Comprehensive Cybersecurity Plan, A Must For Firms

Cyber attacks are changing with the times. Initially, personal cyber-attacks were nothing but digital vandalism, seeking for 15-minutes of fame were mainstream, but the people behind the attacks today shifted to economic reason why they are into it – for money. They target organizations, important infrastructures, and state agencies, the incidents became increasingly sophisticated, complicated and complex. Above all, damage caused by “targeted attacks” against specific targets, and similar campaigns by groups aiming for social and political claims surface. Common people are exposed every day to the digital theft of credit card information and personally identifiable information. The frequent occurrence of illegal fund transfers through weak Internet banking system security infrastructure has been recognized as issues of society as a whole.

Possession of security intelligence (knowledge of attacks) is also an important cybersecurity measure. Threat actors do not always attack the same attack but use espionage campaign methods to conduct surveillance. Therefore, the defender also needs to study new methods and formulate effective measures. In addition, because the attack method is characterized by an aggression method and there is a trap, attrition of the attacker (raising the image of the aggressor) is made or the attack of the next stage is predicted by studying the attack method.

Along with the advancement and diversification of cyberattacks, security measures are not something that should be implemented at a single point, but it is necessary to take measures from different points of view in multiple places. For this reason, security measures to be implemented by customers should also be diversified. There is a significant shortage of security personnel, and it is difficult for many customers to implement such various security measures with their own personnel, and expect external experts for full roll-out and enforcement.

Properties of effective security measures:

Advance measures

It provides vulnerability information management services to visualize and deal with risks within the organization, such as unhandled vulnerabilities.

Security monitoring

Conventional security monitoring services are personal, making it difficult to provide accurate services to many customers.

Subsequent measures

Incident response service is provided as a response when a security incident occurs. A typical incident response service rushes to a customer and investigates, but this takes time.

Security SaaS

Look for a vendor that provides various security functions such as email security, file encryption, Web Application Firewall, etc. on the cloud to reduce customer management tasks.

Consulting and exercises

It is important to systematically strengthen security measures, and measures from a management perspective are also required.

Various vendors are also planning and developing secure solutions that incorporate the cybersecurity products and services introduced here into various solutions. As an example, we have started offering secure mobile work solutions. In recent years, cyber attacks have become more diverse and sophisticated in attack methods, and their number has also increased. For this reason, conventional security specialists are reaching their limits in terms of both quality and quantity, and efforts to strengthen cybersecurity by using AI technology are becoming active.

Cyber attacks that are becoming increasingly sophisticated and sophisticated have the problem that even today’s security technology is difficult to detect. Therefore, the industry needs to establish a technology that can detect unknown attacks by constantly analyzing the detailed system operation status, and developed a countermeasure service. Furthermore, when a cyber attack is detected, security experts use their deep knowledge and experience to infer the full scope of the attack from traces of fragmented cyber attacks, elucidate attack techniques, identify the scope of the damage, and take appropriate action. Formula your cybersecurity technology that utilizes the AI technology that is currently put into practical use can find out how to respond to a specific cyber attack from the vast knowledge of accumulated past attacks, but security experts such as those mentioned above Can not take on advanced tasks.

Source: https://www.thethreatreport.com/comprehensive-cybersecurity-plan-for-firms

PADAYONPAF PERFORM REFORM TRANSFORM : "GUARDIANS OF OUR PRECIOUS SKIES, BEARERS OF HOPE"