Malwarebytes

WHITEPAPER

The business case for layered security

Project description

A project to roll out layered security is relatively simple. Endpoint security can be deployed centrally and work in conjunction with existing anti-virus, intrusion detection and firewall systems.

University College London (UCL) has found layered security from Malwarebytes is easy to distribute and manage. Software updates can be pushed to all systems at once and scans can be performed automatically. And once installed, Malwarebytes can be almost completely hands-free says Richard Whittaker, UCL head of desktop support.

Michael Kraft, IT security engineer at agricultural equipment provider Vermeer, says: “I have the Malwarebytes Management Console up on my screen all day and it just runs.”

The console allows central administration of software on clients while assessing the overall security of the company’s endpoints, all from one screen, he says.

The big picture

Four per cent of revenue is a lot to sacrifice, particularly in the current economic climate. Yet this is the fine proposed in the EU General Data Protection Regulation for companies failing to provide adequate IT security to protect personal data.

The legislation doesn’t specify what those measures should be. It says they need to be “appropriate to the risks”. The problem is the nature of that risk is changing. In a survey of 700 IT and IT security professionals by the Ponemon Institute, 69 per cent said they saw the severity of malware incidents increase in the last year.

While web-born malware attacks are cited as the most common threat (by 80 per cent of respondents), there was significant growth in persistent targeted attacks (up from 50 to 65 per cent) and zero-day attacks, which exploit unknown vulnerabilities (up from 32 to 46 per cent).

This increased risk does not only mean organisations could breach EU legislation, which applies to anyone operating in the political bloc. Malware and associated cybercrime also threaten companies’ revenue, internal efficiency, and brand reputation. At the same time as threats are increasing, budgets are not. In the Ponemon Institute study, only 45 per cent of respondents say their organisation’s IT security budget is set to increase.

As a result, current systems are beginning to show the strain. The Verizon 2015 Data Breach Investigations Report found:

- Vulnerabilities are taking too long to discover
- Known flaws are not being patched
- Security policies are not enforced or well-known
- End users are not being educated
- Encryption is missing or poorly implemented and there is a lack of malware protection

What can you do?

Many IT security experts understand the benefits of a layered security model. Instead of employing discrete tools such as anti-virus software, intrusion detection systems, and firewalls, it takes an integrated approach to managing these technologies, augmented with other techniques which include:

- Anti-attack software, which includes anti-exploit, anti-spam and anti-phishing technology designed to disable attacks before they are able to infiltrate the system
- Management of Internet-facing applications built on Java and Flash, which leave the network vulnerable to attack if they are not updated
- Anti-malware, which targets new threats, cleans infections, and can detect undesired software preventing it from spamming users or draining system resources
- Anti-ransomware, which identifies and blocks zero-day ransomware before it can encrypt files using specialised technology
- Management of network infrastructure, to ensure fully updated and patched operating system software

But gaining approval for funding layered security can be difficult, given existing budgetary constraints. IT security teams need to build a structured and well-argued business case to secure additional investment. The following sections show how.

Situational analysis

In 2015, businesses saw a 38 per cent increase on the 42.8 million detected security incidents from the previous year, according to PwC's The Global State of Information Security Survey 2016. Clearly the threat is growing.

Part of the reason for this increasing vulnerability can be put down to changes in the model most people use to access computing power. A majority of IT admins and security practitioners believe there's a significant increase in endpoint risk because of use of commercial cloud applications (73 per cent), employees working from home or other offsite locations (63 per cent), and employee-owned mobile devices (68 per cent), according to the Ponemon research.

At the same time, the nature of the threat is changing. Hackers and malware authors are increasingly likely to come from serious organised criminal gangs or be employed by nation states.

Attacks can come from cyber espionage, trying to steal confidential or sensitive information, carry out fraud and disrupt business. They design emails or documents to obtain remote access to networks and install Trojans to gain future access as needed. They deploy ransomware to encrypt a hard drive or database so hackers can demand a fee to unlock the data.

Meanwhile authors of financial malware use exploit kits to infect businesses with malware such as Zeus or Zbot that target vulnerabilities in common endpoint software—browsers, Java and Acrobat Reader—to help hackers gain access to online banking credentials.

Anti-virus software, intrusion detection, and firewalls cannot protect the entire infrastructure on their own. These traditional security suites require the malicious software to be both known and detected in order to prevent execution. While security experts can rush to develop signature updates for an outdated security model, the threat landscape continues to change. By the time the security fix is rolled out, the damage has been done. Existing security solutions are largely ineffective, simply because they are too slow to respond and require updating, either by receiving new malware or network attack signatures before they can provide an effective defence.

Problem statement

After analysing the current threats and their approach to defending them, IT managers and security professionals seeking resources for a new, layered approach to security need to put this information together in a succinct problem statement. Successful statements will show how there are gaps in common approaches to managing risk in IT security and help attain necessary budget.

IT security can reveal shortcomings in the existing approach by using remediation tools to pick up signs of infection or dormant code on endpoints. Since malicious threats remain undetected on business endpoints for seven months on average, a typical scan will reveal signs of infection on around 20 per cent of PCs, for example. Security managers only need to scale up from a small test sample to demonstrate the extent of the problem.

A good problem statement describes the operational and financial implications of information security weaknesses.

