CLEARNETWORK

2019

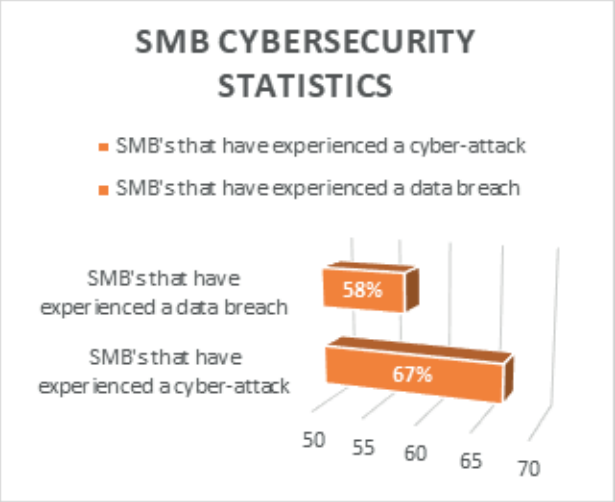
Managed Security Operations Center

Essential for SMB's

Contents

Introduction 2
Background 2
A Real-World SMB Data Breach 4
A Real-World SMB Defense 4
SMB Compliance Success with Managed SIEM and SOC 5
1. Shadow IT 6
2. Where is my Data? 6
3. Insider Threats 6
Making the Right Choice 7
Conclusion 8
ClearNetwork Managed SIEM & SOC 9
References 10

Introduction



According to the Ponemon Institute, "67% of small to medium businesses (SMB's) experienced a cyber-attack and 58% experienced a data breach within the last 12 months" - Ponemon Institute, 2018.

This study is a testament to the growing problem that SMB's face today; Cyber-threats. The catalysts for these dramatic statistics are centered around common facets that make SMB's more vulnerable and attractive targets.

Background

SMB's are under attack from cyber-actors. There are readily identifiable reasons behind these attacks that make SMB's easy-prey for malicious actors.

1. More Connections: Throughout the early years of cyber-attacks and exploitation, malicious actors focused on high-profile targets such as governments, banks, military/defense, intelligence, and other large organizations. There were several reasons for this type of focus. The first reason was due to the fact that the majority of organizations that hosted their own information technology were large entities. Small and medium businesses simply were not leveraging technology as they do today. Therefore, the crosshairs were not set on the smaller entities. In today's digital world, everyone is connected and therefore, everyone has become a target.

2. Lack of Protection: The next critical turning point, after the attackers had realized how to reach down to the small to medium businesses, was the lack of detection and protection mechanisms in-place at such organizations. For years, attackers were combatting advanced security protocols and defenses at large enterprises, governments, militaries, and other high-profile targets. The level of effort was grand and sometimes the returns were non-existent. High profile organizations had staff, tools, expertise, and the resiliency to successfully defend themselves against attacks and rebound afterwards. Also, the counteractions and attention from these attacks was a great concern to attackers. If and when an attack was mounted on a large entity, it was almost certain that law enforcement and counter-intelligence operations would train their sights on the attackers. Small to medium businesses suddenly became more attractive to these malicious groups and offered lower risk with fewer protections. SMB's were not trained on cyber-defense, did not possess the tools nor expertise to defend themselves and, more importantly, cyber-attacks could cause exponentially greater damage than at larger entities.

3. Supply Chain Crawling: Meeting with heavy resistance, attackers soon learned that it could be more advantageous and easier to attack smaller organizations down the supply chain. For example, if an attacker desired to compromise a large banking network, their efforts could be facilitated by successfully compromising a trusted affiliate or partner of that bank and leverage that trust relationship to infiltrate the larger bank. This systematic poisoning of the supply chain could prove extremely valuable to the attackers if they exercise covert techniques during the process. This soon became a reality when supply chain attacks rose 200% in 2017, according to Symantec's Annual Internet Security Threat Report.

4. The Rise of the Botnet: Attack types change with the times. Botnets are a true threat to any SMB and exist for a reason: Attackers now focus their efforts on turning SMB systems into "zombie" systems due to the lack of security protections within SMB's. These systems and networks are compromised, infected, and controlled from a central system on the attacker's side. Once the attackers have enough systems within the botnet, they send instructions to conduct attacks on other networks, companies, and targets. SMB's are frequently used in these attacks to perform lateral exploitation of higher-value targets.

