SAIS 2017 Proceedings Southern (SAIS)

3-25-2017

Intrusion Prevention And Detection in Small to Medium-Sized Enterprises

Young B. Choi
Regent University, ychoi@regent.edu

Gregory D. Allison
Regent University, gregall@mail.regent.edu

INTRUSION PREVENTION AND DETECTION IN SMALL TO MEDIUM-SIZED ENTERPRISES

Young B. Choi
College of Arts & Sciences
Regent University
ychoi@regent.edu

Gregory D. Allison
College of Arts & Sciences
Regent University
gregall@mail.regent.edu

ABSTRACT

In this paper will examine in depth the reluctance of small to medium-sized enterprises (SMEs) to implement cybersecurity measures amidst the growing threat of cyberattacks. Small businesses encompass the vast majority of for profit and nonprofit organizations in the world. Due to the growing connectedness of the global economy through the Internet and e-business, the reluctance of SMEs to invest in security measures threatens the very existence of many organizations and their partners. The detection and defense against attacks through intrusion detection systems (IDS) and intrusion prevention systems (IPS) are two solutions that assist in detecting and deflecting potential breaches of security. An extensive look at how both IDS and IPS can provide meaningful solutions to SMEs through their visibility and control measures (including their unique characteristics, applications, and limitations) will be explored.

Keywords

Intrusion prevention systems (IPS), intrusion detection systems (IDS), small to medium-sized enterprise (SME), security

INTRODUCTION

The increased digitization of the world through the Internet and its various applications has radically altered the way in which the world functions, communicates, conducts business, and creates/consumes information. The growth of a digital ecosystem where individuals and organizations are linked together through various networks – regardless of geographic location – unleashes seemingly infinite possibilities in every sector of human life. As this digital ecosystem flourishes, mankind's growing reliance on information systems and technology hastens the march toward the digitization of nearly every aspect of life. Vast amounts of information from business communications, smartphones, social network friendships, and even home appliances are being digitized and used by various entities to personalize services, analyze trends, spark innovation, and create new products and services.

As the digitization of the global economy speeds ahead, the threat of cyberattacks against individuals, organizations, and entire nation blossoms. In light of the looming cybersecurity threat and its accompanying financial and reputational consequences, many small to medium-sized enterprises (SMEs) are reticent to invest in their security infrastructure. Williamson (2014) comments, "Despite the mounting scale and soaring costs of cyber criminality, protection and countermeasures are still not mission-critical priorities in many enterprises and organizations (p.4)." Fears of large security costs, unfounded assumptions about the unimportance of data, and a biased view of the threat that surrounding them leads many SMEs to the false conclusion that security is inconsequential to their success. Intrusion detection system (IDS) and intrusion prevention systems (IPS) are two security options that can provide one framework to protect these vulnerable organizations. They provide SMEs with the pivotal visibility and control functions that are foundational to any security infrastructure. The ability to monitor network activity for potentially harmful and abnormal events coupled with capabilities to deflect and deter a cyberattack are hallmarks of the security infrastructure provided by these systems. When SMEs recognize the need and benefits of the visibility and control measures provided by IDS and IPS, the threat and consequences of security breaches to these organizations will be minimized.

SMES: BELOW THE RADAR?

Small businesses account for the vast majority of organizations in the United States. According to the latest census data provided by the United States Small Business Administration, SMEs make up 97.7% (27.9 million in total) of all business enterprises in the United States (USSBA, 2012, p. 1). This makes SMEs a prime target for cyberattacks. Despite their overwhelming numbers, the growing web of interconnectivity and interdependency, and the expanding threat of cyberattacks, SMEs are reluctant to implement and invest in a security infrastructure.

False assumptions about the significance and value of SME information and data are rampant. The global scale of the cybersecurity issue coupled with selective reporting of high-profile targets such as government agencies and large companies has a significant effect on this perception. SMEs operate under the assumption that their data are irrelevant to cyber criminals because they do not have information such as missile defense systems or sensitive data on millions of customers. Nearly 60% of SMEs responding to a Kaspersky Research Lab survey believe that their data and information were not of interest to cyber criminals (Ashford, 2014, para. 1). Using the USSBA's data, one can assume that nearly 17 million SMEs in the United States assume they are not at risk of a cyberattack due to the nature of their business and data.

