Title page

Top cybersecurity problems

Introduction

Industries face significant cybersecurity challenges in the current interconnected world. Today companies are involved in data operations online that increase the risks of cyberattacks. Facts reveal that the number of such attacked doubled from 2016 to 2017. The common cyber-related problems encountered by firms include DDoS attacks, malware, phishing scams, internal misuse and data breach. It is thus important for the firms to adopt effective strategies for mitigating the risks and securing the company's data. Practical solutions will enable firms to strengthen security settings that will eliminate potential threats.

Problems related to cybersecurity

Distributed Denial of Services (DDoS) attacks are recognized as a common threat in which hackers sends a request to a single target and computers are affected by malicious software. Memchaching is another challenge faced by firms that rely on unprotected,

Solutions for mitigating cybersecurity risks open-source object system that is capable of processing requests and gains access to sites. Malware is the traditional cyberattack that is introduced through different methods such as operating systems, software downloads and email attachments (Thales, 2016). On installation, the malware disguises by attaching to legitimate code and also spread to other systems. Unauthorized access is granted to hackers who manage to steal confidential information. This restricts the company from accessing the site until they pay the ransom. Phishing scams are also common in the digital age in which attackers target website by sending an email. By clicking on the link users set a path for the hackers that make it easy for them to access the company's data. This causes the company to lose its account details and hackers can blackmail for getting ransom (Shi, 2015). Internal misuse is due to weak controls that provide the opportunity of a data breach to employees. This can allow employees to leak secret data that can cause financial and reputational loss. It is revealed that employees who have fired steal data for taking advantage and pressurize the company for accepting their demands.

Solutions for mitigating risks

NIST helped the industry in the reduction of frauds and combating online thefts. Enhanced protection results in increased value creation for firms. The cyber strategy provides third layer protection that is competent to meet against security breaches and hacking (NIST, 2016). Security Information and Event Management (SIEM) is an effective tool for mitigating risks of cyberattacks. It works by collecting security log events across different hosts having an enterprise allowing storage of data centrally. SIEM products such as ArcSight allow analysis and reporting of the security events in a centralized manner. The central benefit involves detection of the attacks that other systems are unable to identify. They are useful in stopping attacks when they are in progress. They are more ideal for organizations operating at different scales. SIEM architecture involves SIEM software installed on the local server, hardware and virtual appliance. The data filter criteria include ports, protocols, address ranges, geographic location of connection termination points, signatures, strings, patterns, statistical measures of alert features, temporal relationships between alerts (timing), etc. The visible benefits of SIEM include; streamlining compliance, detecting incidents and improving efficiency (Scarfone, 2017).

Reporting of streamlining compliance

The organizations deploy SIEM tools for streamlining compliance reporting following a centralized logging solution. The host needs to include logged security events in reporting regular transfers of log data to the SIEM server. A single SIEM server is capable of receiving log data from the host and generates reports that address relevant information of the security incidents among hosts. Without the SIEM system, an organization is unable to have robust centralized logging capabilities creating rich, customized reports that are vital for compliance reporting (Stoneburner, Goguen, & Feringa, 2002). Generating an individual report for each host is essential for retrieving data from the host periodically and reassembling it for the generation of a report. The inbuilt support is the common feature of the SIEM that enhanced compliance efforts and useful for reporting complaints of suspicious events.

Detection of unidentified events

Another prominent advantage of the SIEM system is the detection of unidentified events. Hosts having log security breaches lack built-in incident detection capabilities. They generate audit logs after observing events and encounters difficulty in analyzing log entries for identifying the malicious activity. The hosts such as end-users can alert when any suspicious activity is noted. The network intrusion prevention system assists in correlating logs with the identified events. Although SIEM tools offer various benefits, they must not replace enterprise security controls for the detection of the attacks. Monitoring raw events related to security is not possible with the use of SIEM only. It is used for communicating enterprise security controls, firewalls and then directing them to block the malicious activity (Scarfone, 2017). The incident capabilities in the system is an effective strategy for the prevention of security breaches. SIEM system is commonly used for ingestion of the threat intelligence data, detection of the malicious activity and taking steps for its elimination (Stoneburner, Goguen, & Feringa, 2002).