Malware Availability

As of 2018, Dark Web sales of malware listed the following prices:

- **Data-Stealing Trojans ($10), Ransomware ($270)**
- **Remote Access Trojans ($490)**
- **Botnet Malware ($200)**
- **ATM Malware ($1,500)**

-Positive Technologies

5. Malware Availability: Malware used to be a fine-art for some. The acquisition of malware was not as easy of a task as it is today. Now, malware can be purchased, traded, or downloaded for free. With the rise of ransomware and business email compromise, attacks on SMB's has shifted to more automated methods that do not require much, if any human intervention. Adding fuel to the fire, in 2016, McAfee discovered four new strains of malware every second, as opposed to a one single new strain ever 12 minutes in 2005 (Slate.com). There is no surprise why antivirus is 30%-40% effective in detecting and blocking malware.

There are many more reasons that attackers are consistently growing their arsenals to attack SMB's. However, the circumstances above are directly related to the growing number of cyber-attackers geared for the small to mid-market organizations. With no sign of slowing, the time to protect our assets is greater now than ever. Managed Security Operations Centers were previously too expensive for SMB's. **In 2019, the cost options favor smaller organizations.**

A Real-World SMB Data Breach

In February 2018, a mid-sized marketing company was brought to it's knees by a cyber-attack. The company had approximately 115 employees, a firewall, antivirus, and relatively limited expertise within cybersecurity. The company did not have a SIEM solution or managed Security Operations Center (SOC) and was not adequately prepared for what they faced in the coming days.

The attackers breached the accounts of 5 employees through a phishing campaign. Once the accounts had been compromised, the attackers used the same credentials to login to the company's virtual private network (VPN). Once inside, the malicious actors implanted malware that bypassed the antivirus and set footholds within the network. The attackers remained for more than 4 months, stealing data, more credentials, account numbers, customer lists, and communications. Until one day in May 2018, the attackers turned their attention to a trusted partner of the marketing company: a large bank. A customer of the marketing company, the bank was a sizeable and a more attractive target. The attackers leveraged the email credentials and trusted relationship between the two companies to send malware to the bank. The malware bypassed the filters of the bank, did not produce any hits on signature analysis and eventually put the bank at-risk. Several sensitive emails from the bank were intercepted and phishing campaigns were continuously launched at the bank and ***nearly all customers of the marketing company.***

A Real-World SMB Defense

An IT service provider, consisting of 45 employees, was attacked in May 2017. The company had employed a 3rd party managed cybersecurity provider to monitor all systems and personnel through the use of a Security Information and Event Management (SIEM) platform. The 3rd party cybersecurity provider boasted a managed Security Operations Center (SOC) to continuously monitor, alert, and respond to security threats to the organization. The effectiveness of the solution was put to the test via an all-out assault on the IT service provider.

- Attackers began by sending phishing emails to employees. This was detected by the managed SIEM & SOC through the logs forwarded from the on-premise email server to the SIEM platform. The phishing attackers were rapidly responded to and blocked within a matter of 20-30 minutes. Any person that downloaded an attachment, clicked a link, or visited the malicious link was detected and credentials were immediately reset and the computers were placed on a watch-list.

- Attackers were scanning the firewalls and external perimeter of the company. The scans included both passive and active scans and were immediately detected. Not only were the scans detected quickly, but the response to the scans was nearly immediate. The response team identified an IP addresses scanner and blocked them from reaching the network perimeter. A rule was set within the SIEM to immediately alert on any similar scanning in the future.

This attack followed the same preliminary steps as the previous case. However, the IT service provider had chosen a proactive defensive posture and achieved a victory in this cyber-battle. What could have been a negative scenario for the IT service provider turned into an opportunity to learn about their adversaries and adapt to defend against similar attacks.

SMB Compliance Success with Managed SIEM and SOC

Organizations across the SMB space are faced with the same or similar regulations to that of their larger counterparts. Achieving compliance is no small task for smaller organizations as the resources required are, at times, greater than the risk of non-compliance. This was true until the changes in cost and functionality of managed SIEM solutions. Organizations can now keep track of their compliance from holistic and granular technical perspective with managed SIEM and SOC solutions. Regulations such as PCI-DSS, HIPAA, NIST 800-53, NIST 800-171 (DFARS), NYS-DFS (NYCRR 500), ISO 27001, and more can be seamlessly tracked and reported within the platform.

