Malwarebytes

WHITEPAPER

Calculating the return on investment in layered security

Understanding the threat

What if it never happens? That's the question which hangs over every investment in security. It's the same with IT security. Big hacks can hit sales, down operations and damage the brand. But they're not common—or so many businesses believe.

The problem is that this is difficult to know. Businesses are only aware of the hacks that make it into the public domain, such as the Ashley Madison attack which saw members of the discreet dating website have their personal details stolen, effectively destroying brand value. But the majority of security breaches never make it that far.

In fact, 90 per cent of large organisations and 74 per cent of small firms have suffered some kind of attack, according to a survey by consultants PwC. What's more, the cost of each attack is escalating sharply. The PwC study, which drew responses from 664 IT managers and senior business executives, found that the average cost of an IT security breach ranged from £1.46 million to £3.14 million in 2015, more than double the respective figures for 2014.

The average cost of an IT security breach ranged from £1.46 million to £3.14 million in 2015, more than double the respective figures for 2014.

But it is not only major breaches that create costs and damage businesses. There is a constant drip feed of viruses, Trojans, phishing attacks, and other types of malware. These slow systems down and create vulnerability to further attack. Managing these threats and repairing the damage done creates a constant drain on IT resources. According to a survey of 1755 C-level executives by consultancy EY, 43 per cent saw malware as the top threat in 2015, compared with 34 per cent in the previous year.

The good news is the IT security industry has developed new methods and technologies to help reduce the threat of a major breach while reducing the cost of day-to-day upkeep. The common way of protecting systems is to employ discrete tools such as anti-virus software, intrusion detection systems and firewalls. A more efficient and sophisticated approach, layered security, integrates the management of these technologies 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, cleanses infections and detects 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

The question for chief information officers and IT directors is how to demonstrate return on the investment in layered security necessary to move to the new model.

Where to start

Before calculating the return on a new approach to IT security, businesses should look at their existing infrastructure. Most common antivirus and security suites in use today defend against malicious payloads such as a Trojan, rootkit, virus, bot, or other attack. But before they can detect a payload and prevent it executing, they need to have prior information about it.

This approach has a serious flaw. Businesses can only defend themselves against threats after the security industry discovers them and rushes to develop signature updates. Because the malicious code continually changes, the damage has often been done by the time the security fix is in place.

In a survey of 700 IT and IT security professionals by the Ponemon Institute, 69 per cent said they have seen the severity of malware incidents increase in the last year.

The increasing number of security threats exacerbates this problem. In a survey of 700 IT and IT security professionals by the Ponemon Institute, 69 per cent said they have seen the severity of malware incidents increase in the last year.

The combination of a reactive defence and a growing threat, results in security solutions that are increasingly unfit for purpose. They are too slow to respond and require updates before they can provide an effective defence on their own.

Organisations wishing to demonstrate this weakness need only use remediation tools to scan their endpoints for evidence of malware. Typically, signs of infection will show up on 20 per cent of PCs.

Further examples of external best practice and internal benchmarking will build a picture of an organisation's existing performance. The question is: What is the cost of this poor performance?

Inefficiencies and waste

The day-to-day cost of the current approach to defending against malware lies in the number of endpoints with dormant infections or the remnants of an attack. Cleaning these up costs IT administration in man hours but leaving them creates ongoing vulnerabilities and makes systems unstable and more prone to crashes.

Currently, the average time taken to find, clean and re-image a PC is between three and five hours. Add to this an estimate of user downtime during the process and the cost to the business is considerable.

Meanwhile, the cost of cleaning up machines is increasing as malware becomes more prevalent and organised criminals increasingly use malware to open up a back door into corporate systems.

But it is not just the ferocity of the attacks that requires current methods to become more efficient. As software becomes more complex, the number of vulnerabilities in it becomes more costly to manage. As business people introduce personal mobile devices to the workplace and use unsanctioned cloud services, it makes the problem worse.

We know this because hackers regularly exploit vulnerabilities that are well known in the security industry. Of the 7 million publicly known information security vulnerabilities, just 10 accounted for almost 97 per cent of the exploits observed in 2014 while 99.9 per cent of the exploited vulnerabilities were compromised more than a year after they were published, according to the Verizon 2015 Data Breach Investigations Report.

