3 Pillars for Cybersecurity Success

Syscomm

Table Of Contents

From the relatively harmless computer '80s' worms to the ransomware of today

It's About the Money

Viruses as we know them today really started to become a problem in the late 1980s, as computers became more commonplace and individuals began to experiment to see what kind of problems they could cause by imbedding some kind of malicious code. Early on, these 'worms' encountered virtually no security barriers and, as a result, were able to quickly spread. They were generally fairly harmless or would corrupt data and destroy files for no other reason other than to cause problems – acts of cyber vandalism but not an malicious acts of ransomware. However, over time, things began to change and computer viruses like ILOVEYOU found new and innovative ways to wreak havoc on the internet.

A Modern Approach to Cybersecurity

With the advent of the AIDS Trojan and the Michelangelo virus, things began to change and the first truly destructive and malicious viruses began to emerge. Companies who had viewed security as a secondary concern started shifting priorities, and antivirus products, once seen as a nice luxury, became absolutely essential.

In 2007 however, users around the world witnessed first-hand just how unsecure their data really was when TJ Maxx admitted that hackers had compromised its database, stealing at least 45.7 million credit card data.

Since then, the hacking industry has exploded. Since 2015, cyberattacks have cost businesses £87 billion, cording to a new study by specialist business internet service provider (ISP) Beaming.

The term 'anti-virus software' is also becaming outdated as new types of malicious programming are regularly released. Today, malware has become the umbrella term for an ever-growing list of cyber security risks that include:

- Ransomware
- Trojans
- Spyware
- Adware
- Worms
- Spam
- Viruses
- Scareware

Each comes with different threat trajectories and delivery methods – locally installed security software simply is no longer enough to keep your business safe.

You need a combination of several cybersecurity solutions to protect your business and data

Perimeter Security

A Barrier Between your Network and the Internet

Web services, cloud technologies, and mobile devices bring countless opportunities for organisations, while also significantly increasing the number of services and solutions that need to be monitored. A single weakness amidst your many connections is all a piece of malware needs to take hold of to spread across your entire network.

The key to addressing these types of threats starts with a strong perimeter security framework that polices and controls access to critical applications, services, and data, while denying known threats and monitoring suspicious activity. Some examples of perimeter security solutions include:

Firewalls

A firewall is a hardware or software device designed to permit or deny data through a computer network in order to protect the resources of a private network from users from other networks. In essence, a firewall examines all data trying to pass it to determine whether to forward it onto its destination. In most server infrastructures, firewalls provide an essential layer of security that, combined with other measures, prevent attackers from accessing your servers in malicious ways.

Modern firewalls filter traffic based on many packet attributes such as source IP address, source port, destination IP address or port, destination service like WWW or FTP. In addition, they can screen traffic based on protocols, TTL values, netblock of originator, domain name of the source, and many more user-defined attributes.

Firewalls are used for preventing malware, such as Trojans, from sneaking into a network and creating ways to bypass security solutions. However, they can also be configured to prevent employees from transmitting sensitive data from inside to outside the network.

Whilst regular endpoint security solutions such as a firewall are a part of the solution, their weakness is that they rely upon signatures and awareness of the threat before mitigating the risk – protecting against the 'knowns'.

It follows that regular endpoint solutions are unable to protect against a threat they do not yet know about (the 'unknowns') and can therefore leave an organisation susceptible to a zero-day threat or one that has been amended to bypass identification.

Endpoint Detection and Response

A logical companion to a firewall is Endpoint Detection and Response, a solution designed to recognise malicious network activity. This solution employs something called 'anomaly-based detection' to sift through applications, network packets, IP addresses, and data to look for patterns that could indicate an intrusion - even if it appears to come from a safe source. This method of detection is extremely effective against hackers who alter existing malware just enough to evade detection.

When malicious payloads are detected an Endpoint Detection solution immediately quarantines and/or kills them before the infection is able to spread.

EDR also provides comfort for the board, regulators and customers that your organisation has taken its security posture seriously and is responding to the punishing realities of today's evolving cyberthreats by rearchitecting your network defences accordingly.

Phishing Protection

Some studies show that 91% of cyberattacks start with a phishing attack, usually delivered via email. Phishing is a cyberattack that uses disguised email as a weapon, with the goal to trick the recipient into believing that the message is something they want or need - a request from their bank, a link for some important news, or even a note from someone in their company – causing them to click a link or download an attachment.

Anti-phishing solutions block unsolicited ads and flag emails with suspicious attachments to ensure employees don't receive potentially dangerous messages in their inboxes. More advanced solutions come with 'safe browsing' features, which inspect the destination of the URL to make sure it's safe for users to click.

