- Computer crimes

What can companies do after a cyberattack?

The Philippine Star · 19 Nov 2018 · C4 · By ANGEL REDOBLE

The possibility of an organization getting back stolen private and sensitive data after a breach is slim to none. When it comes to cybersecurity, the question everyone should be asking is not what to do after, but how to stop attacks from happening in the first place. In order to fully prevent data breaches, an organization must have the ability to be a few steps ahead of cyber criminals by going on the offensive against them, instead of waiting for an attack to happen. This means that a company must not only be able to prevent attacks from happening but also employ measures that allow it to predict and detect incoming attacks. Once detection and prediction protocols are in place, then a company can appropriately respond to an attack. All-seeing, all-knowing

Complete 24/7 detection within a company is needed when it comes to cyber security as this is crucial in picking up the telltale signs of an attack. This means that aside from monitoring their own whole hardware infrastructure and network, an organization must also observe every bit of data that comes in and out of a network. Through this, data security personnel can immediately flag any possible threats such as anomalous and malicious data and block its access to the network.

However, detection can only go so far, which is why prediction is also an essential element in any cybersecurity protocol. One main reason why attacks are steadily increasing is because there are always new malwares being created. Since they are new, these attacks could go under the radar of even the most sophisticated data detection programs. To fight these new attacks, there are various prediction practices such as Threat Hunting that organizations can utilize. This entails cybersecurity researchers to look for the newest malware even in the deep recesses of the dark web where gifted programmers are paid to make malicious software.

Another prediction practice that companies should regularly do is to test their defenses and resilience by orchestrating a simulated attack. Penetration Testing is designed to simulate real-world attack scenarios to discover and exploit security gaps before an attacker does. By analyzing security vulnerabilities from the perspective of an attacker, organizations can determine ways to mitigate and protect vital business data from future attacks.

Enhanced detection and prediction capabilities are pivotal especially at this time when the numbers of cyberattacks are at an all-time high.

In its latest Cyber Incident & Breach Trends Report, the Online Trust Alliance declared that 2017 is the worst year ever in data breaches and cyberincidents around the world. The report showed that there were 160,000 ransomware attacks last year, which is nearly double the amount of 2016's 82,000. Coordinated efforts

Since the practice of detecting, predicting, preventing, and responding to cyber-attacks occurs almost simultaneously, proper coordination is necessary to maximize its effectiveness. The best way to keep all efforts synchronized is through a Security Operations Center (SOC), which can be best described as a cyber clearinghouse run by security professionals who leverage technology to monitor an organization's entire network. This can be a team, often operating in shifts around the clock, and a facility dedicated and organized to prevent, detect, assess, and respond to cybersecurity threats and incidents and to fulfill and assess regulatory compliance to security standards.

The Security Operations Center we use at ePLDT to monitor our clients' networks is one example of this. First, we enroll a company's entire IT infrastructure, including all devices, in our SOC. From there, we can now simultaneously perform those above: constantly monitor all data coming from hardware and software, regularly perform Vulnerability Assessment and Penetration Testing, research for new threats and add them to our threat database, and once we identify and recognize that incoming data is a threat, block its access, thereby preventing a cyber-attack from happening.

While it is easy to discuss the importance of detecting, predicting, preventing, and responding to cyber-attacks, its application in enterprises is an entirely different matter and can be difficult to execute. Not many companies have core competencies in technology, specifically, cybersecurity. For most, they may not have the right people, processes, and technology to protect their digital assets from exploitation.

Instead of facing cyberattacks on its own, a company can opt to outsource its cybersecurity needs to a third-party organization that has the sophisticated combination of expertise, skills, and technology to effectively run a Security Operations Center. Doing this relieves a company of the difficulties of looking for the right skills and technology needed to face ever-evolving cyber-attacks, and allows them to focus on improving core business.

Redoble is the chief information security officer of PLDT, Smart, and ePLDT Group and chief information officer of ePLDT.