www.wipro.com

WIPRO
Applying Thought

COMBATING CYBER THREATS: A HOW TO FOR THE CISO.

Gopinathan. K,
Practice Head - Managed Security and Network Services,
Global Infrastructure Services (GIS), Wipro Infotech

Contents

Abstract

Digitization and the consumerization of IT have resulted in an increasingly connected world with enterprises adopting mobility to enhance collaboration, productivity and retain talent. Enterprise IT, however, is struggling to ensure the security of sensitive data in an environment where employees seek anytime, anywhere and any device access to corporate networks and applications. This is further compounded by the continually evolving threat landscape with hackers developing sophisticated tools to launch targeted attacks that the existing security tools are powerless to detect or prevent. Moreover, enterprise IT lacks complete visibility over end-user activities on unsecure mobile devices and organizations are not equipped with the necessary expertise or resources to manage end-to-end security in-house. To address these challenges and improve their response to security incidents, organizations are partnering with strategic security service providers.

This paper takes a look at the emerging security and threat landscape, the evolving role of the information security officer and the approach organizations need to adopt to overcome their security limitations.

Introduction

Today, enterprises operate under the looming threat of online attacks that can occur at any time. Successful attacks can wreak havoc with an enterprise's reputation, adversely impact business and employee productivity underscoring the need for adopting a strategic approach towards enterprise security. However, the in-house security function of enterprises often lack the requisite resources to detect and effectively respond to emerging and advanced threats forcing IT teams into reactive postures. As a result, several enterprises are outsourcing the management and implementation of their security programs to Managed Security Service Providers (MSPPs) equipped with advanced technologies, expertise, processes and tools. Enterprises can enhance security without investing heavily by partnering with MSSPs.

Cyber Crime Reaches a New High

Cyber criminals are successfully infiltrating numerous government and corporate networks and the range of attacks is expanding to include government-sponsored spying, watering hole attacks and zero day threats. Organizations are therefore finding it increasingly difficult to protect critical, proprietary and sensitive data. Going forward, the frequency and magnitude of security attacks is only set to increase. Also, the attacks will target a variety of components making their detection almost impossible. Given the advanced nature of security attacks, organizations will find it challenging to combat them effectively.

Cyber criminals invest in developing sophisticated hacking tools to exploit security vulnerabilities and have successfully developed robust tools with advanced features such as anti-forensics, easy to customize application programming interfaces (APIs), etc. Cyber criminals use advanced exploit kits that take advantage of vulnerabilities in the browsers and their plug-in features, email spams, operating systems, infrastructure and applications. Traditional security solutions such as intrusion detection systems/intrusion prevention systems, firewalls, content filtering and anti-spam products are powerless to detect these attacks.

Security Demands Are Growing

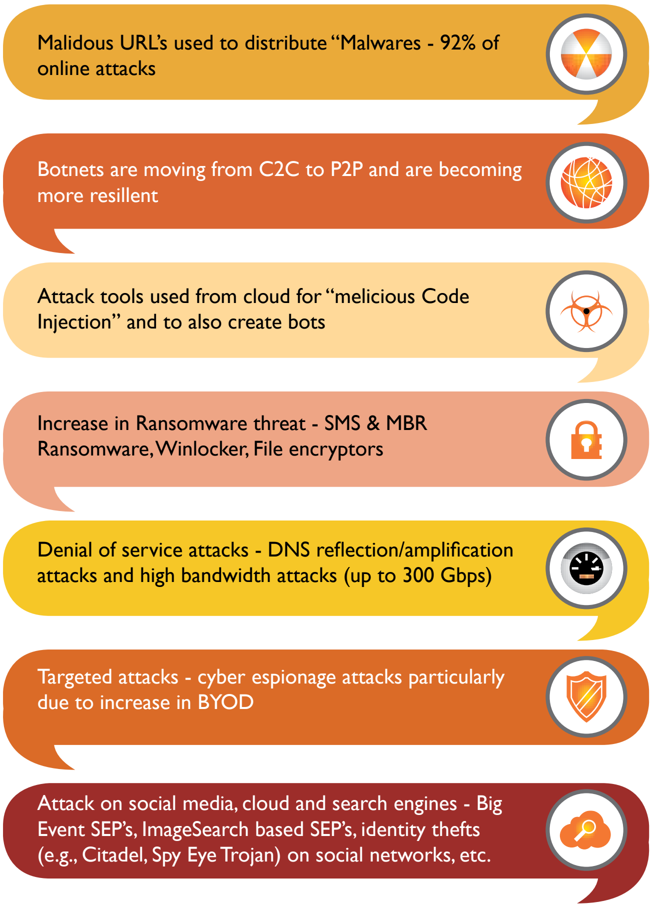
As enterprises increasingly rely on security technologies to help alleviate risks and reduce vulnerabilities, security naturally is slated to become a top priority for enterprises by 2016. Despite the global economic slowdown constraining IT budgets, global security spend is expected to increase to $86 bn in 2016 from the current level of around $70 bn.

