THE BUNKER

Part of the CYBERFORT group

FACTSHEET

CYBER SECURITY:
Layered Approach

TODAY'S CYBER CRIMINALS ARE JUST TOO PERSISTENT

In light of all the headline-grabbing network security breaches, it's understandable that organisations might be on high alert to prevent their own businesses from being thrust into the spotlight. Unfortunately, the silver bullet they are looking for does not exist.

A lot of cyber crime involves highly organised groups and market forums. These groups and individual hackers are usually able to infiltrate systems because much of the IT infrastructure in organisations is outdated and inconsistent in the way security is implemented. That's why having multiple layers of security is so important. It's virtually guaranteed that you won't be able to completely prevent a hacker from gaining access; however, having multiple defences gives businesses more time to identify and delay the attacker fromreaching the most valuable data and assets.

YOUR BUSINESS IS LIKELY TO BE INFECTED; BUSINESSES ARE SUCCESSFULLY COMPROMISED EVERY DAY

WHAT MAKES IT SO HARD TO FIND THE ATTACKERS?

They are patient and can lie low for weeks — even months — until they're ready to attack and disable critical systems or steal your data. Alternatively, they exploit vulnerabilities on webfacing applications and grab data before you even realise what happened.

There has been a focus on building layered security defences for years. However, traditional security architectures and tools are failing in today's threat landscape.

The State of Advanced Persistent Threats study published in December 2013 by the Ponemon Institute, advised that advanced attacks went undetected for an average of 225 days. The proverbial "needle in a haystack".

MYTH:
Your business is not vulnerable

REALITY:
Attackers bypass traditional security defences every day

Telephone: 01304 814800 Email: info@thebunker.net

"Layered security", also known as "layered defence", describes the practice of combining multiple mitigating security controls to protect resources and data.

The term is similar to "defence-in-depth", which is adopted from a military strategy that involves multiple layers of defence that resist rapid penetration by an attacker. As the incursion progresses, resources are consumed and progress is slowed until the incursion is halted and turned back.

The information assurance use of the term defence-in-depth assumes more than just the deployment of technical security tools. It also implies policy and operations planning, user training and physical and logical access security measures.

This security is implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response. Defence-in-depth also seeks to offset the weaknesses of one security layer by the strengths of two or more layers. The security of each of these mechanisms must be thoroughly tested before deployment to ensure that the integrated system is suitable for normal operations. After all, a chain is only as good as its weakest link.

Within a defence-in-depth security strategy, layered security is regarded by some as merely a delaying tactic used to buy time.

PUTTING IT SIMPLY, FOR EVERY CATEGORY OR LAYER OF THREAT, THERE SHOULD BE AN EFFECTIVE CONTROL DEPLOYED TO MITIGATE THE THREAT

HAVE I GOT THE RIGHT TOOLS?

As cyber threats continue to evolve, old security solutions just don't cut it. Cyber threats and the entire nature of information security are evolving at a blistering pace.

NEXT-GENERATION FIREWALLS

Historically, Next-Generation Firewalls (NGFWs) use an application-centric approach to classify network traffic in an effort to stop malware and other attacks. However, NGFWs have been proven ineffective against advanced attacks as they are rules-based and therefore can be fooled.

ANTI-VIRUS SOFTWARE

In the face of zero-day and advanced persistent threat attacks that exploit unknown vulnerabilities, anti-virus is all but helpless in preventing modern cyber threats. Some research suggests that 90% of code elements in malware morph within an hour, allowing them to sneak past anti-virus software that relies on signature-based detection which may be out of date by hours, days or weeks. This window is also long enough for the malware to install other infections that can include password crackers and key loggers that embed deeply into the compromised host system.

WEB GATEWAYS

The cyber security industry has given us a legacy of pattern matching. Web gateways employ these same technologies. Web gateway technology uses databases and lists of known "bad" internet sites, but do not take today's real, evolving threats into account. Policy enforcement and low-level security are about the only value that web gateways bring to the security table as cyber-attacks have evolved to render gateways ineffective. The dynamic nature of malware delivery and communication renders lists of "bad" websites and internet sites obsolete.