However, as global and local economies become more interconnected through e-business and e-commerce, it is not necessarily the data that cybercriminals are after. Williamson (2014) contends, "SMEs are usually suppliers, customers, or partners of larger enterprises and organizations, and the IT supply chain can function as an unwitting conduit for cyberattacks (p. 9)." The nature of SMEs' relationships with larger companies and their lax security protocols makes these small organizations ideal targets for cybercriminals. For example, the $420 million data breach suffered by Target was the result of stealing Target's network credentials from a small heating and air conditioning company hired to work in certain Target locations (Krebs, 2014). Hackers were able to get information from this small company to gain entry into Target's system and steal confidential customer data.

DIRECT TARGETS

While an indirect breach such as the Target example above may not have been directed at the small HVAC organization, trends of malware attacks are showing that SMEs are increasingly becoming direct targets. According to Symantec's 2016 Internet Threat Security Report, SMEs constitute 65% of all spear-phishing cyberattacks committed in the last year (2016, p. 44). Furthermore, businesses of 1-250 persons have seen the frequency of attacks more than double in the last five years, making up a majority of direct attacks (p.44). Simultaneously, the share of attacks directed at large companies shows a steady decline. The trend is clear; cybercriminals are targeting their attacks at smaller organizations with budgetary restraints on security spending and a culture that views security as unimportant.

Large organizations have the capacity and urgency to direct resources at security infrastructure and personnel. Furthermore, media and industry attention is typically focused on large-scale security attacks and breaches. This gives the business community and the public a biased view of the full nature of the cybersecurity threat. The Symantec Report explains, "Cybersecurity headlines focus on nation states vying for company secrets, and the tens of millions of credit card details and other personal data exposed in breaches. It's all too easy to believe that a targeted attack only happens to other companies (p. 46)." Only as more and more SMEs are directly affected by cyberattacks and the business repercussions that accompany them, will there be any significant change.

Much of the resistance to cybersecurity investment comes from SME focus on the bottom line. Kelly (2011) asserts, "The pressure on SMEs is to grow their business, and security is often low on the to-do list (p. 12)." Many SMEs direct their energies at profit maximization and frugality when it comes to spending, investment, and infrastructure expansion. As more and more SMEs are targeted directly, the cost of not investing in a security infrastructure may prove to be a fatal mistake. Security experts at Kasperky Lab assert that an average cyberattack on SMEs results in damages of $50K, and that an attack launched *directly* at an SME results in an average of $92K in damages (2013, p. 2). The Kaspersky authors also note that monetary damages averaged between $52K to $66K in additional shutdown costs and $22K in missed business opportunities (2015, p. 8). This puts the price tag for many firms well into the six-figure range, which may prove fatal for a number of organizations unable to recover.

Further complicating the problem, monetary repercussions are only one facet of the damage caused by cyberattacks and security breaches. Many harmful aspects of cyberattacks are difficult to measure in terms of a price tag; however, they are no less felt by the victims. In particular, an organization's reputation is one of the principal areas of collateral damage caused by a security breach. Cafferky (2012) comments, "Reputation is owned by society, not by the company who enjoys it. Reputation is a value that is offered on conditional loan but held in trust by society (p. 154). When security breaches result in the exposure of sensitive customer data and information, the public is likely to withdraw its support. Similarly, suppliers and other business partners may refrain from doing business with the company, particularly if transactions involve the exchange of trade secrets, financial data, or other proprietary information.

There are other areas of collateral damage that stem from cyberattacks. Mossburg (2015) encourages businesses to consider factors such as increased regulatory compliance scrutiny, insurance rate fluctuations, public relations and potential legal costs, and a lower credit rating for needed capital or investment (p. 78). These are all vital areas for the proper functioning of a business firm and they are just as likely to be negatively impacted by a cyberattack. When companies assess the risk of cybersecurity damages, they must also consider these factors into the total dollar value of potential damages. Mossburg goes on to say, “Cyber incidents are not necessarily more dangerous today because the attackers are more fierce and determined, but the capacity to do great harm is simply more achievable via our networked lives (p. 78). As business functions and processes become more interconnected both internally and externally; and, as the damage from security breaches spreads easily across these networked areas, the need for security measures to combat the growing threat must be implemented across businesses of all sizes.

