ISSUE
02
SEPTEMBER
2010

TechCorner

this issue

Exploring network & computer security

Computer security is a very interesting topic as there are so many different angles and approaches you can take along with all the various technologies you can implement but at the end of the day security is not black and white.

You may be wondering why we have made such a statement at the start of this article, but I promise all shall become clear. With security, we have said that it is “not black and white”. This is for the simple reason that there is no definitive right or wrong way to protect your system. This is because there are many methods and practices that work for all businesses but, “one size does not it all” hence the statement.

What security should we implement? Well this is the magical question and takes planning to answer, as the security should be based around how you:

1. Use your systems
2. Where they are stored
3. What cost / overhead it place on your business and its operation.

When planning your security you, do not just need to look at the electronic threat and protection but also the physical threat and protection. With this in mind we would always start with what we class as the basics, like a lockable door on the office and server room followed by alarms.

We start like this because you would have to get passed both of these before getting physically near a desktop or server allowing an attempt at passwords etc.

In this article we have tried to give you a brief overview of the different classes of security and what types of protection that can be implemented. This article does not list all possible solutions and is not designed to specifically implement anything discussed; but instead raise awareness of the possible problems and solutions you can have.

The different layers / classes of security covered in this article are: -

- Physical Security
- Computer Security
- Perimeter Security
- Mobile Computer Protection
- Data Protection

We hope this article raises a good awareness of the possible threats and some of the possible solutions in helping to keep your business and staff safe.

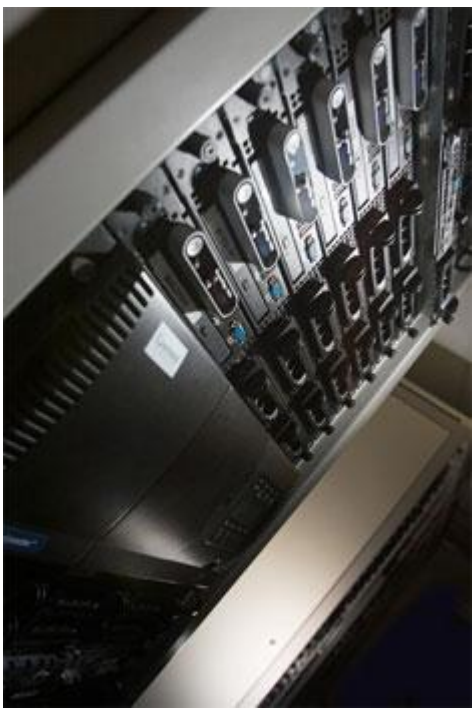
strobeIT

Physical Security

When looking at security you first must look at the basics and what can easily be done.

Physical security is based around breaking and entering or possible unauthorised access to working computers and the network via your premises.

This type of security is not just aimed at outsiders to the business but also employees.



Servers, networking & routers
Servers and switches are the core of most companies' networks holding all their data and controlling the security / access to that data, as they play such an important role they should be protected.

- Secure room – Servers (and networking if applicable) should be stored in a locked room with restricted access to keys
- Cabinets – Edge networking switches / devices should be in secure locked cabinets
- Temperature control – Servers generate a huge amount of heat and some form of temperature control like air-conditioning would help keep the machines at an optimal temperature meaning the life of the device will be extended.

Building / Office Access
Access to the company's offices or building is a great way of limiting people getting at your hardware / data. This could be as simple as an employee within the company not having access to a different department's office.

- Keys / Security Cards – These forms of locks can control access to different areas of the business.
- Alarms – Secures a building from unauthorised access.
- Security Cameras – Cameras are a very good method of protection. They provide an immediate visual deterrent but, they also provide valuable evidence should a break-in occur. In the modern computer world these cameras can work on your existing IT infrastructure and integrate on your network meaning they can be accessed by a PC on a secure connection day or night from anywhere.
- Security Guards – Depending on your type of business security guards may be required to monitor the in / out activity of staff and customers.

Computer Security (Internal Security)

This type of computer security is based around someone being in one of your offices and having access to either a computer, network data outlet or broadcasted wireless network.

