White Paper

The Holistic Approach to IT Security

The Alternative to Papering over the Cracks and Filling in the Gaps

02070936000
talk@htl.uk.com
www.htl.london

An Existential Threat

CIt is widely accepted that IT security is a necessity. Today, news of IT security breaches and cyber crime is so commonplace as to be ubiquitous. It's likely that some have become deaf to it. However, there is no room for complacency; the need for IT security is now of greater importance than it has ever been.

On 7 July 2016, the National Crime Agency Strategic Cyber Industry Group published the report Cyber Crime Assessment 2016, in which it didn't pull any punches. The opening sentence of the Executive Summary states:

"A cyber attack that poses an existential threat to one or more major UK businesses is a realistic possibility."

On-premise Architecture

The familiar on-premise approach to providing for the computing needs of a business puts servers, storage and back-up devices in the same geographic location as the business. This enabled the move away from the expensive mainframe systems on which business computing was previously based, in the 1960s and 70s.

The age of the PC had a democratising effect, putting standalone desktop and client - server computing within reach of smaller firms and enabling them to share in the benefits of the information age. It's certainly possible to view the disruptive nature of much of today's tech as an amplified echo of this.

The Very First Virus

As the 1980's progressed, and Microsoft Windows started its inexorable rise to dominance, malware started to appear. It is somewhat ironic that the first virus, called Brain, was written to protect copyright infringement of medical information. Brain debuted in early 1986 and the rest, as they say, is history.

Through the 1990s both threat and sophistication increased as the Internet provided the conduit for benevolent and malevolent information to flow across the world. Phishing attacks, with the intention of stealing personal information and credentials to commit fraud, began to be seen.

The 21st Century has seen the rapid growth of cyber criminal activity. The classification system used to define and describe threats has had to grow to keep in step. Now, hacking, zero-day and rootkit attacks sit alongside terms such as worm and Trojan. The malware family has multiplied to include adware, spyware, and ransomware.

In Defence of an On-premise Environment

Generally speaking, defending any computing environment is about preventing breaches of the network perimeter. For a conventional on-premise environment this is difficult, because there are many ways for threats to penetrate the network. Email, websites and ordinary documents may all have threats of one kind or another attached to them. Users also routinely use devices and storage media to exchange data with the network. Essentially, there is large attack surface.

The general approach to defending on-premise computing environments may be characterised as one that is composed of point solutions. This means security tools and processes are discrete, not integrated and often manually executed. This includes items such as:

- Security appliances and firewalls
- Anti-virus software
- Identifying suspicious email with heuristic scanning engines
- Patching security vulnerabilities
- Updating application versions

In many SMBs and some larger businesses where IT teams might be short-handed and there might be a vacuum of security expertise, there is a significant risk threat of a security breach.

Cloud Architecture

Cloud computing concentrates server-side infrastructure in a data centre. Typically, a Managed Services Provider (MSP) is contracted to provide IT services to the customer firm or organisation. The MSP delivers information services over secure internet connections from the data centre to the customer's site(s).

Depending on the requirement, the server and storage infrastructure may be shared between a number of customers. This is multi-tenancy, and different tenants do not have access to each other's data, eliminating security issues. Where required, the infrastructure may also be provided in a single tenancy arrangement.

Cloud Services and Centralised Security

The standards of reputable data centres are governed by extremely robust frameworks. For the UK, this ISO 27001, an internationally recognised standard for information security. This ensures very high levels of physical security of the data centre. The measures that might be considered include access control, IP HD CCTV, sound monitoring and prohibiting unaccompanied visits to data halls.

mportantly, cloud architecture puts digital security of the infrastructure under the control of a specialist IT team with very high-level, expert skills. Centralised control enables ISO 27001 security best practice to be applied in a well managed and integrated fashion.

A layered approach to data centre security is widely adopted. This ensures that each individual security element has a backup, helping to eliminate gaps. Extending the idea further, each separate layer is designed to act on a specific area of the attack surface.

With the elements working together, a layered approach to security reduces the network intrusion risk to a cloud computing environment, when compared to an on-premise one using point solutions.