INTRUSION, VISIBILITY, AND CONTROL

A fundamental view of security and the role that IDS and IPS play in making up a security infrastructure will assist SMEs in navigating their security decision-making process. Despite the use of the term “intrusion” in these particular systems, it must be noted that this term accounts for more than an outsider attempting to gain unauthorized access to a system. As many attacks are instigated from within an organization itself, it is useful to define what is actually meant by intrusion. Brown, Suckow, and Wang (2002) define intrusion as, “actions that attempt to bypass security mechanisms of computer systems. They are any set of actions that threatens the integrity, availability, or confidentiality of the information and the information system (p. 1).” Therefore, an IDS and IPS monitor network activity for a number of suspicious activities that occur both internally and externally.

At the foundational level, security is the combination of visibility and control (Holland, 2004, p. 4). The ability to both monitor network activity and act upon perceived threats is the hallmark of any good security system. As will be discussed later, IPS provide the control function of the security formula. IDS provide the visibility function that firms need to monitor their networks for irregular activity, attacks, and malware. Singh, Goyal, and Agarwal (2015) claim, “Visibility is important to decision making and makes it possible to create a security policy based on quantifiable and real-world data (p. 48).” Absent network visibility, a firm is blind to the activity taking place within its’ various information systems and is unable to take action against potential threats. As the methods of cybercriminals evolve and become more clandestine, the gap between an attack and its detection has been widening in the past several years (Nguyen, 2014, p. 18). To close this gap, firms will want to explore implementing an IDS and/or IPS to monitor and provide real-time reports of network activity.

INTRUSION DETECTION AND PREVENTION SYSTEMS

IDS are passive security systems deployed outside of the network. They are considered passive due to their inability to take action and prevent a perceived threat from entering the system. Much like a surveillance camera, they only monitor the flow of activity at many different points along the network. These systems sit outside or “not in-line” with network activity because they simply watch a network’s traffic and cannot interact with it or “cause network interruptions (Lukaszuk, 2005, p. 42).” Instead, IDS are similar to a finely tuned alarm system that employs various algorithms to analyze network data. Tuning is the act of defining the rules by which an IDS filters data based on acceptable network activity as specified by network administrators and the needs of the organization (Goodall, Lutters, and Komlodi, 2009, p. 96). If the IDS observes activity that does not fall within the pre-defined acceptable behavior, the incident is flagged or logged and the proper individual is notified.

An IDS provides incredible visibility to network activity, which SMEs will find valuable. Some firms may be surprised at the number of harmful activities taking place on their network. With the help of an IDS, a firm can uncover employee security policy violations, infections, information leakages, system and application configuration errors, and unauthorized use of certain systems (Snyder, 2009, para. 12). This network visibility enables SMEs to identify and focus directly on problem areas and begin to enforce their security policy. A security policy and acceptable use policy are useless without the ability to observe network activity and enforce consequences of improper use. While the visibility provided by an IDS is beneficial, SMEs will also need a way to take action against harmful activity.

Where IDS are passive in nature and represent the visibility portion of the security formula, IPS represent the control function and are able to take an active role in securing a network. In its simplest form, “Prevention actions are carried out before an attack occurs and are intended to limit the vulnerability to attack and to enable speedy detection and response to attacks when they do occur (Williamson, 2014, p. 13).” In this way, IPS represent a step up from IDS because they can both identify and thwart intrusions and other potentially malicious network activity. Additionally, an IPS is deployed in-line with network traffic. Rather than passively monitoring network activity from the outside like an IDS, the IPS controls traffic going directly through it. This allows the IPS to work directly within the firm’s security policy; both implementing and enforcing predetermined parameters of what traffic should be denied (Qassim, Patel, and Mohd-Zin, 2014, p. 500).