THE LAYERED APPROACH!

It is hard to compartmentalise security down to a single person or department's job. While the facilities department focuses on physical security by maintaining the building, IT is hard at work keeping viruses, hackers, unauthorised users and unauthorised content from damaging the information infrastructure.

Multiple layers of network security can protect networked assests, data and end-joints — just as multiple layers of pohysical security can protect high-value assets.

With a defence-in-depth approach:

- System security is purposely designed into the infrastructure from the beginning. Attackers are faced with multiple hurdles to overcome if they want to successfully break through or bypass the entire system
- A weakness or flaw in one layer can be protected by strength, capabilities or new variables introduced through other security layers
- The focus should be on more rapid and smarter detection of unusual activity

DEFENCE-IN-DEPTH

TYPICAL DEFENCE-IN-DEPTH APPROACHES INVOLVE FIVE AREAS: PHYSICAL, NETWORK, APPLICATION, DEVICE AND COMPUTER.

I. Physical Security

It seems obvious that physical security would be an important layer in a defence-in-depth strategy, but don't take it for granted. Guards, gates, locks, port block-outs, and key cards all help keep people away from systems they shouldn't touch or alter. In addition, the lines between the physical security systems and information systems are blurring as physical access can be tied to information access.

2. Network Security

Network security should be equipped with firewalls, intrusion detection and prevention systems, and general networking equipment such as switches and routers configured with their security features enabled.

A demilitarised zone allows data and services to be shared securely.

3. Application Security

Infusing applications with good security practices, such as role-based access control, which locks down access to critical process functions; force username/password logins, combinations, etc.

4. Device Hardening

Changing the default configuration of an embedded device can make it more secure. The default security settings of routers, switches, firewalls and other embedded devices will differ based on class and type, which subsequently changes the amount of work required to harden a particular device.

5. Computer Hardening

Well known (and published) software vulnerabilities are the number one way that intruders gain access to automation systems. Examples of computer hardening include the use of:

- Antivirus software
- Application whitelisting
- Host intrusion-detection systems and other endpoint security solutions
- Removal of unused applications, protocols and services
- Closing unnecessary ports

Computers are susceptible to malware cyber risks including viruses and Trojans. Software patching practices can work in parallel with these hardening techniques to help further address computer risks. Follow these guidelines to help reduce risk:

- Consider disabling software automatic updating services on PCs
- Maintain an inventory of all hardware and software including applications and software versions and revisions
- Subscribe to and monitor vendor patch qualification services for patch compatibility
- Obtain product patches and software upgrades directly from the vendor
- Pre-test all patches on non-operational, non-mission critical systems
- Schedule and apply patches and upgrades and plan for contingencies

WHAT ABOUT YOUR DATA?

In the face of rising threats, the UK Government has launched several initiatives to try and improve the cyber security awareness of small businesses. This included "Cyber Essentials", a certification scheme introduced in 2015 designed to help consumers establish whether an organisation has implemented basic cyber security measures.

Despite this, data security breaches are at an all-time high with no end in sight. Over the past decade, we've seen some major breaches at well-established organisations who have had traditional network and data security defences in place yet were still breached for one reason or another: Target, TalkTalk, Sony, LinkedIn, Yahoo, Tesco Bank and Sports Direct, to name a few.

What have we learned from all these breaches? Why are organisations still struggling with the age-old problem of information security?

To put it simply, the approach has always focused on everything but the data, securing the network and perimeter, securing the servers and endpoints, and securing the applications. IT departments and security teams are still using technologies and methodologies which were deployed assuming an organisation owned everything on and inside their network — most organisations are not re-evaluating their data security strategy and tools fast enough to deal with realities driving the business today.

WHY ARE ORGANISATIONS STILL STRUGGLING WITH THE AGE-OLD PROBLEM OF INFORMATION SECURITY?

These days there is a need for business acceleration through collaboration, primarily driven by the proliferation of cloud application and mobile devices.

History has shown us that IT security teams have added more and more layers to try to fix the data security problem.