Improved efficiency

The most important benefits of the SIEM system include enhanced efficiency in activities of incident handling. It is capable of saving time and resources by efficiently taking actions. The handling of the events speeds the incident containment that reduces the amount of damage that security breaches have caused. The incident handler is enabled for determination of the attack's route and rapid identification of the hosts influenced by a specific attack. It also automates mechanism for stopping attacks in progress, and that contain compromised hosts (Shi, 2015). SIEM is an ideal system for the organizations due to its capability of uniting the log data of security controls and host operating systems. The SIEM tools assess larger security log data volumes for determination of attacks, security threats and compromises.

ArcSight Enterprise Security Manager (ESM)

ArcSight is capable of enhancing cybersecurity and visualization capabilities. It allows powerful real-time correlation of security events for immediate detection of the security events, leading to timely mitigation. The common advantages of the model include its scalability and customization. Through multiple sources, it enriches event data inputs and offers the most powerful and intelligent correlation capabilities. It is capable of determining the threats immediately and taking actions on the earliest basis. It supports multi-tenancy for disturbed security environments. Implementation of out of box security correlation rules and use of cases also leads to fast deployment. ArcSight ESM is a powerful, scalable SIEM solution leading to real-time threat detection and provides compliance management platform that increases data enrichment capabilities. ArcSight helps in detection and direction of cybersecurity threats by responding to indicators of compromise. The flexibility of ArcSight makes it a more useful tool compared to the other mitigation tools. The visible use of the tool includes the ability to understand contextual information of events for making informed security-related decisions. Simplification of the operation centre process and reduced time for mitigating threats add to overall benefits for the enterprise.

Data enrichment and categorization

Collection of information from multiple sources permits ArcSight to conduct analysis, categorization and correlations for determining the level of threats. Categorization is crucial in converting logs of the original data to a universal format for using SIEM product. It is useful in determining the situations needing investigation and immediate actions for focusing on high-risk threats (Scarfone, 2017).

Real-time correlation

Correlation of events and alerts conducted by ArcSight assists in prioritizing the threats and using ESM engine for collecting real-time correlation of events, accurately escalating threats and violating internal rules. It is designed to recognize 75,000 events per second. A firewall is capable of passing hypertext transfer protocol to the external systems for protecting the system from exploitation and web server applications. IPS is capable of monitoring the deeper content of the web traffic and discovering a true event identifying the malicious connection with the subsequent matching packets. The system is also useful in blocking the buffer overflow type attacks that are configured on reporting network scans. The reliance of the organization on the IDS and IPS gain leverage in monitoring, auditing and enforcing the security procedures (Stoneburner, Goguen, & Feringa, 2002).

Conclusion

Due to increased threats of cybersecurity faced by the firms in the digital age, it is crucial to adopt adequate strategies. The companies can perform data analytics for identifying threats before the occurrence of any such event. The strategy if overcoming problems focus at creation of policies, standards, and guidelines are applicable in the present scenario and help organizations to overcome the issues of cyber threats. Multi-layered security system prevents information from third-party. Software assurance limited flaws and ability of an adversary. Through system awareness, industries can improve cybersecurity providing clear direction to the security agents. SIEM and ArcSight are two effective methods for resolving these issues and building a strong cybersecurity policy. By integrating these strategies the industry will be able to take prevention measures in anticipation.

References

NIST. (2016). *NIST Impacts: Industrial Control Systems Cybersecurity*. Retrieved 2019 from https://www.nist.gov/industry-impacts/nist-impacts-industrial-control-systems-cybersecurity

Scarfone, K. (2017). *SIEM benefits include efficient incident response, compliance*. Retrieved 2019, from https://searchsecurity.techtarget.com/feature/Three-enterprise-benefits-of-SIEM-products

Shi, B. (2015). National Cybersecurity Strategy of the U.S. and Its Constructive Implication for China. *Sociology Study,  Vol. 5, No. 11*, 825‐831.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* National Institution of Standards and Technology.

Thales. (2016). *Protecting Applications from Malware and APTs*. Retrieved 2019, from https://www.thales-esecurity.com/solutions/by-business-issue/protecting-applications-from-malware-and-apts