An IPS is configured in much the same way as an IDS. These systems must be tuned to meet the specific organizational and network needs of a firm. Given its ability to shut down or thwart specific network traffic or events, extra care must be taken during the tuning phase in order to avoid denying harmless or necessary network traffic. “There is always a very fine line between what a company wants to block or let through, especially for companies that rely on e-commerce to conduct day-to-day business (Lukaszuk, 2005, p. 43)." Denying valid network traffic may negatively affect a firm's bottom line, particularly if transactions are prevented from taking place.

The control capabilities provided by an IPS will enable SMEs to thwart both internal and external security threats, identify and prevent malware from entering the system, and provide real-time monitoring and enforcement of a firm's security policy. The enforcement of the firm's security policy is an added bonus for SMEs as they may lack the expertise or time to regularly analyze their network's activity. With human error making up a majority of a firm's security risks and breaches, having an automated system such as an IPS identifying and thwarting unacceptable activity is a benefit that will save time and money.

Both IDS and IPS are able to detect potentially harmful activity using two methods: misuse detection (also known as signature-based detection) and anomaly detection. Applying the misuse method, the systems survey the network for any activity that correlates with *stored* intrusion patterns and raises an alarm if activity matches up with one of these signatures (Singh, Goyal, and Agarwal, 2015, p. 48). In this way, they make use of preprogrammed or learned intrusion patterns to detect and prevent similar intrusion attempts. The anomaly-based approach identifies new or unconventional intrusions based on normal network activity and flags them as suspicious (p. 48). Using what the system considers proper network behavior as a foundation, the system will flag or stop any activity that deviates from what is considered normal.

DRAWBACKS AND LIMITATIONS OF IDS AND IPS

Farhaoui (2016) comments, "It is impossible to build a fully secure system…and difficult to develop complex software free of design errors (p. 65)." Though IDS are great tools for monitoring, logging, and alarming suspicious network activity, SMEs should also consider their limitations when deciding whether or not to invest in them. A significant variable in the effectiveness of an IDS is the human factor. Laudon and Laudon (2015) insist that information systems "are useless without skilled people to build and maintain them, and without people who can understand how to use the information in a system to achieve business objectives (p. 16)." The same can be said for security systems like IDS.

IDS and IPS are not standalone pieces of software and hardware that operate devoid of human interaction. They require significant monitoring, updating, and tuning. Additionally, they require administrators with security, technology, and business expertise. Left alone, these systems will likely find improper network behavior; however, the number of false alarms can be incredibly high. This creates a large amount of data to sift through to find the actual threat and determine the proper action to take. Instead, they are best run alongside a human expert. Sommestad and Hunstad (2013) ran an experiment that put a standalone IDS against an IDS operated in cooperation with a security administrator. They conclude that the "administrator produces significantly better filtered output than IDS systems do alone, and the administrator's filtering does not significantly impact the detection rate (p. 36)." This has serious implications for SMEs as the proper operation of the system likely requires the hiring of a security administrator. Snyder (2009) rightly asserts, "A visibility tool only brings you value if you have time to look at what it's telling you. With tight budgets and overstressed staff, the kind of senior security engineer it takes to really get value out of an IDS is in short supply (para. 19)." For companies focused on the bottom line, this may be an expense they cannot undertake.

Another issue that affects both IDS and IPS are the detection methods themselves. Both the misuse (signature) and anomaly-based detection methods have vulnerabilities that may result in an unidentified intrusion. Since misuse detection relies on prior knowledge of intrusion behavior "it lacks the ability to detect newly invented attacks. Signature databases must be constantly updated" (Patel, Qassim, and Wills 2010, p. 282). As cybercriminals consistently develop new methods to attack networks, the inability to detect new attack signatures may result in a serious breach. Conversely, the anomaly-based detection method may not rely on prior knowledge; however, this lack of knowledge of previous signatures will result in a high false positive rate (p. 282). False positives may not appear to be an issue; but in a large network with above average activity, false alarms can number in the thousands. This requires individuals to sift through each alarm and determine its validity. This waste of time and resources will negatively affect the productivity and efficacy of the system.

