SHACKLETON
your information technology team

FOUNDATIONS OF CYBERSECURITY

How Shackleton's Layered security suite
can protect your business

Introduction

With businesses facing more cyberattacks than ever, it is essential that companies have a basic level of security protection to their business and their clients. While "basic" at one time may have meant antivirus software, today that's not enough. A layered approach to security is required, bringing multiple essential security services together to deliver greater protection.

Today's businesses face more IT risks than ever before, including ransomware, phishing, hacking, data breaches, distributed denial-of-service attacks, and corporate espionage. There are also many more points of entry to company data through which these attacks can be initiated: web and email traffic, USB drives, unsecured logins, devices like smartphones and laptops, applications and data (both at rest and in transit).

There is no "silver bullet" that can protect against such a wide range of threats. To truly protect your business it is essential to move beyond a simple antivirus and implement what's known as a layered, "defence-in-depth" approach that brings together multiple security tools and controls to defend your IT system. This approach means that if one security control fails or is bypassed, the other overlapping defences should be there to mitigate the threat.

Think about the many layers of security that people use to protect their homes. They put up a fence, lock their doors, install an alarm system and keep their most valuable possessions in a safe. And if all of those fail, they can always fall back on insurance to replace what's been lost.

SHACKLETON
your information technology team

The Building Blocks of IT Security

FIREWALL A firewall works by examining and filtering all the information coming in through your internet connection. It represents an important first line of defence because it can stop a malicious program, or attacker, from gaining access to your network and information before any potential damage is done.

PATCH MANAGEMENT - Many breaches are the result of a hacker exploiting unpatched systems or software. Shackleton monitor and apply software updates to prevent hackers from taking advantage of security vulnerabilities.

MANAGED ANTIVIRUS The best antivirus solutions protect against both known and new malware. Managed antivirus allows Shackleton to deploy across devices and servers and schedule automated scans for times that won't disrupt end users.

WEB PROTECTION More often than not, phishing attacks, drive-by downloads and other web-based attacks happen because an unwary user inadvertently stumbles upon a malicious site. Shackleton can block malicious URL requests to prevent connections to domains known to be used by attackers though web protection software as well as applying content-filtering policies, website blacklists, browsing policies, and more.

MAIL FILTERING The majority of security threats arrive via email. By analysing incoming and outgoing messages for potentially malicious attachments, scripts, domains, URLs and text strings, mail filtering software makes it easy to protect against spam, phishing attempts, and malware.

DARKWEB MONITORING Stolen data - like usernames and passwords - are a leading cause of cyber-attacks. With Dark Web ID, we can find out if your data is for sale on the dark web - allowing you to proactively change it before a breach or cyber-attack.

BACKUP Backup is a lot like insurance: it's not always needed, but when it is, it's a lifesaver. A cloud-based backup and disaster recovery solution is the best defence against most ransomware attacks, making it possible for businesses to get back to work by quickly and easily restoring corrupt or encrypted files.

Layered Security in Action

To illustrate why a layered approach to security is so important, consider the many ways in which ransomware can enter an organisations network.

73% Email attachments

54% Phishing emails

28% Users visiting malicious or compromised websites

Email and web use are by far the most common starting points for a ransomware infection. In most cases, end users unintentionally land on a compromised or malicious website, often lured there by a legitimate-looking link or attachment that tricks the user into clicking or opening it. Just as there are many ways ransomware can get into the network, attacks can be detected in several different manners, with most attacks caught by endpoint security tools, email and web filters, or intrusion detection systems (i.e. network firewalls):

83% Anti-malware/antivirus/ endpoint security tools

64% Email and web gateways

46% Intrusion detection system

SHACKLETON
your information technology team

If a business relies on antivirus alone, almost one in five of all ransomware attacks will get through. But if multiple overlapping security controls are used, even if a threat gets past the first layer of defence, it can still be caught by the next as it moves from device to device. Using "best-in-class" solutions from different suppliers is also good practice as if one solution/company is unaware of a threat, the other are likely to thus decreasing the chance of a new threat getting through the defences.

With layered security, each component is designed to complement the others — and even compensate for the others' gaps — to stop advanced security threats. Patch management helps keep software and operating systems up-to-date with the latest security patches to prevent attackers from exploiting vulnerabilities. Antivirus detects and blocks many known threats. Mail and web filtering quarantine suspicious messages and prevent communications to "command and control" sites. And data backups allow for easy retrieval in case of unexpected loss.

CONTACT US

If you would like to find out about how we can help protect your business from cyber threats then please contact us in the usual way through:

enquiries@shacktech.co.uk
01382 250900

Or contact your **Client Account Manager**.

SHACKLETON
your information technology team