MAX RemoteManagement™

MAX INSIGHT

Whitepaper

How to capitalize on the complex cyber threat landscape

By Jay McCall

Table of Contents

Overview

Enterprise security threats are more challenging than ever. Cyber attackers are more sophisticated. Their attacks happen at an alarming rate with new malware variants and vulnerabilities emerging virtually every day.

Multiple research studies confirm that businesses (especially SMBs) are not prepared for the threats in this new landscape, which translates to a huge opportunity — and responsibility — for IT service providers (ITSPs).

This white paper will consider this opportunity and how Managed Service Providers (MSPs) and ITSPs can help their clients mitigate the inherent risks of doing business within this increasingly complex cyber threat landscape.

In particular it will cover:

- Understanding the human element behind cyber threats
  - Corporate leaders who unknowingly increase the risk of attack
  - Employees bringing their own devices, apps – and threats
- The top 8 threats facing customers right now:
  - Web app attacks
  - Cyber espionage
  - Point-of-sale (POS) hacks
  - Payment card skimmers
  - Insider misuse
  - Crimeware
  - Miscellaneous errors
  - Distributed denial-of-service (DDoS) attacks
- Delivering holistic Managed Security Services
  - Starting with BYOD/computer usage policies
  - Following with a multifaceted security solution

Introduction

In a 2013 PWC study, a sample of corporate CIOs and CTOs was asked a series of questions concerning cyber security within their respective businesses. The topics included: knowledge of financial loss due to cybercrime, the greatest cyber threats to their businesses, what preventative measures have been enacted, the causes of the threats or crimes, and more. More than 20 percent of respondents answered "I don't know." It became very clear to the surveyors that "organizational leaders do not know or appreciate what they are up against, and they lack a clear understanding of the nature of today's cyber threats, and those who pose these risks."[1]

As new threats pop up each day, such as Advanced Persistent threats, Denial of Service attacks, and IPv6 attacks, (not to mention malware and hacking still topping the list of security woes) it appears that companies do plan to beef up IT security. In fact CompTIA reports that 28 percent of firms view security as a significantly higher priority today as compared to two years ago, with 37 percent of firms expecting security to be a significantly higher priority two years from now.[2]

[1] Key findings from the 2013 US State of Cybercrime Survey
[2] Information Security Trends CompTIA, November 2013

Understanding the human element behind cyber threats

Many of the problems faced lie in the great divide between the level of security needed for a company's network and what's available through traditional IT security tools. These attacks are a part of life and working with antiquated technology models doesn't cut it in today's environment.

In fact, it has come to the point where there is no choice but to significantly heighten IT security and make incremental improvements to bridge the threat gap created by today's highly adept hacktivists and other cybercriminals.

CompTIA research showed that the human element has become a major piece of the IT security puzzle. Not only does human error cause the majority of security breaches but companies tend to be overwhelmed by IT security in general. Added to that is the problem caused by the very small pool of security professionals who actually have the right skills to handle today's threats. The study claims that, as companies increasingly seek IT security "cloud security, mobile security, data loss prevention, and risk analysis are four areas where skills are seen to be lacking."

So where are the sources of these threats? **The answer: cybersecurity threats occur everywhere within all businesses, from the top down.**

To get a clearer picture of the "who" behind the gaps in cybersecurity, Stratecast conducted a survey of IT employees and line of business (LoB) managers, all of which said they were either "decision-makers" or "influencers" of software purchases in their given companies.
Here's what they found[3]:

Corporate leaders unknowingly increase the risk of attack
Any of the following can threaten the security of a company's information: social collaboration, growth in mobile device use, transitioning to the cloud for data storage, digitizing sensitive information, moving to smart grid technologies, and encouraging workforce mobility. These new trends are all well and good — and vital to keep pace with the business world. However many company leaders don't consider how new technological innovations can impact their business' IT security, therefore opening up more opportunity for hackers.