Clearly, if businesses are leaving machines infected with undetected malware and well-known vulnerabilities remain unpatched, there is an increased risk to the business and current spending is both inefficient and not sufficiently mitigating risk.

The wider cost of inefficient security

Not only do inefficient security models waste time in IT administration but they also increase the risk of online theft and being held to ransom. At the same time, they expose the business to greater losses from reputational damage.

For example, financial malware and ransomware are being delivered via vulnerabilities in software such as browsers, Java, and Acrobat Reader. Special exploitation kits infect users via downloads of malware such as Zeus or Zbot, which enables the hackers to access online

banking credentials. They can also infect databases with ransomware, such as Cryptolocker, to both encrypt files on users' hard drives and demand a ransom to unlock the files.

There is growing evidence of direct theft as a result of hacking. PwC found the theft of 'hard' intellectual property increased 56 per cent between 2014 and 2015, for example.

Anecdotal evidence supports the data. Aerospace supplier FACC suffered a single hacking incident in early 2016 which cost the financial accounting department around $55 million.

Interruption to operations can cost the business. In 2014, Sony Pictures Entertainment suffered an attack and lost tens of millions of dollars in productivity while operations were brought back online, according to security experts.

Lastly, there is the cost to reputation. Shortly after the Ashley Madison attack, Wells Fargo analyst Gray Powell said the breach showed security was about more than straightforward financial loss. Lost customer data can dramatically impact business plans, brand perception and company valuations, he said.

73% of consumers would reconsider buying from a company if it failed to keep their personal data safe

Communicating risk to the business

Having established the inefficiencies in current models of security, IT leaders will improve their defenses if they demonstrate the threat to the business.

In consumer-facing businesses, for example, IT security can directly affect the relationship with customers. Research from Deloitte shows only 51 per cent of consumers consider switching companies if they are charged a higher price for a similar product. However, it also shows 73 per cent of consumers would reconsider buying from a company if it failed to keep their personal data safe. When security is more important to consumers than price, suddenly the business case leaps into focus. It is not just consumer-facing businesses that are affected. In the business-to-business supply chain security is also important. A study by consultancy EY found that subtle and persistent cyber breaches in supply chain and online ordering systems lead to degradation of production and receivables collection. This results in missed revenue projections of 2-3 per cent.

Meanwhile, there are legal ramifications to insufficient security. The EU General Data Protection Regulation, proposes a fine of 4 per cent of annual revenue for companies failing to provide adequate IT security to protect data.

The legislation does not specify what those measures should be. It says they need to be "appropriate to the risks".

Together, legal, financial, and reputational risks make a compelling case for a modest investment in a new model for information security.

Business benefits of a new model

Some organisations have succeeded in increasing their protection against cyber threats while creating more efficient internal security processes. The answer lies in a layered approach that complements existing anti-virus, firewall, and intrusion detection.

A key complementary layer is dedicated anti-exploit technology. Anti-exploit technology provides four layers of protection against exploit-based malware attacks by:

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

Another key complementary layer is anti-malware technology. Anti-malware technology 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

Anti-malware solutions can also remove all traces of malware, including malware artefacts, from endpoints. This avoids wasted man-hours in IT administration, improves system performance and reduces future vulnerabilities.

Anti-ransomware technology is increasingly becoming a required layer. 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

These approaches reduce data loss and save on IT resources by protecting against so-called zero-day malware which is unknown to the security community and is difficult to track down with traditional security solutions.

Demonstrating returns

How many hours does IT administration spend cleaning up and re-configuring PCs and other systems after malware infection? How much does it cost per hour? What is the cost of business downtime while repairing systems? Answering these questions helps demonstrate the waste in the current IT security model and hence what businesses can save in moving to layered security.

However, there will be additional benefits that are more difficult to quantify. Business leaders might believe a serious cyber security breach won't happen to their organisation but cyber attacks can cost businesses hundreds of millions in direct financial theft, lost revenue and damage to reputation.

Layered security helps organisations mitigate these risks. Measuring these avoided costs can be difficult but they can come as an 'added extra' since the move to layered security can be covered by day-to-day efficiency savings in security and IT administration.

Lastly, layered security can provide greater additional assurance that the business is complying with legislation. Combined, these benefits create a solid case for the return on investment of layered security and is recognised by an increasing number of successful IT leaders.

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