TOTAL COST OF OWNERSHIP

Investing, implementing, maintaining, and updating a new security system can go well into the six-figure range for certain systems. One of the major drawbacks of intrusion detection and prevention systems is their need for constant tuning, updating, and maintenance by highly skilled professionals. This may require the hiring of an expensive specialist, which may be quite difficult. These facts may lead many SMEs to abandon efforts to employ an IDS and IPS in their network. Losing the visibility and control aspects of a security framework would leave many organizations vulnerable.

Despite these drawbacks and challenges, technological advancements in next generation IDS and IPS are greatly reducing the total cost of ownership (TCO). Schultz and Butler (2014) explain that next generation security systems utilize automated tuning, impact assessment, and are able to link individual users with specific security events (p. 2). Patel, Qassim, and Wills (2010) assert, "These systems will evolve through the use of intelligent programming techniques together with knowledge-based systems and technologies that can reduce the human effort required to build these smart systems and can improve their performance (p. 288)." Automated tuning will drastically reduce the amount of human interaction needed with these systems, thus greatly reducing expenses related to human resources, maintenance, and updating. Through impact assessments, the system will be able to analyze unique events, determine the potential systems impacted, and respond without human interaction or need for approval. The ability to link specific end users to security events provides incredible visibility and allows a firm to improve the enforcement of their security policy. This decreases the amount of time spent by specialists analyzing data to find culprits of unapproved activity. It also increases efficiency, saves on costs, and provides nearly real-time enforcement of a firm's security guidelines.

CONCLUSION

Given the upward trend of the number of cyberattacks and their economic effects, the need for all business firms to invest in their network security is obvious. Security threats are increasing and cybercriminal tactics are continuously evolving. The digital arms race is taking place whether or not business owners care to take part. Contrary to the assumptions of many SMEs, cybercriminals are directly targeting their companies resulting in enormous financial consequences for their inaction. As SMEs face the increasing likelihood of cyberthreats, the need for securing their systems must be made a top business priority.

The proper securement of any system requires both visibility and control. Through a properly tuned IDS, a firm will have incredible visibility into the operations and traffic of their network. The IDS can provide actionable data through the flagging and logging of suspicious activity. It also provides deeper insight into the problem areas of their network and will assist the development and implementation of a security policy.

IPS provides the control function needed to directly interact with network activity while deflecting and deterring any potential security risk from entering the network. IPS act as the enforcement arm of a firm's security policy by taking an active role in suppressing harmful activity.

Taken together, IDS and IPS provide defense in depth. Scott (2014) explains, "Defense in depth and breadth, a strategy underpinned by a flexible orchestration platform to ensure multiple defense tools are working together in automated or semi-automated fashion, provide a practical and proven way to maximize your security capabilities and your return on security investments (p. 19)." Though security goals and needs will certainly vary from firm to firm, it must be stressed the IDS and IPS be implemented alongside other security platforms. These systems are merely part of a more holistic solution to security. Singh, Goyal, and Agarwal (2015) stress that these systems be combined with, "strong organizational policies and procedures, vulnerability assessments at regular intervals, and secure configuration of routers and firewalls (p. 47)."

The choice of whether or not to invest and implement an IDS or IPS as part of a SMEs' security infrastructure must be determined by the specific goals and needs of the firm. The visibility and control needs of a firm as well as their security budget and policies will influence this decision. Despite the limitations of these systems, technological advancements are helping to make them more effective as well as reducing the total cost of ownership. High-performance and low cost security technologies are becoming more available for use by small companies. As the total cost of ownership goes down for these systems, the cost of inaction continues to rise. IDS and IPS are two effective tools enabling SMEs to efficiently manage their network security and ensure that their systems are safe. As more SMEs implement meaningful security measures, consumer confidence will rise, investment and innovation will grow, and the threat to their survival will be diminished.