It covers how much IT administration time is wasted in fixing infected machines, the demands of legislation on IT security, the risk of financial loss, the cost of operational downtime, and the damage to brand value in the event of a serious incident.

Help in measuring risk

The financial risks resulting from cybercrime are real. In 2016, aerospace supplier FACC said a single hacking incident had cost the financial accounting department around $55m. PwC found the average total financial losses due to security incidents were $2.5m in 2015 and that theft of "hard" intellectual property increased 56 per cent. A discussion with the finance department would further outline what is at risk if their systems are breached while legal departments can provide information about the value of intellectual property.

Reputation also suffers after a cyber attack. Online dating website Ashley Madison suffered an attack from hackers who threatened to leak personal and credit card information of 37 million customers worldwide. Although it secured the site shortly afterwards, parent company Avid Life postponed a $200m listing on the London Stock Exchange. At the time, Wells Fargo analyst Gray Powell said the breach demonstrated that security was about more than simply budget dollars and that lost customer data can dramatically impact business plans, brand perception, and company valuations. Marketing teams may be able to help understand the corporate brand value and the cost of any damage from a security incident.

Lastly, there is the cost to operations in the event of a severe data breach. In 2014, Sony Pictures Entertainment faced $100m in losses from a computer hack, according to cybersecurity experts. This included lost productivity while operations were brought back online. Reaching people in the business who can break down the cost of operational downtime will help calculate the value of improving information security.

Proposing the solution based on the problem statement and risks

There is a relatively new approach to information security which goes beyond traditional anti-virus and anti-hacking techniques. It presents three different dedicated technologies to harden vulnerable attack vectors and to protect against new and advanced threats.

Anti-exploit tools add a fundamental layer to the protection of software and data by reducing opportunities for malware to become attached to software, rather than focusing on the malware itself.

By shielding vulnerable applications, such as browsers, PDF readers, Microsoft Office applications and media players, anti-exploit tools can stop attacks before they occur by detecting malicious activity, such as Adobe Acrobat Reader attempting to download and run an .exe file from the internet–a clear indication of infection.

While traditional tools such as anti-virus and web filtering products can provide effective protection in some cases, and organisations should continue to use them, an anti-exploit layer will offer businesses four additional levels of protection:

- Prevents shellcode executing by hardening outdated or unpatched applications so they are less susceptible to exploit attacks
- Avoids operating system security bypasses, using multiple advanced memory protection techniques to detect attempts to bypass existing operating system protections
- Provides memory caller protection, to prevent exploit code from executing from memory
- Protects against application behaviour designed to circumvent all memory protections such as those typically used in Acrobat Reader and Java exploits

Another essential layer is anti-malware technology, which is optimised to detect and remediate unknown and known threats that circumvent anti-virus and traditional endpoint security. Anti-malware enhances an organisation's security posture with three fundamental capabilities:

- Detects and remediates advanced zero-day threats
- Employs behaviour-based heuristic detection to detect polymorphic malware
- Runs alongside other endpoint security solutions/ layers without conflict

Ransomware, a relatively new threat actor, now poses a significant operational threat to organisations of all sizes. Anti-ransomware technology identifies and blocks zero-day ransomware before it can encrypt an organisation's data. Though some anti-virus products may prove effective against well-known ransomware, anti-ransomware technology adds unique defensive capabilities:

- Detects and remediates unknown and known ransomware
- Employs specialised behaviour monitoring technology to identify zero-day ransomware
- Is engineered from scratch to defend against ransomware
- Does not use signatures; does not require database updates

Creating a layered approach to security by adding anti-exploit, anti-malware, and anti-ransomware technologies provides a level of protection traditional approaches on their own cannot match.

Cost-benefit analysis

The cost of introducing layered security, in terms of licensing and implementation costs, will be tens of dollars per PC, dependent on negotiations with specific vendors.

The first benefit: avoided risk

Layered security slashes dwell time–the window of opportunity hackers have between installing malware and discovery of the malware by the IT team–so systems are less vulnerable. Security managers can argue that without additional measures, the business has a certain five-year probability of suffering serious data breach or operational outage. Using examples of successful attacks on others, they can estimate the value of risks avoided in financial and brand value terms.

Second benefit: layered security reduces damage to endpoint systems

Where malware is found, it can be removed and damage remediated remotely, without re-imaging. Currently, the average time taken to find, to clean and to re-image a PC is between three and five hours.

These two benefits, combined, massively reduce man-hours spent on routine IT administration.

Bottom line

Whether trading with customers or suppliers, businesses today are online by default. Cloud computing and ubiquitous mobile devices are added dimensions that can lead to vulnerabilities. Not only is the criminal community more determined to exploit gaps in information security but the reputational, financial and operational damage to the victim is greater. Building a solid business case for layered security will ensure the IT organisation gets the resources it needs to better protect the business.

About

Malwarebytes provides anti-malware and anti-exploit software designed to protect businesses and consumers against zero-day threats that consistently escape detection by traditional anti-virus solutions. Malwarebytes Anti-Malware earned an “Outstanding” rating by CNET editors, is a PCMag.com Editor’s Choice, and was the only security software to earn a perfect malware remediation score from AV-TEST.org. That’s why more than 38,000 SMBs and Enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, Malwarebytes is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts.

malwarebytes.com

emeasales@malwarebytes.com