Even with a strong network perimeter, hackers can find ways to bypass your 1st line of defence. Beef up your business network with multiple layers of security.

Intranet Security

A firewall can't prevent an employee from plugging in an infected USB drive

Firewalls, End Point Detection and Response, and Spam filters can protect your network only from threats that originate on the internet side of your digital perimeter. But protecting individual computers and devices from threats that have compromised your local network are still one of the three fundamental aspects of modern cybersecurity. There are a number of ways to protect your intranet, but the most basic strategies include:

Patching and Updating

No program or application is perfect. Technology is always changing, and as new features are added new vulnerabilities are bound to emerge. Software vendors regularly release security patches, making the patching of vulnerabilities essential for front-line defence. Yet unpatched vulnerabilities remain a leading cause of data breaches because many security professionals tend to delay or put off updating or patching their systems.

While general software updates can include a variety of features, patches address specific vulnerabilities. Vulnerabilities are weaknesses in the security of a software programme or operating system through which malicious actors can then use code to exploit. In short, patches minimise your attack surface and protect your system against attackers.

Patching vulnerabilities in a timely manner may be what saves your business from a breach. Automated patch management solutions can make the process of patching for vulnerabilities more streamlined, helping to ensure that updates are deployed to every device in your network.

Maintaining good cyber hygiene practices is essential for minimising your attack surface and keeping breaches at bay.

Anti-malware Software

Early on, anti-virus software was all that companies needed to protect themselves. With the rapid sophistication of today's cyberthreats, anti-malware programs are what your network needs today. With regularly updated catalogues of every known virus, trojan, worm, keylogger and whatever else has been released over the years, anti-malware software is installed on individual machines and protects them from todays known threats.

Outdated malware continues to pop-up time and time again. Regardless of whether a computer is infected because someone plugged in a USB drive that hasn't been formatted in years, or because an employee accidentally clicked on a link in a Coronavirus phishing email, anti-malware solutions will prevent an infection. However, it is critically important that you remember that these solutions cannot protect your organisation from new and bleeding-edge malware threats.

Syscomm recommends customers implement two layers of Endpoint security - a pre-execution and a post-execution security solution at the PC, Laptop and Server Endpoints. This ensures that your business has highly tuned endpoint protection that maximises effectiveness and performance.

Physical Security

With hundreds of new cybersecurity threats being discovered every day, it can be easy to get caught up focusing on just the digital defences. It's helpful to remember that software is not your only weapon when it comes to cybersecurity. Physical cybersecurity defences need to be another critical tier in your lines of defence and must be woven into everything you do - particularly if you operate in a regulated industry.

Every data regulation standard - Sarbanes-Oxley, the Payment Card Industry are two key examples - requires you to safeguard your information with video surveillance, restricted physical access to databases, and more. Taking such physical cybersecurity defence measures gives your organisation a solid security foundation on which to build its other digital security defences.

The weakest chain in cybersecurity tends to be your employees!

The Human Factor

Cybersecurity: The Responsibility of Everyone

When security breaches make headlines, they tend to be about powerful malware attacks on large organisations undertaken by cunning hackers or foreign governments, causing many of us to believe that these are the only threats we should be worried about. Because of this, businesses tend to focus all their resources into perimeter and intranet security, often overlooking the risk exposure created by their own employees.

But if we're going to win the battle against cybercrime, everyone, from corporate executives to their customers, has a role to play in preventing future attacks.

Human error accounts for 52 percent of the root causes of security breaches, according to a new study from CompTIA, with mistakes such as answering unsolicited emails, connecting to unsecured networks, and setting weak passwords being the most common. If even the most 'low tech' of solutions are failing when it's trusted individuals that are introducing the cyberthreats, however inadvertently, firewalls, anti-malware software, and spam blockers won't be able to protect your business.

Fortunately, there are several ways to ensure your employees don't fall into these traps.

Education and Awareness

Comprehensive security awareness training must be provided so that employees know how to defend themselves and your business against different threats. Whilst it would be unreasonable to expect everyone to become a cybersecurity expert, having a basic understanding of the risks and how they may present themselves could mean the difference between falling victim to a cyberattack or someone spotting it before it becomes an issue. Regardless of whether you're conducting training seminars in-house or getting expert third-party support, it is imperative to cover these key topics:

Malware

Devote time to defining the various types of malware (e.g., ransomware, Trojan horses, worms) and explain what each are capable of. This helps staff identify the onset symptoms of malware and what to do if they suspect their device is infected.

Public Hotspots

If your company has remote work or bring-your-own-device policies, your staff needs to know how dangerous public WiFi networks can be. Hackers are able to tap into these unsecured networks (or create their own) to intercept incoming and outgoing traffic. Your employees ned to be extra cautious about connecting to any WiFi hotspot in a public place. To save their work and private information, traffic, and browsing data as well as to protect themselves from possible identity theft, stay away from unsafe networks or use a VPN.