Organizations are facing cyber security threats such as data breaches that steal user/organization data, attacks on social media that exploit the trust of the brand, mobile malware attacks, sophisticated Distributed Denial of Service attacks particularly those on targeted host, and denial of service attacks.

In most cases, security vulnerabilities are identified only after the organization has suffered the consequences of a security incident or attack with substantial impact on business. Such incidents are primarily due to improper assessment of business risk, poor security incident detection, inadequate monitoring and weak response mechanism/controls.

Cyber Threat and Risk Landscape

Malicious entities use a variety of methods to infiltrate corporate networks thereby eroding customer confidence.



Malidous URL's used to distribute "Malwares - 92% of online attacks

Botnets are moving from C2C to P2P and are becoming more resillent

Attack tools used from cloud for "melicious Code Injection" and to also create bots

Increase in Ransomware threat - SMS & MBR Ransomware, Winlocker, File encryptors

Denial of service attacks - DNS reflection/amplification attacks and high bandwidth attacks (up to 300 Gbps)

Targeted attacks - cyber espionage attacks particularly due to increase in BYOD

Attack on social media, cloud and search engines - Big Event SEP's, ImageSearch based SEP's, identity thefts (e.g., Citadel, Spy Eye Trojan) on social networks, etc.

Fig 1 depicts the different types of tools used to mount such attacks.

Enterprises Need To "Gear Up"

Enterprises need to change the way security operations are managed to handle the complex cyber threat landscape, its sophistication and the havoc it can create. They should invest to build the necessary infrastructure and hire skilled resources to proactively gain intelligence on threats, traffic behaviors and risk that cannot be detected by traditional means. They should therefore hire threat intelligence analysts to proactively detect suspicious/malicious behavior. While some entities in the government and financial sectors have integrated this function into their organizational setup, a majority of the enterprises have not taken this step.

Leveraging and seamlessly integrating existing physical and IT security systems with unified communications and flexible command and control systems is essential to enhance an organization's ability to foresee and protect itself from potential threats.

Changing Role of Today's CISO

In today's increasingly connected world, the role of the Chief Information Security Officer (CISO) has evolved into the role of a chief security officer encompassing physical and technical aspects of organizational security. Additionally, the CISO is expected to:

- Manage advanced threats
- Create security best practices
- Provide support to fix security breaches and data leakage
- Comply with security related regulatory and legal requirements

Handling these responsibilities efficiently and implementing a comprehensive security program demand specific skills and expertise that may not be available in-house. As a result, despite investing substantially in security technologies, organizations continue to face data breaches due to improper implementation of security programs.

In this scenario, CISOs should consider engaging with a service provider equipped with the expertise to provide the support that enables them to fulfill their responsibilities without compromising quality. While outsourcing will relieve the CISO from managing security systems in-house, lower total cost of ownership and capital expenditure besides providing better security expertise, the responsibility of a data breach will lie within the organization. Hence, CISOs should conduct a thorough investigation of the Managed Security Services Provider (MSSP) before entering into an agreement. CISOs should carefully examine the following criteria while selecting the MSSP:

- Market reputation of the MSSP
- Service offering
- Alliances with security technology vendors, OEMs and certification status
- Maturity level of onsite and offshore Security Operations Centers (SOCs) and their capabilities, resources, processes, tools and technologies, disaster recovery/business continuity planning
- Experience in managing security programs with similar requirements
- Depth of knowledge with regard to physical security, cloud security, governance, risk, compliance, threat intelligence, advanced threat management, setup of SOC and its processes
- Experience in consulting, system integration, professional services and support in security domain
- Domain expertise in security, network, database, application, platform, virtualization, cloud, end- user, BYOD, physical security, telecom
- Security technologies used and dashboards provided
- Experience in delivering security services in related and other industry verticals – banking and financial services, telecom, automobile, aviation, manufacturing etc
- Back-end domain expert support in case of business impact due to security breach/attack
- Executive management, practice support
- SLA commitments