Becoming compliant and remaining compliant are two separate initiatives that require different levels of resources and methods. Many regulations require that organizations perform various continuous activities such as vulnerability scanning, log correlation and collection, behavior tracking, intrusion detection, and asset discovery. These types of activities, if sought through multiple programs, are expensive and can require significant efforts. However, remaining compliant with such regulations has been simplified by leveraging a managed SIEM and SOC. Not only can your compliance status be displayed on secure dashboards and regularly-scheduled reports, but your security posture yields financial returns as well.

When a customer or partner company asks the question: “Are you compliant with ISO-27001, DFARS, PCI, HIPAA, or another framework?” – Your answer can be a resounding YES. This is not merely a security advantage, but a business enablement tool as well! Compliant companies are awarded government contracts faster, with lesser hassle, receive payment card information with lower fees, are not fined by the regulators, and **experience less scrutiny when and if breached.**

Compliant companies can still be attacked. However, when leveraging managed SIEM and SOC, the damage is often minimized, the time to detection is shorter, and the path to recovery is clearer and streamlined. Also, when organizations that rely on managed security services do experience a cyber-attack, regulatory auditors know that the company has been performing due diligence by employing the use of a managed SIEM and SOC. The reaction from these auditors is much different than when performed on an organization that has not taken regulatory compliance seriously.

Managed SIEMs and SOCs make it easy to get compliant today and **stay compliant.** Track your compliance points and perform required due by leveraging the right tools and trusted methods. You may not have the budget or staff resources to create your own SOC or to manage a SIEM, but ClearNetwork has brought real solutions that are both effective and economical to the SMB market.

1. Shadow IT

Many organizations do not have a firm grasp on the systems that are within their organizations. This is especially true for small to mid-sized companies that have experienced rapid growth over a relatively short time period. New laptops, servers, workstations, mobile devices, and more all appear on these corporate networks. The cybersecurity health and legitimacy of these new devices can cause waves of uncertainty and risk within the organization if not properly detected and addressed. A managed SIEM and SOC can detect these new and, at times, rouge devices as they appear on your networks.

2. Where is my Data?

How do you adequately protect your critical data if the location of the data is dispersed through end-user computers, mobile devices, on-premise servers, cloud systems, and removable storage (USB) devices? This common problem has caused headaches for years. Tracking your systems and data within a managed SIEM can facilitate your protection and response efforts and lessen the time that it takes to thwart a data breach.

3. Insider Threats

Insider threats are common and attribute to nearly 45% of data breaches according to the PwC US State of Cybercrime Survey. These can be both malicious insiders with intent to damage an organization or simply employees who make critical mistakes, jeopardizing the security of their organizations. When a disgruntled employee has trusted access to sensitive data, this can be a recipe for disaster. Also, malicious attackers that have legitimate user access is equally dangerous. Monitoring malicious behavior from legitimate insiders has historically been exponentially more difficult to achieve than outsiders, until the introduction of managed SIEM and SOC. Now you can monitor the behavior of insiders (and outsiders) to detect abnormal actions. This is one of the most critical benefits of a managed SIEM and SOC service.

Insider Threat Epidemic

A recent study by PwC showed:

90% of insiders displayed no warning signs prior to their attacks and 80% of the attacks were committed during work hours on company-issued assets.

Organizations place high-trust levels into the internal IT staff members. However, only 28% of organizations were found to have visibility into their IT staff's activities. – Netwrix.

Lacking the visibility into the IT staff activities is a dangerous concoction since these employees are usually holding the highest levels of access within the company. Monitor their activities with a managed SIEM and SOC solution. In the event that an internal IT staff member becomes compromised, get alerted quickly.

Kaspersky recently showed that 52% of businesses admitted that employees are their biggest weakness in IT security. Additionally, employee carelessness contributed directly to 48% of cybersecurity incidents and 28% have lost highly sensitive customer or employee data as a result of irresponsible employees.

Our problem, in 2019 is not at the firewall layer. Our greatest threats reside within the hardened walls of our organizations.

Making the Right Choice

Small to mid-sized businesses are continuously faced with threats from cyber-actors. The rise in SMB targets has become a topic of conversation among business networks around the world. Ten years ago, cyber-attacks among SMB's were limited. In 2019, most SMB's have experienced a cyber-attack themselves or know a company that has. The threats are near all of the time and have placed the bullseye on SMB's for numerous reasons. For example:

1. SMB's are connected, all of the time and always online. Attackers can reach SMB's directly, through mobile devices, cloud applications, email, on-premise networks, and on many other digital fronts.