Most employees bring their own devices, apps — and threats
You can bet that the majority of employees, both IT and non-IT, are currently using their personal smart phones or tablets and using non-approved applications on them (even if those apps likely help employee productivity in one way or another). Even as companies worldwide adopt bring your own device (BYOD) and bring your own application (BYOA) policies, business managers and stakeholders must be on alert.

Here's why:

- Nearly 15 percent of all employees who participated in the Stratecast study said they have experienced or perceived at least one malware infection, data loss, unauthorized, or blocked access incident.

- More than 80 percent of survey respondents admitted to using non-approved SaaS applications in their jobs.

[3] Frost & Sullivan: The Hidden Truth Behind Shadow IT —
Six Trends Impacting Your Security Posture, 2013

- Only 19 percent of line of business employees and 17 percent of IT employees refrain from using non-approved SaaS applications.

- At least 35 percent of all SaaS apps are purchased and used without permission. A large number of participants say they have experienced proven or perceived cyber-attacks — particularly with social media applications.

The top 8 threats facing your customers right now

Verizon researched 50 contributing global organizations in 95 countries for its 2014 Data Breach Investigation report. Through the research, it found 1,367 confirmed data breaches as well as 63,437 security incidences. [4]Here's the breakdown of the most frequent cyber-attacks:

1. **Web app attacks** are the most common data breach, and the report says apps are "the proverbial punching bag of the Internet." The criminals use phishing techniques, install malware, and as a result discover the passwords and credentials they need to gain unlawful access to companies' sensitive information.

2. **Cyber espionage** has tripled over the last year. Verizon stated that these incidents are caused by a larger group of "threat actions" than all other attacks. This means that intruders make themselves at home in companies' data — scanning networks, exporting data, and more. Verizon also warned China isn't the only culprit anymore. Statistics showed that more than 21 percent of reported incidents can be traced to Eastern Europe.

3. **Point-of-sale (POS) hacks** were a top headliner for 2013, too. With the high-profile Target breach whereby hackers gained access to the credit card numbers of approximately 40 million customers, it seemed like 2013 was the year of the retail hacker. Recent highly publicized breaches of several large retailers are bringing POS-related threats to the forefront once again.

4. **Payment card skimmers** mostly affect ATMs and gas pumps, requiring a skimming device added to a machine. This tactic has been around for years, but the methods have changed. Now, a thief can remotely collect data from Bluetooth or other wireless technologies.

5. **Insider misuse** includes employees "using forbidden devices or services to send intellectual property to their personal accounts — or, more deliberately, posing as another user and sending messages aimed at getting a colleague fired." Verizon reports that a high number of people committing these crimes are payment chain personnel and end users, which includes C-level executives.

6. **Crimeware** is a threat category that includes malware which is designed to steal someone's online banking credentials. These incidents occur, for example, through activities such as the unintentional downloading of a virus through a pop-up window.

7. **Miscellaneous errors** are another threat category encompassing unintentional data disclosure, such as accidentally emailing sensitive information to the wrong person or accidentally posting non-public information to a company's web server.

8. **Distributed denial-of-service (DDoS) attacks** are the biggest threats to businesses within the financial vertical, retail vertical, and public sector. Cyber criminals' motives behind shutting down organizations or customer-facing websites range from extortion to a sick sense of humor. These attacks are not new, but attackers' tools are becoming more sophisticated.

[4] Verizon 2014 Date Breach Investigations Report

Although not (yet) making the top eight list on Verizon's report, ransomware threats such as CryptoLocker have gained widespread notoriety within the past year. The CryptoLocker virus works its way onto computer networks much like any virus does – through a phishing scheme that tricks unsuspecting victims into opening an email attachment (e.g. "USPS – Missed Package Delivery"). Although the attachment may appear to have a harmless .pdf or .doc extension, behind that façade is an executable file that launches when the attachment is opened. Once activated, the program is engineered to scan computers and networks for common business file extensions such as .doc, .ppt, .xls, and .accdb, after which it encrypts the files using a 2048-bit RSA public/private asymmetric key pair, where the public key is stored in an off-site class 2 (C2) file server that the victim is unable to access. Once CryptoLocker has encrypted all detectable files, victims receive a popup message letting them know their desktop has been hijacked and unless the user pays a ransom fee within 72 hours (approximately $300, payable through BitCoins or GreenDot MoneyPaks), the private half of the encryption key will be deleted.