User authentication via username & password

- Usernames and passwords via a central managed authentication system like Microsoft Active Directory should be in place to control user access and rights to the computer and network resources.
- Technologies like finger print or smartcard can auto enter details
- Passwords should be complex - eg. 8 characters long with numbers and letters (some systems can enforce this upon users)
- Passwords should be changed on a time basis (Some systems can enforce this)

File Location

- Mapping drives to secure shares on your server so data is kept in a central secure area.
- Redirect special folders like “My Documents” to secure areas on the server.
- Use server based versions of data applications like SQL

File Permissions

- Correct / structured filing system to reflect your business, so permissions can be applied
- NTFS / Share (Server Message Block [SMB]) security permissions assigned to server shares, allowing only the required groups or users access to the files.
- EFS (Encrypted File System) with NTFS for file / folder encryption.
    - EFS integrates in with Microsoft Active Directory to give seamless encryption for files and folders within the business.
    - EFS only works with shares / drives formatted with NTFS. Encrypted files copied to NFS or FAT based drives are decrypted and then saved.
    - EFS does not work with Mac based clients
    - EFS adds a CPU overhead to the server & client accessing the file.

Network Security

- 802.11x network authentication.
- IP communication security like IPSEC.
- MAC address / Device access limitation (This can be a huge administrative task)
- Wireless encryption – Secure wireless connections using WEP or WPA etc
- Not broadcasting your wireless network.

Perimeter Security

This form of security is based around electronic / cybercrime and how you can protect you, your staff and the data they access.

Depending on your business and how secure you would like to make your system will determine what you class as a perimeter and what protection you put in place.

Traditionally perimeter security is all based around protecting your business from the internet by the connection to your ISP (Internet Service Provider).

With security required to stop so much more we class perimeter in a different way. We look at a perimeter as any exit / entrance to your machine / network, so a computers LAN (Local Area Network) connection is a perimeter to that device for example.

Below is a list of technologies and what they protect against and how.

Desktop Anti-Virus

- Scans files and folders accessed or created by the computer to make sure infection free.
- Email scanning - protect your inbox from infection
- Spam / Phishing filtering – protecting your inbox from false email trying to get your information by deception.
- Internet / network traffic scanning – protect network traffic from infection

Desktop Firewall

- Stops unwanted traffic from getting to the PC
- Application control for controlling what applications can use the network to communicate

Content filtering / Blocking

- Desktop website filtering / blocking – Stops content from being displayed / accessed at the users' desktop.
- Gateway or Router content filtering / blocking – Stops content from entering your network at source.

Gateway or router Protection

- Virus scanning – Stops infected traffic / emails entering your network.
- Firewall – Stops unwanted traffic and hackers entering your network.

Mobile Computer Protection

F-Secure

Mobile Security

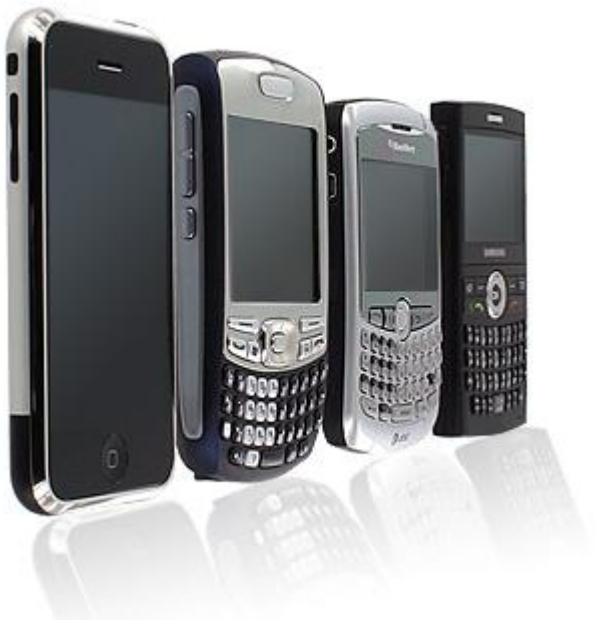
F-Secure Mobile Security is a complete security solution for your smartphone. In the unfortunate event your phone is lost, stolen, infected by mobile malware or even spied on, Mobile Security helps to safeguard your personal and confidential data. The new Browsing Protection feature identifies which websites are safe to enter and which should be avoided. Harmful sites are blocked automatically to ensure safe surfing. With the help of the new remote GPS locator feature, you always know where your phone is located. F-Secure Mobile Security makes your smartphone completely safe for today's connected life.