File-sharing

A surprising number of breaches occur simply because employees carelessly share sensitive files or leave them open while they're away. It's important to educate your staff about which documents they're allowed to share and with whom they can share them.

If your business or employees are using a file-sharing network, keep in mind that the risk of these networks being riddled with malware, phishing and a lot of other similar risks is quite high and that file sharing can come with serious threats for your business network. Although having a strong firewall in place will help mitigate these risks, as much as possible, avoid using these websites.

Phishing

To prepare your employees for these threats, help them identify the tell-tale signs of online scams such as emails that urge users to click on a link, or pop-up ads that offer free goods in exchange for completing a personal survey.

Ultimately, your goal is to teach your staff to develop a healthy skepticism of every link, file attachment, and website they see online.

Password Policies

Generic passwords tend to be Achilles heel of most cybersecurity frameworks, with recent reports finding that '123456' and 'password' are still commonly used passwords, allowing today's hackers to easily guess login credentials and hijack accounts. This threat can be addressed simply by ensuring your employees set strong and unique passwords for every account.

Complicated passwords with a mix of uppercase and lowercase letters, numbers and symbols are increasingly the norm, but you should also make it compulsory to create unique passwords for different accounts. This way, even if a hacker manages to expose the login credentials of one account, they won't be able to gain easy access to others.

2FA / MFA

Businesses and employees may be comfortable simply using a single password, and it can be hard to change the status quo. But the fact of the matter is MFA provides a substantially higher level of security. In an attempted security attack, this extra layer can prove to be the difference between being compromised and staying secure.

2FA / MFA can be done in a variety of ways, but the most common way it is deployed is via mobile device. Your IT system can be configured to send out a security code via text, email, or mobile app to a specific user should his or her credentials be used in a login attempt. If the login attempt is legitimate, the user will simply be prompted to input the security code on a secondary login box within a specific time frame, enabling them to access the network as normal. If it were a brute force hack attempt, the hacker will have no way of getting the security code, leaving them locked out of the system.

And as businesses move to more remote working environments, which bring increased security risks and additional challenges for IT teams, adopting MFA within your organisation can help overcome security challenges around mobility

With regular on-going cyberattacks, it appears MFA is here to stay and will eventually become standard practise in the near future.

Security Testing

Security testing essentially reinforces the best-security-practices you want to see in the workplace – password policies, employee awareness, patching and upgrades, etc.

Beyond simple quizzes or spot checks, it is important that businesses consider hiring penetration testers or security researchers to simulate real-world attacks that truly test both your network security and your employees' security habits.

Remember, tests and security training should be conducted frequently (at least once every quarter). The ultimate goal in the human security layer is to develop critical thinkers who can defend against a variety of threats.

Only when Perimeter, Intranet and Human Factors are working in concert can you be certain that all your cybersecurity pillars are in place.

Joining all Three Pillars

The Key is Personalising your Plan

Up to even a few years ago, employing some level of anti-virus software and a healthy dose of scepticism might have been sufficient to protect businesses from the dangers of the internet - and off-the-shelf solutions could be used as an ideal solution.

But todays cyberthreats are not so easily overcome.

Everything from your firewall to your employee training sessions need to be tailored to meet the unique challenges and demands of your business, including the risks inherit to your location, industry and product and service.

But sometimes, that's not possible - cybersecurity can be a significant investment, both in terms of capital, and the expert personnel needed.

Given the strict needs of a good cybersecurity policy, businesses should seek as much help as possible. Sometimes that can be done through in-house IT, where expert staff is available to set up security guidelines and have the resources to purchase and properly configure and manage complex security hardware and software.

Turning to Expert Help

A more cost-effective approach for many medium and larger businesses is to turn to an expert Managed Service Provider (MSP). A trusted 3rd party MSP can be an invaluable resource for businesses who need assistance managing their technology needs, especially cybersecurity.

This helps them reduce costs and improve efficiency when handling the dangers of digital threats, even if they don't have the same resources as a major company. For an affordable monthly fee, your business can gain 24x7 access to more talent than you could ever afford in house.

The broad array of expertise an MSP provides means your business gets personalised plans for each branch of cybersecurity covered in this eBook. Preventative measures, deployments, optimisations, and ongoing support are provided as a unified service that keeps your business cybersecure - no matter what the future has in store.

Call today to talk with one of our seasoned consultants. We're happy to answer your questions, provide recommendations, and audit your current IT network.

Phone: 0247 771 2000 Email: sales@syscomm.co.uk

Syscomm


32%
23%
INTRUSION DE
HACKING
74%
18%
Syscomm