Those who wait for the CryptoLocker countdown to expire find a second chance offer begins – only this time the ransom is upped to nearly $10,000! A June 2014 press release on FBI.gov estimated that within the first two months since CryptoLocker emerged more than $27 million in ransom payments were made, and to date an estimated 117,000 computers have been affected in the United States alone.

Deliver holistic managed security services

In addition to the likelihood of cyber threats increasing as employees bring their own devices (and non-approved applications) to work, there's also a very good chance your customers/prospects don't really know what their employees are using their computers for during the workday. In addition to leaving businesses vulnerable to the host of threats outlined earlier, it can lead to serious bandwidth-related issues. VARs and MSPs can help clients mitigate these risks by providing comprehensive managed security services that include the following elements:

Start with BYOD/computer usage policies. Despite the growing external cyber threat landscape, the vast majority of breaches occur as a result of human error (e.g. neglecting to update antivirus software) and poor judgment (e.g. opening email attachments from unknown senders). Before discussing security technology, be sure to address your client's BYOD/computer usage policies.

Following are some important questions you should address with clients to establish/improve their computer usage policies:

- Are you considering allowing employees to use their personal devices in the workplace?
- If so, are you concerned about securing access to your network from personal devices?
- Do you currently have a corporate BYOD/computer usage policy?
- How are you securing access to the applications your employees are using to access your corporate data?
- Are you isolating/containerizing applications that access your network?
- How are you minimizing corporate liability associated with personal devices in the workplace?
- Do you currently have visibility into the websites employees are visiting and the applications they're using during work hours as well as the bandwidth they're consuming?
- How are you ensuring your BYOD/computer usage policies, including the protection of your employees' rights, are being enforced?

A good BYOD/computer usage policy should outline each party's responsibilities, too. For example, during this discussion you and your client can determine your level of support, which types (and brands) of devices will be supported, and what is expected of employees when using their personal devices at work, among other things. This will ensure you are covered if an employee uses a device on the network that is not supported by your managed security service.

Follow with a multifaceted security solution. Over the past few years the SANS Institute, a security focused cooperative research and education organization that reaches more than 165,000 security professionals around the world, worked with a consortium of U.S. and international agencies to develop what's known as the Critical Security Controls (CSC). This list of security controls focuses on prioritizing security functions that are effective against the latest advanced targeted threats, with an emphasis on providing best practices for defending against the threats. The U.S. State Department reported that, by following the top 20 controls outlined in the CSC, it was able to reduce its measured security risk by more than 94 percent. The Defence Signals Directorate (DSD) in Australia estimates that 85 percent of targeted attacks could be mitigated by implementing the top 4 security controls in the SANS Top 20 list of CSC[5].

Two of the four security controls include **patching operating systems and applications** to ensure that vulnerabilities are eliminated, making automated patch management a must-have. (The other top two security controls entail actively monitoring the network to ensure only authorized devices and authorized software are accessing and running on the network.)

Web monitoring and filtering tools also provide a goldmine of information about end users' web browsing activities, including how much time is spent on shopping sites (e.g. Amazon, eBay), how much bandwidth is being consumed on video streaming sites (e.g. YouTube, Vimeo), as well as attempts made to access blocked sites (e.g. peer-to-peer/bit torrent sites).

Implementation of **AV (antivirus) software** is also essential. Like patch management, AV software requires continuous updating. Security tools that require any involvement from customers are a recipe for failure, which is another selling point for your managed security service.

Email filtering is another critical part of a managed security service offering, reducing the number of viruses coming into your customers' work environments through hyperlinks and attachments, not to mention reducing the time-wasting junk mail that employees otherwise have to wade through.

BDR (backup and disaster recovery). Even the best defenses aren't perfect, and that's why having a reliable backup system is so important, allowing IT service providers to quickly recover customers' data to a pre-computer virus state. As is the case with every other component of the managed security solution, using an automated system that can be remotely monitored and offers the ability to perform remote data recovery is highly important.