2. SMB's have a lack of protective mechanisms, largely due to cost misconceptions that lead to a false sense that SMB's cannot afford military-grade cybersecurity. Today, SMB's can afford a managed SIEM and SOC.

3. Facing heavy resistance from large organizations, attackers shift to trusted, yet smaller, partners. Breaching the 3rd or 4th organization from the original target is exponentially easier, offers less resistance, and greater opportunities for damage.

LANDSCAPE CHANGES

According to the Thales Data Threat Report, 67% of organizations noted cloud privileged users as a top-rated security concern. While many benefits exist for cloud IT environments, new threats and risks are also present.

Organizations with fewer than 250 employees were found to devote a smaller portion of their IT budgets to cybersecurity as opposed to their larger counterparts – Hiscox Cyber Readiness Report 2018.

4. Botnets are an epidemic. Millions of computers currently await instructions from their evil controllers. Smaller networks at SMB's play a vital role in this distributed malicious strategy. Your systems are candidates for exploitation.

5. Malware creation has exploded. Simply put, there is too much new malware created every minute for antivirus to keep up. It is impossible for antivirus vendors to research every new strain of malware and it is showing through. Additionally, malware can simply evade antivirus solutions. A cybersecurity silver bullet does not exist and is certainly not antivirus.

The costs of managed SIEM and SOC solutions have not always been within reach of small to mid-sized organizations. However, times have changed. SMB's are now a highly prized market segment for SIEM and SOC solutions and cost-effective options are available. As an SMB in 2019, you can have enterprise=class security without breaking the bank.

ClearNetwork Managed SIEM & SOC

The Managed SIEM & SOC solutions provider by ClearNetwork can rapidly elevate your security posture. By employing the Managed SIEM & SOC program by ClearNetwork, your organization can take advantage of industry leading solutions:

- Security Monitoring: Scalable security monitoring for every type of infrastructure. AWS, Azure, cloud applications, and on-premises physical and virtual environments.
- Asset Discovery & Inventory: Know what you have, all of the time. Monitor for new devices such as cloud systems, workstations, laptops, IoT, servers, network devices, mobile devices, and more. Understanding your environment is key to your cyber-success.
- Behavioral Monitoring: Monitoring for insider threats can be daunting. The Managed SIEM and SOC program from ClearNetwork helps to ensure that the human element is monitored for suspicious changes. Don't let malicious insiders or other trusted employees make mistakes or intentionally compromise your organization.
- Correlate and Log Events: Take the events from all of your devices and platforms and streamline threat intelligence to detect malicious incidents. Staying in front of such events is critical!
- Continuous Threat Intelligence: In the world of information security, your security intelligence is paramount. Attacks are changing every minute. Stay ahead of the newest threats with enterprise-grade threat intelligence.
- Vulnerability Assessment: Enable the ClearNetwork Managed SIEM & SOC service to scan your systems and devices for vulnerabilities. Ensure that you have adequate time to patch and mitigate vulnerabilities, flaws, misconfigurations, and bugs before they are exploited.
- Intrusion Detection and Alerting: With cyber-attacks lingering for more than 1-year on average, don't be late to respond. Know what is happening now so that a response can be formulated quickly to mitigate threats before they become data breaches.
- Log Management: Centralization of logs is a critical facet of any information security program. Gathering and combining logs from all sources into a single source is a best practice that expedites security discoveries.
- Compliance and Reporting: Simplification of regulatory compliance can be achieved through the use of ClearNetwork's Managed SIEM/SOC. Gathering all of the valuable security intelligence and metrics to be relayed in clear and concise reports can help you to get compliant and remain compliant.

Contact ClearNetwork regarding Security Operations Center information and SIEM benefits today

Sales: sales@clearnetwork.com
Phone: (800) 463-7920
Web: clearnetwork.com

References

https://betanews.com/2018/11/16/smb-cyber-attacks/

https://www.ponemon.org/

https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

https://www.ptsecurity.com/ww-en/

https://slate.com/technology/2017/02/why-you-cant-depend-on-antivirus-software-anymore.html

https://itsecuritycentral.teramind.co/2018/04/03/insider-threat-research-reports-and-surveys-the-top-facts/