How to Navigate a Cyber-Attack A Case Study

Cyber-attacks on organizations have become inevitable. Security is no longer about preventing attacks; it's about preparing for them. This means spotting them and dealing with them in real time. The longer a cyber-attack goes undetected (on average 154 days), the more damage it does to the business and the more it will cost for the business to recover.

A significant shortfall in skilled security resource is reducing the down time to detection of security breaches as organizations simply don't have the bandwidth to manually trace all alerts across their security fabric, organizations are therefore adopting managed solutions to provide a single pane view in real time of all external and internal threats, allowing them to be proactive in dealing with the attack before it has time to exploit.

Today, customers can choose from a wide range of software and other security technologies, however, many organizations have realized that software alone will not bring the full level of security required. Continued investment in experienced personnel and detailed operational processes place a heavy burden on finances and time. By leveraging managed services, companies can remove these constraints whilst ensuring full visibility, allowing them to focus on tasks that are essential to their business.

The Challenge

Too much data but not enough actionable information…

A medium sized enterprise has a small IT team, with no dedicated security consultants. The company houses a number of systems which in turn generate thousands of log entries and alerts per day. The company lacks the infrastructure to transform this data into actionable information of potential cyber threats, posing the risk of multiple unidentified attacks infiltrating the network. Similarly many small to medium sized organizations are targeted by 1000 cyber-attack attempts within any 24 hour period! Without a dedicated team to focus on this, it is inevitable some threats will be missed, causing both financial and reputational damage.

Only the most obvious attacks are investigated…

With so much unmanageable data, the company can currently only investigate what is perceived as easily recognizable cyber-attacks. This however results in many false positives and does not leave room for the IT team to drill-down to find and react to REAL attacks that would result in significant business impact.

Inability to isolate the root cause of an attack…

The lack of visibility means intrusions cannot be analyzed without consolidating data from multiple point systems. In a decentralized environment, the company is required to view and understand the nature of issues and alerts on several systems, in order to confirm an attack. This is a highly ineffective means of determining the root cause of an attack, as well as determine its response. Additionally, time to remediation will also dramatically increase, leading to a greater financial loss in the event of an attack.

Lack of visibility to employee activity…

Insider threats are a bigger risk to cyber security than external hackers, with 74% of cyber incidents happening from within the company. Employees are inadvertently causing corporate data breaches and leaks daily resulting in expensive remediation efforts. Loss of credentials due to phishing theft, or even carelessness invites malware into the system when an employee clicks on a link in a spam email or unknowingly brings an infected device to work.

The Solution

The company onboarded a managed service provider enabling real time, rapid and thorough analysis of security events originating from both internal and external sources to it's network.

Managed services are designed to detect anomalies, uncover advanced threats and remove false positives. It consolidates log events and network flow data from devices, endpoints and applications distributed throughout a network.

Managed services provide a team of security analysts who monitor incoming alerts and events. These services remain continually up to date with the latest threats and vulnerabilities provided. It then it in-house expertise to normalize and correlate this data and identify security offences requiring investigation.

The Outcome

Continuous improvement

The methods that determine what is being attacked and how to stop an attack, are constantly being monitored; as the hackers evolve, managed services evolve with them, providing the client real time detection.

Increased efficiencies

To address the constant growth of IT environments, as well as the dramatic increase in the number of threats and attacks. The goals are to streamline security solutions while reducing operational costs and staffing requirements. Managed service providers consolidate this data from multiple sources, including networks, servers, databases, applications, and so forth; this enables analysts to monitor everything from everywhere, in one central location.

Identify at-risk users

Account takeover, disgruntled employees, malware actions. Streamlined incident investigations – Immediate insights into risky user behaviours, action and activity history.

Single view of vulnerabilities

Single centralized view of all vulnerabilities with their status and their context.

Prioritize by threat and impact

Analyze threat intelligence, vulnerability status and network communications to assess true vulnerability risk.

CSG TECHNOLOGIES

IT Security & Business Continuity go hand & glove. Cyber-security includes your people, information systems, processes & procedures. Antivirus, spam-filtering, firewalls and employee education are all essential elements of a robust defense against the criminals and hacker.

CSG Technologies will help you calculate your risk and design & implement an IT Security & Business Continuity Plan that will protect your business.

Developing a Business Continuity Plan includes risk assessment, incident response and a disaster recovery strategy. Using this approach, we design solutions that ease your concerns over potential threats by implementing customized solutions for data backup, downtime avoidance and exceptional network performance.