Security event log checking. Also known as the proverbial canary in the coal mine, checking security event logs allows IT service providers to detect suspicious anomalies, such as an application not having the correct security clearance to perform a specific action, resulting in multiple failed attempts. Performing routine system, application, and security event checks adds another invaluable layer of protection that's also useful for detecting and remediating outside hacking attempts.

Although becoming a managed security services provider may initially appear to be an exercise in futility, studies suggest a much brighter outlook. Managed security service providers that help their clients implement the right IT security strategy — which includes computer usage policies and promoting awareness of the threat environment, combined with a holistic security solution can help customers stave off 95 percent of cyber threats. And, with a good BDR system in place, your customers' data will still remain safe on the off chance a virus makes its way onto their network. Being able to offer this kind of business insurance to customers should give aspiring managed security service providers enough assurance to be more assertive about engaging customers and prospects about their security needs.

[5] CSIS: Raising the Bar for Cybersecurity, February 2013

Summary

Throughout this white paper we have consider not only the different types of threat which make up this complex cyber threat landscape, but also how MSPs and ITSPs can help protect their clients from the risks such threats can pose.

By offering a managed security services solution including web monitoring, AV Software and mail filtering services, among others; you can ensure your customers systems are being monitored and protected. Minimizing the possibility of a security breach, avoiding data loss and mitigating the impact on business should a problem occur.

MAX RemoteManagement

MAX RemoteManagement now includes an advanced Web Protection feature based on award-winning GFI Web Monitoring solution, allowing MSPs to protect customers' networks from web-based threats by limiting access to malicious websites, enforcing corporate browsing policies and monitoring bandwidth.

By combining this new feature with MAX RemoteManagement's managed antivirus and patch management capabilities, MSPs now have the ability to offer clients complete network protection, saving time and money on remedial support costs by addressing threats before they become issues.

The Web Protection features can also help you to increase your clients' productivity and improve network performance by setting common-sense web browsing policies and optimizing bandwidth usage.

MAX RemoteManagement's Web Protection features include:

- **Web Security** – Stop clients' end-users from accidentally visiting malicious websites that host malware, proxies, spyware, adware, botnets and spam, as well as websites designed to perform phishing attacks.
- **Web Filtering** – Clients can ensure that employees are staying productive while at their desks by enforcing web browsing policies designed specifically for the workplace through the use of whitelists and blacklists that complement category based filters. Web filtering policies also allow customers to protect themselves from legal liability and reduce the risk of a security breach through proactive Internet access controls.
- **Bandwidth Monitoring** – Be automatically alerted when there is excessive bandwidth activity on a client's network so that you can identify the cause and address the situation before it disrupts business operations. Internet activity can also be filtered by day, category and URL to reveal trends, spikes and irregularities that may be affecting productivity.

About MAXfocus

MAXfocus is the platform of choice for the largest community of future-focussed MSPs and IT support companies in the world. The MAXfocus platform empowers MSPs and IT support companies to deliver world-class IT Operations and IT Service management to their customers with a customisable set of services that has the lowest total cost of ownership in the industry. MAXfocus sits at the heart of a global community of more than 10,000 of the world's leading MSPs and an extensive network of partners and industry leaders and delivers the commitment and investment to enable MSPs to evolve their service offerings as strategic, consultative services to their clients.

Learn more about MAXfocus, our products and how you can deliver a highly effective Web Protection service to your clients using our solution portfolio by visiting www.maxfocus.com/remote-management/app-control

USA, Canada, Central and South America

4309 Emperor Blvd, Suite 400, Durham, NC 27703. USA

Europe and United Kingdom

Vision Building, Greenmarket, Dundee, DD1 4QB, UK

Australia and New Zealand

2/148 Greenhill Road, Parkside, SA 5063

www.maxfocus.com/contact

WP0013-v1.0-EN

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. LogicNow is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, LogicNow makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. LogicNow makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

We are Max

MAXfocus™
From LogicNow