In the mid-1990s, e-commerce grew significantly. Security back then was limited largely to browser- based encryption. This provided a protected communication channel but the credit card information was not protected once it got to the other end. Most times it was sitting in clear text.

By the mid-2000s, more sophisticated web apps were developed. Hackers figured out that attacking credentials versus the transport layer was a lot easier and more fruitful, leading to the rise of phishing attacks, which we still see in abundance today—exploiting the ever-vulnerable human element in systems of controls.

And finally, in the past 10 years, multi-factor authentication has come into the mix to help solve the weak passwords problem, but that isn't working either. Valuable data is still being stolen from organisations.

In the last two generations of the Internet, all we've done is made it harder to get to the data but we're not really fixing the data protection issue. Today, the Internet is the most untrusted it has ever been. The solutions we put in place 5 years ago just won't solve the problem anymore. We've built walls around the data, but at some point that data has to be shared with someone else: then you lose visibility or direct control of where that data goes, where it resides and where it ends up.

TODAY, THE INTERNET IS THE MOST UNTRUSTED IT HAS EVER BEEN

IT'S NOT PERFECT BUT IT'S CLOSE

The stark reality in today's digital, connected world is that there can be no absolute security, but this by no means suggests the good guys can't fight to win.

Although absolute security will always be out of reach, facilities and IT teams can work together to manage security risks to their organisations and to their mission critical systems.

BY FOLLOWING GOOD SECURITY DESIGN PRACTICES AND APPLYING THE RIGHT PRODUCTS AND SERVICES, RISK CAN BE REDUCED, REMOVED, TRANSFERRED OR BROUGHT TO AN ACCEPTABLE LEVEL

How effective is the defence-in-depth approach in practice?

NSS Labs produced a report in 2013 entitled "Correlation of Detection Failures". They tested the security effectiveness of typical defence technologies that are deployed in layered security, such as NGFW, IPS, and endpoint protection (also referred to as antivirus/malware detection). They used realworld attack scenarios to measure the exploit-blocking abilities of 37 security products from 24 different security vendors.

The 1,711 exploits that were used in these tests target 816 software products from 208 different software vendors, thereby covering 21% of all vulnerabilities published against these software products in the last 10 years.

The results of these group tests provide a unique set of data to assess not only the detection performance of individual devices, but also the performance of any combination of security devices.

KEY FINDINGS FROM THE NSS LABS RESEARCH

Security performance varies greatly not only between individual products, but also between combinations of specific products.

The joint failure rate for all combinations of security device pairs was lower than the failure rate of any single device; however, the exact combination of products makes a significant difference. The best combination of two IPS devices, for example, detected all but 2 exploits, while the worst combination failed to detect 61 exploits.

There is only limited breach prevention available.

They examined 606 unique combinations of security product pairs (IPS + NGFW, IPS + IPS, etc.) and only 19 combinations (3%) were able to successfully detect all exploits used in testing. This correlation of detection failures shows that attackers can easily bypass several layers of security with the use of only a small set of exploits.

Exploits by passing detection attack prevalent and relevant software, not niche products.

The exploits that bypass the most systems almost exclusively target software from mainstream software vendors that is used regularly within the enterprise and private environments. For example, none of the 33 network security devices (NGFW and IPS) that were tested were able to successfully detect all exploits against Microsoft products, and only 5 of the 33 systems tested were able to successfully detect all exploits against Apple products.

Correlation matters.

The number of exploits that were found to bypass multiple security devices is significantly higher than the common expectation. Security professionals must take into account the effects of correlation when modelling risk.

IN CONCLUSION

Layered security is beneficial when looking to secure the enterprise; however, it is the choice of security solutions and intelligent combinations with core security practices and controls that is key to realising substantial security gains and to offsetting the increase in complexity, management and cost.

This is the second in a series of three cyber security white papers. In the final paper of the series, we will be investigating the world of cyber intelligence. It would appear that traditional security measures are no match for today's unrelenting, well-funded attackers and accelerate their ability to limit new risk and apply intelligence to stop attackers. We will demonstrate how forward-thinking organisations can improve their risk position and reduce the likelihood of exposures, through a considered and targeted cyber intelligence programme.