Typical cloud security layers include:

- Web protection
- Patch management
- Email security and archiving
- Vulnerability assessment and analytics • Anti-virus software
- Data encryption
- Firewalls
- Digital certificates
- Anti-spam and spam filters
- Privacy controls

Cloud Services and Security on the Desktop

There is more than one way for users to interact and perform computing tasks under a cloud architecture. The conventional client - server arrangement seen in the conventional on-premise approach is widely used. This simply relocates the servers and storage infrastructure off-premise to the data centre, and users remain unaware that the server is offsite.

Another approach, which is being widely adopted, is to use thin clients on the desktop. Thin clients are network devices that simply enable control and display of a hosted desktop. Hosted desktop computing is executed on a host, the server in the data centre. Thin clients require no disk storage, processors and RAM, offering significant cost reductions over PCs, and users get a familiar Windows desktop.

Hosted desktops offers better endpoint security than PCs. They limit the ability for users to plug in devices and personal storage to upload data (and nasties) onto the network, and download valuable and / or sensitive business data off it.

Nailing down the Loose Ends: Endpoint Security

No matter how much an IT architecture centralises resources, it is only as secure as the endpoints. Hosted desktops might limit the ability of users to physically connect devices and copy data to them; however, this does not address the issue of Wi-Fi enabled mobile devices which many organisations permit to connect to their networks.

Whether company owned, or part of the culture for using personally owned devices in the workplace (Bring Your Own Device or BYOD), smartphones and tablets are a significant threat to network security.

To secure the network perimeter against attack through network and Internet enabled mobile devices, an appropriate Mobile Device Management (MDM) solution is required. This centralises the management of all authorised network devices and ensures that usage policies are not breached, such as those governing upload and download of data to and from the network.

The most appropriate mobile device management software includes capabilities such as remote configuration of a single device, or set of mobile devices; sending software and OS updates; and remote locking and wiping for situations of loss or theft. This makes a well designed MDM solution invaluable to IT teams for managing mobile devices and helps to button down the loose ends of network endpoint security.

Summary

Coupled to network complexity and the use of point solutions to provide defence, on-premise computing environments are at greater risk of security breaches than those that utilise cloud-based computing architectures.

Data-centre based cloud services offer robust physical and digital information security through implementation of ISO 27001 best practice.

Endpoint security at the desktop is increased, when using hosted desktop / thin client cloud services, compared with cloud services that users access through conventional PCs.

An appropriate MDM solution helps to prevent network perimeter security from being breached, as well as prevent the inherent data loss risks from loss or theft of devices.

Many businesses and organisations, which retain an on-premise approach, attempt to fill in IT security gaps and paper over the cracks by adding more point solutions.

This simply wastes money and creates more problems by forcing stretched in-house IT teams to rapidly adopt and get up to speed with a new technology.

Given the level, agility and sophistication of today's IT security threats, a holistic approach built on a secure cloud reduces risk, while at the same time increasing efficiency for lower cost.

Why is HTL Support a Preferred Technology Support Provider

HTL provides a range of services to support the use of technology in today's businesses. Whether it is infrastructure and user support, internet connectivity or voice communications, we provide the high degree of personalised service. We are very proud to be able to say that we offer impartial advice because we are independent of suppliers, vendors and manufacturers. Ultimately this enables clients to obtain more value from business technology.

For businesses that are concerned about IT security, the cloud is a logical step that enables them to take control and eliminate commonly identified flaws and loopholes, to reduce the risks associated with an on-premise computing architecture.

About HTL Support

HTL Support was initially founded in 2009 by Managing Director Justin Dean, to provide specialist IT support and IT consultancy services to financial services sector clients. Since its launch, HTL has rapidly evolved to offer a full range of cutting-edge, integrated and flexible products and services to a worldwide client base across all industries. Our experience and professionalism has been endorsed both by our clients and by many of the world's leading hardware and software manufacturers.

All companies need to know that their IT support provider is not going to let them down when it comes to important projects. We will always find the right solution and are equally happy either functioning as project managers for your internal IT department or providing an experienced team to work under your own IT Director or project leader.

References & Further Reading

HTL Support
5 business advantages of cloud-enabled working practices
https://www.htl.london/white-paper/5-business-advantages-of-cloud-enabled-working-practices

HTL Support
Managed Services and the IT Support maturity model
https://www.htl.london/white-paper/managed-services-and-the-it-support-maturity-model

Mobile device management
From Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Mobile_device_management

Thank You for Downloading Our White Paper

02070936000
talk@htl.uk.com
www.htl.london

30 Churchill Place,
London, E14 5RE