

The Boss' Guide to Geek Speak

Do you speak Geek?

Every company today relies heavily on technology to complete even the most basic of day to day activities. Yet this reliance comes at a price. The news is full of organisations having to put their hands up to a breach of sensitive data from one source or another – be it a deliberate attack or a victim of circumstance with a mislaid laptop. Combine this with the ICO's determination to name and shame any who do not adhere to the Data Protection Act and enforce its eight principles and its simple to see the financial implications of taking an ostrich's approach.

The problem is fully comprehending the weaknesses you face and how best to strengthen them. You've got your top man on the job but when he presents you with his report it's full of acronyms, end points, phishing, pod slurping and other such terms that are better suited in the dialogue of an episode of Red Dwarf. Geek speak often sounds like normal English that doesn't quite make sense because familiar words have been given a new meaning. For example, a port is no longer where a ship docks and a spool isn't for thread and, for that matter, a thread is no longer a thin strand of cotton. Executing a program is not at all the same thing as killing it.

This article aims to decipher the jargon, converting it to real business contexts, enabling you to not only understand what is being asked for, and how much it will all cost, but fully comprehend why it is needed. Simply, it will give you the power to communicate with the Geeks.

So let's start at the beginning

Let's look at some of the everyday terms used to describe the technology we use and how it works :

Architecture : a term applied to both the process and the outcome of thinking out and specifying the overall structure, logical components, and the logical interrelationships of a computer, its operating system, a network, or other conception. Computer architecture can be divided into five fundamental components: input/output, storage, communication, control, and processing.

Client/Server Architecture : network where some computers are dedicated workstations (often referred to as clients) and some are dedicated servers; information is centralised on the server and an administrator sets policies and manages it.

LAN (Local Area Network) : network that operates within a small geographic area, usually within a building, office or department.

WAN (Wide Area Network) : geographically dispersed network of computers.

WWAN (Wireless Wide Area Network) : wireless connectivity to the Internet. That allows a user with a laptop or PDA and a WWAN card to surf the Internet, check email, or connect to a Virtual Private Network (VPN) from anywhere within the regional boundaries of mobile services.

Operating System : sometimes abbreviated to OS it is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called applications. For example, Microsoft Windows Vista is the operating system, while Microsoft Word and Adobe Acrobat are applications.

Data : information that has been translated into a binary digital form that is more convenient to move or process. It is measured in bits (the smallest unit of data in a computer) and bytes (the standard size - 8-bits).

The Boss' Guide to Geek Speak

Do you speak Geek?

Mobile Device / End Points : This includes mobile phones, laptops, PDAs, memory sticks, CDs, iPods, even digital cameras. It encompasses anything portable that data can be transferred to.

Wi-Fi (Wireless Fidelity) : a term for certain types of wireless local area network (WLAN) that use specifications in the 802.11 family.

What we're trying to avoid

Now that we understand what we're talking about protecting, let's look at some of the things that we're trying to protect them from:

War Driving : locating and exploiting security-exposed wireless LANs. Unless adequately protected, a Wi-Fi network can be susceptible to access by unauthorised users who use the access as a free Internet connection.

Spyware : any technology that aids in gathering information about a person or organisation without their knowledge. On the Internet (where it's sometimes called a spybot or tracking software), spyware is programming that's put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

BotNet : a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer (often home-based) is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator.

Keylogging : records every key pressed on the computer keyboard to get at sensitive data, such as passwords.

PodSlurping : the unauthorised download of data from a computer to a small device with storage capacity,

such as a Flash drive or an iPod or other MP3 player. The small size of the devices and the ease of connectivity - for example through the USB port or a wireless Bluetooth connection - makes it possible for anyone with computer access to surreptitiously download files from it.

The Best Defence is a Solid Defence

This final section looks to decode what can be used to protect against some of these threats :

Firewall : a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Authentication : the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks, authentication is done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

Encryption : the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorised people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to "tap" than their hard-wired counterparts.

Full-Disk Encryption (FDE) : a process that encrypts everything on the hard disk, i.e. the media - this means that when data is saved to an encrypted disk it is encoded, all without user action. This includes the oper-

The Boss' Guide to Geek Speak

Do you speak Geek?

ating system, swap file, any temporary files and all the free space on the drive. The swap and temporary files can often leak important confidential data to a hacker. FDE also provides support for pre-boot authentication. It's an effective technique, but encryption can double data access times, particularly when virtual memory is being heavily accessed also, it is only effective if the machine is switched off. With FDE, only one key is used to encrypt the entire disk. Usually keys are stored on the local system, and their sole protection is typically the user's password or passphrase. And we all know how weak they can be! FDE does not protect against the most damaging breaches posed by an authorised user who has "legitimate" access to sensitive information who either accidentally or maliciously chooses to misuse or leak that information.

Full Data Encryption : full disk without the risk – only encrypting the data, not the media it is saved to. Encryption can take place whether data is on a desktop, laptop, PDA, or USB stick and it's granular, so administrators can set policies to determine which data is protected and against whom. As FDE uniquely protects individual users' data, without interfering with the other operational processes (upgrades, patches, etc) that need to be done, it protects against the internal threat and provides lower TCO.

IDSes (Intrusion Detection Systems) : pretty much what it says on the tin detecting potential intrusions.

IPS (Intrusion Prevention Systems) : a pre-emptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. Intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator.

VPN (Virtual Private Network) : a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunnelling protocols such as the Layer Two Tunnelling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

NAC (Network Access Control) : a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that comply with a defined security policy. NAC restricts the data that each particular user can access, as well as implementing anti-threat applications such as firewalls, antivirus software and spyware-detection programs.

DLP (Data Loss Prevention) : security products that focus on keeping sensitive enterprise data in.

PKI (Public Key Infrastructure) : enables users of a basically unsecure public network, such as the Internet, to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

The threat against laptops and mobile endpoints is real and you need to arm yourself against data loss! Don't let a language barrier come between you and the team trying to present you peace of mind.