part by:

Seeking threat intelligence to fight against cyber threats. Given the sheer volume and variety of threat types, it can be easy to lose sight of the most dangerous threats. Threat intelligence can help by proactively monitoring network traffic and automatically correlating it against known malicious communication before analyzing the threat data and prioritizing it. Armed with this information, organizations can quickly take the necessary steps to defend themselves from these threats.

Adopting a defense-in-depth security approach. Since most – if not all – technologies have inherent weaknesses, companies need to have multiple layers of defense to reduce the likelihood of being compromised. For instance, organizations should deploy network-based security solutions to strengthen the protection provided by traditional point security solutions. The former can help detect a threat and provide the necessary defenses (be it rerouting malicious traffic or filtering spam, etc.) before it reaches the organization's systems and users.

Plugging the Talent Gap with Managed Security Services

Coupling the rise of both known and unknown threats with the shortage of cybersecurity talents in the market, it can be challenging for IT teams to maintain a proactive security posture. By using a managed security services provider (MSSP) to manage and monitor security services, organizations can improve the synchronization of their security policies across applications and workloads for greater protection. A leading premium schools organization based in Hong Kong, for instance, leveraged CenturyLink's managed security services to cope with the increased cybersecurity threats, in the wake of data breaches. The move enabled it to gain visibility into its security posture and ensured that proper security policies and procedures are enforced across all the systems in the school.

As workers become increasingly mobile, they may be at higher risk of being hacked by vulnerable things that are beyond the company's control such as unsecured public Wi-Fi. To make matters worse, cyberattacks are increasing in sophistication and frequency and companies are facing a talent gap in cybersecurity expertise. But this does not mean that all hope is lost for cybersecurity. Enterprises can still reap the benefits of digital transformation without compromising security by taking a holistic approach that is informed by actionable threat intelligence. ■