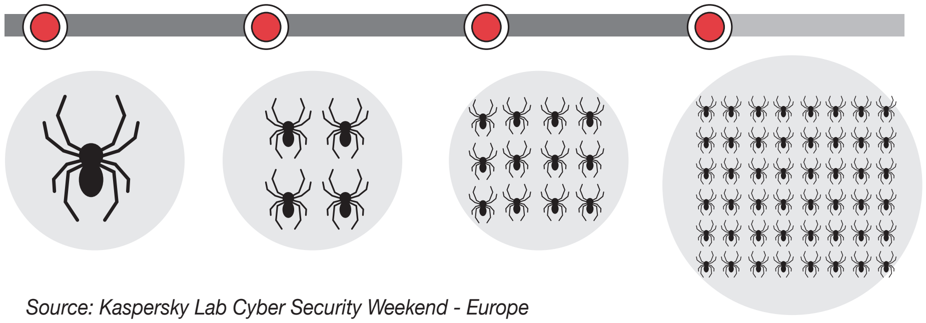
IT Security

Today, your business doesn't just rely on IT, it's dependent on secure IT. Against the backdrop of a constantly evolving security threat landscape, increased demands around compliance and the potentially devastating impact of a security breach, businesses are facing significant pressure to keep their information assets secure.

Scale of the threat

1994	2006	2011	2014
1	1	1	315,000
New virus every hour	New virus every minute	New virus every second	NEW SAMPLES EVERY DAY



Source: Kaspersky Lab Cyber Security Weekend - Europe

Risk Exposure

The stakes are high; in the event of a security breach, the organisation could be exposed to financial and reputational damage, while non-compliance with legal and other standards alone can result in steep penalties and even criminal liability. While most organisations appreciate the importance of ensuring that data is treated with confidentiality, integrity and prescribed availability, IT security and compliance is one of the most challenging organisational disciplines to understand, implement and maintain. Without an information security regime tailored to specific corporate governance requirements, it's nearly impossible to know your risk exposure.

What's in place?

Much of the pressure lands on the IT team. You need to have the right security policies, processes, architecture and expertise in place if you're to maintain a robust and reliable security posture and report risk status back to the business in a standard, understandable language. Even if you're conducting regular assessments and collecting vulnerability data, have you got the tools and resources to turn this data into actionable intelligence and can you create reporting that's aligned to business priorities?

Prioritizing the spend

In the current economic climate particularly, doing 'more with less' is the name of the game. Budgets are cut and expert resources are limited, but the security demands from the business are higher than ever. Cost management is driving the consolidation of suppliers and technologies as organisations look to trim the number of business partners they deal with and the number of technologies they manage. But the security technology market is very fragmented, and there are typically a large number of security hardware and software products installed in an IT estate. How do you rationalise your vendor suite without opening up gaps in your security profile?

Mobility – your data is out there!

Alongside all of this, the pace of innovation continues unabated and business needs to keep up to remain competitive. IT needs to chart actionable roadmaps to support the multiple devices of an increasingly mobile and geographically dispersed workforce - and enable greater numbers of third-party connections - all without exposing the organisation to risk. As with mobility, security is a key area of consideration for organisations on their journey towards virtualisation, as well as private or public cloud environments. Do you have the extensive internal competency and skills resources that you need to get this right?

tTech IT Security Services

Intrusion Prevention Systems

Now more than ever, companies have to rely on the use of Intrusion Prevention Systems (IPS). This is primarily due to the risks from security threats posed by experienced hackers and malicious viruses. Visibility into traffic traveling across networks is essential and companies use Intrusion Prevention Systems (IPS) solutions to identify exploits and actively block these threats and generate alerts. tTech works with the widest used IDS/IPS systems in the industry based on the Snort technology.

Anti Malware systems

The need for anti-virus is essential for any organization in today's high tech environment. tTech provides services to design and implement anti-malware solutions, review existing anti-malware deployments, leverage existing infrastructure to get the best protection for that deployment, and ongoing management of the customer's anti-malware infrastructure.

Active Directory Design

tTech offers active directory infrastructure design, deployment and management services. We are able to deliver safe and secure Microsoft Windows environments. This will improve security and increase reliability of the network by preventing unauthorized applications from being installed and inappropriate access or use of your systems.

Internal Vulnerability Assessments

Many organizations do not know the vulnerabilities present on their internal network. Without knowing what vulnerabilities are present, it is impossible to mitigate those vulnerabilities. Vulnerability Scans are security assessments that identify known network, operating system, web application and web server exploits/vulnerabilities with the use of automated tools. Internal vulnerability scans can give you an overall picture of the vulnerabilities present on your internal network and assist in vulnerability risk management.

Through the use of the best tools available tTech provides services in conducting internal vulnerability assessments, helping organization identify where the threats lie and how to mitigate them.

Penetration Testing

Penetration testing provides "real world security". Penetration test involves vulnerability assessment and further exploitation of said vulnerabilities. This is in attempt to provide a view to the business of what vulnerabilities exist with their network and how those vulnerabilities can cause considerable damage if they are not addressed. Penetration tests are excellent tools to measure the level of security a business has implemented.

Security Awareness Training

Often times organization spend millions implementing security technology and little or no thought to the awareness of the employees. The human element is often seen as the weakest link in the security chain. Through it partners tTech Ltd delivers the essential information that all employees need to protect the company's sensitive data.

Windows Patch Management

The most important, proactive security step to implement. Many organisations either don't do patch management or they do it when the get a "chance". Many of the security risks that exists today can be mitigated with implementing a patch management regime.

tTech can provide design, implementation and management of patch management services.

Firewall Administration

tTech can design and implement firewall policies to protect the corporate network, and manage corporate firewalls.

Security Consulting Services

We assist our customers with security projects such as the implementation of audit requirements, design of security policies and the evaluation of emerging security technologies.

tTECH Limited
69 ½ Harbour Street,
Kingston, Jamaica
t 876-656-8448
f 876-922-0569
e info@ttech.com.jm
www.ttech.com.jm
Twitter @*tTechJamaica*