An MSSP's Role in the Current Landscape

The managed security services market is expected to grow from $12 bn in 2013 to over $22.5 bn by 2017. Several industry sources have predicted that the global managed security services market will grow at over 16 percent a year through 2016 registering revenues of more than $15 bn. It is evident from this data that organizations no longer believe that they are equipped to handle the evolving needs of information security.As a result, MSSPs will play a greater role in the security landscape and offer the following benefits:

- Monitor and manage security incidents andanticipated threats, evaluate the possibility of occurrence at regular intervals and prepare organizations to mitigate advanced threats if they occur
- Provide industry experience in handling the business and technology related risk for the organization
- Provide ready-to-use and proven processes, technologies, knowledge-base and threat intelligence to help organizations reach the SOC maturity level
- Develop APIs and adaptors for unsupported device/ application security monitoring, Center of Excellence and skill development process
- Integrate physical and IT security to handle end-to-end security risk management
- Impart training and knowledge on new tools and emerging technologies in the security domain
- Provide and Maintain a pool of resources on various security technologies eliminating the hassles of talent management for organizations
- Ensure cost optimization in overall security management
- Enable dashboards and SLAs for the services outsourced
- Ensure regulatory compliance by providing the required support

Conclusion

The continual occurrence of security breaches has underlined the inadequacy of enterprise IT to protect confidential information and manage the security needs of the organization effectively. Enterprises can, however, engage with an MSSP and leverage their superior technologies, processes, tools and expertise to enhance security which is essential for protecting data as well as ensuring regulatory compliance.

Reference Links

http://ciothinktankseries.com/security/images/icxopdf.pdf
(Gopinathan K, Practice Head for managed security and Network Services, Wipro Infotech)

http://www.gartner.com/newsroom/id/2156915
http://www.securityweek.com/threat-intelligence-staffing-evolve-security-operations
http://www.infosecurity-magazine.com/view/36205/industry-predictions-for-2014-part-4-managed-security-services/
https://www.nsslabs.com/reports/enterprise-security-landscape-changing

http://www.cioandleader.com/cioleaders/news/9380/dont-fearful-losing-control-mssp
(Gopinathan K, Practice Head for managed security and Network Services, Wipro Infotech)

Author Profile

Gopinathan. K. is the Practice Head for Managed Security and Network Services, Global Infrastructure Services (GIS), Wipro Infotech. Managed Services Business is the services arm of Wipro Infotech, focusing on providing Infrastructure Management Services including End User Computing, Cloud and Data Center Services. With 12,000 plus employees, it is one of Wipro's largest divisions and contributes strongly to Wipro's leadership position in the region. Gopinathan's practice responsibilities span across India and Middle East geographies.

About GIS

Global Infrastructure Services (GIS), a unit of Wipro Limited, is an end to end IT infrastructure & outsourcing services provider to global customers across 57 countries. Its suite of Technology Infrastructure services spanning Data Center, End User Computing, Networks, Managed Services, Business Advisory and Global System Integration. Wipro, is a pioneer in Infrastructure Management services and is amongst the fastest-growing providers across the world. GIS enables customers to do business better by enabling innovation via standardization and automation, so that businesses can be more agile & scalable, so that they can find growth and succeed in their global business. Backed by our strong network of Integrated ServiceNXT™ Operation Centers and 11 owned data centres spread across US, Europe and APAC, this unit serves more than 500+ clients across with a global team of 23,800 professionals and contributes to over 30% of Wipro's IT Services revenues of Wipro Limited.

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading Information Technology, Consulting and business Process Management company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology". helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation, and an organization wide commitment to sustainability, Wipro has a workforce of over 140,000 serving clients in 175+ cities across 6 continents. For more information, please visit www.wipro.com.

WIPRO
Applying Thought

DO BUSINESS BETTER

WWW.WIPRO.COM

CONSULTING | SYSTEM INTEGRATION | BUSINESS PROCESS SERVICES

WIPRO LIMITED, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256. email : reachus@wipro.com