

## Network Security Basics for SMEs

*Network security is about prevention not cure. Yet, a staggering 85% of network attacks penetrate successfully through vulnerabilities for which patches and updates have already been released\*. Many small and medium businesses (SMEs) fall into the trap of not taking adequate precautions because they think the threat is highly exaggerated and they do not hold any critical data.*

While it is true that high profile security breaches involve the unauthorised release of confidential data, the reality is that most systems are not compromised for the data they contain but for other purposes such as being used as zombies in large scale attacks and even to send SPAM.

A common misconception is that hackers spend their days typing in credentials into log in screens until they guess it right. In fact, most attacks are performed using automated tools which exploit known vulnerabilities in operating systems and applications. A “dictionary” attack can bombard a password field with thousands of dictionary words at the click of a button. The threats to network security are numerous and relentless; keeping abreast of them is no easy task that requires a thorough approach and in depth technical knowledge.

### Top 5 threats to SME data security:

1. Automated exploit of a known vulnerability
2. Malicious HTML email
3. Reckless web surfing by employees
4. Web server compromise
5. Data loss on a portable

Network security is not available as a single product. Instead it is about combining multiple security elements, such as antivirus products, firewalls, internal policies, etc. into multiple layers of defence. It is critical to secure all possible loopholes - it is no good having a well configured firewall if network account passwords are simple dictionary words.

Best security practices involve a combination of both technical controls and logical processes. It is easy for bad processes to undermine otherwise excellent products and vice versa, good practices can compensate for shortcomings in bad products. At the network level, the following are some of the security elements that form the basis of a good security defence:

- Updated and patched systems
- An antivirus solution with up to date definitions
- Properly configured firewall
- Use of complex passwords
- Intrusion detection systems
- Good internal security practices

Many SMEs incorrectly believe that good security finishes with installing a firewall and an antivirus product. Unfortunately, it is not as simple as that. Virus attacks represent only a small part of many other security threats, e.g. malware, insider attacks, reckless web surfing by employees and even multifunctional printers. For example, unless configured properly a networked printer is just another potential route for hackers to get in.

The cost of a security breach can outweigh by far the cost of the solution. For many SMEs the task of securing their network may seem beyond their IT budget. However, some of the security elements above are just common sense, e.g. internal policies, and others are available for free through open source software. A good network security solution does not have to cost the earth so there really is no excuse for not taking security seriously.

\*Gartner Research