REFERENCES

1. Ashford, W. (2014). SMEs believes they are immune to cyber attack. Retrieved November 16, 2016, from http://www.computerweekly.com/news/2240216202/SMEs-believes-it-is-immune-to-cyber-attack-study-shows
2. Brown, D. J., Suckow, B., & Wange, T. (2002). A survey of intrusion detection systems. Retrieved November 12, 2016, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.408&rep=rep1&type=pdf
3. Cafferky, M. E. (2012). Management: A faith based perspective. Boston: Pearson Education. Donaldson, P. (2014). Time for Cyber War Laws?. *Armada International*, *38*(6), 48.
4. Farhaoui, Y. (2016). How to secure web servers by the intrusion prevention system (IPS)?.*International Journal Of Advanced Computer Research*, *6*(23), 65-71. doi:10.19101/IJACR.2016.623028
5. Goodall, J.R., Lutters, W.G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People*, *22*(2), 92-108.

6. Holland, T. (2004, February 23). Understanding IPS and IDS: Using IPS and IDS together for defense in depth. SANS Institute Reading Room, 1-13. Retrieved November 8, 2016.
7. [Kaspersky Lab]. (2013). *Global IT security risks survey 2013*. Moscow.
8. [Kaspersky Lab]. (2015). *Global IT security risks survey 2015*. Moscow.
9. Kelly, L. (2011). The security threats facing SMEs. *Computer Weekly*, 11-12.
10. Krebs, B. (2014, February 14). Target hackers broke in via HVAC company. Retrieved November 19, 2016, from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
11. Laudon, K. C., & Laudon, J. P. (2015). *Essentials of management information systems* (11th ed.). Upper Saddle River, NJ: Pearson Education.
12. Lukaszuk, A. (2005). Intrusion Prevention and Detection: Changing the Battle Lines. Certification Magazine, 7(1), 40-44.
13. Morgan, S. (2016, January 17). Cyber crime costs projected to reach $ trillion by 2019. Retrieved November 14, 2016, from http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#47b9c8b63bb0
14. Mossburg, E. (2015). A deeper look at the financial impact of cyber attacks. *Financial Executive*, *31*(3 & 4), 77-80.
15. Nguyen, P. (2014). Under attack: Resliency requires a high-level plan. *TM Forum Quick Insights.* TM Forum: Morristown, NJ.
16. Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, *18*(4), 277-290. doi:10.1108/09685221011079199
17. Qassim, Q., Patel, A., & Mohd-Zin, A. (2014). Strategy to Reduce False Alarms in Intrusion Detection and Prevention Systems. *International Arab Journal of Information Technology (IAJIT)*, *11*(5), 500-506.
18. Schultz, E. E., & Butler, J. M. (2014). Calculating total cost of ownership on intrusion prevention technology. *SANS Institute Reading Room.* Bethesda, MD.
19. Scott, S. (2014). Defense in depth and breadth: Securing the Internet of things. *TM Forum Quick Insights.* TM Forum: Morristown, NJ.
20. Singh, G., Goyal, S., & Agarwal, R. (2015). Intrusion Detection Using Network Monitoring Tools. *IUP Journal of Computer Sciences*, *9*(4), 46-58.
21. Snyder, J. (2009). Do you need an IDS or IPS, or both? Retrieved November 4, 2016, from http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both
22. Sommestad, T., & Hunstad, A. (2013). Intrusion detection and the role of the system administrator.*Information Management & Computer Security*, *21*(1), 30-40. doi:10.1108/09685221311314400
23. [Statistics Times]. (2016). List of countries by projected GDP. Retrieved November 13, 2016, from http://statisticstimes.com/economy/countries-by-projected-gdp.php
24. [Symantec Corporation]. (2016). Internet Security Threat Report. Retrieved November 12, 2016, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16628758&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2
25. [United States Small Business Administration]. (2012). Advocacy: The voice of small business in government. Retrieved November 15, 2016, from https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf
26. Williamson, J. (2014). Privacy & security: Locking value into the digital economy. *TM Forum Quick Insights*. TM Forum: Morristown, NJ.
27. [World Economic Forum]. (2014). *Global risks: 2014* (9th ed.). Geneva: World Economic Forum.