Anti-Theft for Mobile

Anti-Theft is a free application to your mobile device that provides a great way to protect your phone if it gets lost or stolen.

* Not for iPhone

Mobile computer protection is a big topic; and the title maybe misleading as this does not just cover your mobile computer, but also covers the protection of Smart phones, PDAs (Portable Digital Assistant), USB memory sticks and other such mobile products that can store data about you and your business.



Smartphone
As the world is getting more technologically advanced we are able to take our office with us in many ways, one of the most common ways is email via a mobile phone. Email is not the only way but device that do this like Apple's iPhone or a Blackberry our classed as a "Smartphone".
These devices are basically small computers and have all the same security risks, here is a list of possible protection methods: -

- Pin / Password
  Prevents access to phone
- Firewall
  Stops hackers and unwanted traffic across Bluetooth and other connections
- Anti-Virus
  Protects against infection
- Anti-Theft
  Uses GPS to provide txt message to allocated number with location or wipe sensitive data from device.

Other
Unfortunately the list of portable devices is only getting bigger as technology advances. The main category is portable storage like an external hard drive or a USB pen drive.

The majority of these devices are just dumb storage systems only; which with the right setup can be encrypted to prevent access without the correct password etc.

Becoming more and more available are external hard drives with pin codes / finger print protection built-in to the casing which links to an internal encrypted system or similar protection.

Laptop
As these devices are mobile computers they not only have the security issues covered in "Computer Security" but now also come under threat of being stolen and lost to gain access to possible data stored within.

Depending on your setup two other technologies can be enabled to help fight against this: -

- Redirected folders with mobile computers gets cached so can be accessible while away from the office, by default this CSC (Client Side Caching) folder is encrypted
- Full HDD encryption (using products like Microsoft BitLocker and TrueCrypt)

strobeIT

Data Protection (Redundancy)

Data protection is one of the most important topics, but unfortunately is the topic that gets most over looked especially by the small business. This form of protection is not so much against the criminal but more against the accidental deletion, office flood, fire or even a hardware failure.

Backup
A backup is an off-line / not active copy of your data which can be used if necessary to recover your data. The following should be true of your backup system: -

- Minimum of a daily backup
- External Media (Tape, online)
- Off Site storage to protect against a natural disaster

RAID (Redundant Array of Independent Disk)
RAID is a technology that enables the server or a NAS (Network Attached Storage) device to use multiple hard disks in a fashion to provide anything from performance to data protection, here are a list of the most common versions: -

- RAID 0 (Striping)
  [*Block-level striping without parity or mirroring*]
  Uses multiple disks as one hard drive with no redundancy / fault tolerance

- RAID 1 (Mirroring)
  [*Mirroring without parity or striping*]
  Writes the same data to 2 or more disks protecting against disk failure.

- RAID 5
  [*Block-level striping with distributed parity*]
  Writes data across most of the disks and then creates a parity / check file on the final disk, this gives the system performance but also disk failure redundancy as the file can be generated using most of the file and parity bit.

We at Strobe IT hope this article has been a useful guidance in the world of security.

Robin Toy
robin@strobe-it.co.uk

UPS (Uninterruptable Power Supply)
UPS is an electrical apparatus that provides emergency power to a load when the input power source, typically the utility mains, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide instantaneous or near-instantaneous protection from input power interruptions by means of one or more attached batteries and associated electronic circuitry for low power users. The on-battery runtime of most uninterruptible power sources is relatively short but sufficient to allow time to bring an auxiliary power source on line, or to properly shut down the protected equipment.

Fireproof Safe
This may not sound too complicated but can provide very good protection, a list of reasons for having a safe are: -

- Protects against natural disasters like fire and floods

- Keeps data / documents safe and secure from thieves

- Server CD's & License – Keeps safe your CD's & licenses that are required to keep your server up and running.

- Desktop Applications – Without the applications your business cannot install / move or upgrade so storage of your CD's and licenses is advisable.

- Backup Media – While backup media is on-site, keep it safe and secure.