Keyloggers – your security nightmare ?

The House of Commons takes security seriously, with metal detectors, body searches and rather large numbers of gun-toting police officers. So the recent security breach by a six-year old schoolgirl called Briannagh must have caused more than one red face.

Sacha Chahrvin of SmartLine Inc; takes a look at the incident…

Briannagh, in an experiment for BBC South, managed to get a keylogger past the security guards and, while an MP left her office unattended for 60 seconds, attach it to a computer.

Briannagh is a typical six year-old, with all the knowledge of sophisticated computer hacking techniques that a six-year old normally possesses. Yet she managed to infiltrate one of the world's most secure buildings, and attach a bug to a sensitive computer without raising a single alarm.

This story shows how the line between physical and IT security is becoming blurred with the proliferation of hardware keyloggers. These devices – rather than the software versions that arrive via a Trojan or spyware-infested spam - are fast becoming the weapon of choice for today's high-tech gangster.

Keylogging as a technique isn't new. Nicodemo Scarfo Jr, of the New York and Philadelphia organised crime families, was brought down by the Magic Lantern keylogger that the FBI installed on his computer via a Trojan. The Magic Lantern recorded every keystroke made and sent the information to the Feds – who were then able to piece together enough evidence to indict him for running an illegal gambling ring and loan sharking.

Concerns were raised at the time about computer privacy, but as the nature of keyloggers, and those who use them, has changed it serves as a useful reminder that there is a positive side to keylogging. But it is the darker side that is more familiar to the majority of IT and security professionals.

Whether used as a tool for industrial espionage, accessing government data, or simply stealing an individual's personal financial details, keyloggers pose a serious threat. They can damage business relationships, financial standing, and reputation. They can even cause an organisation to breach major pieces of legislation such as the Data Protection or Sarbanes Oxley Acts.

Any individual or organisation that accesses private information is vulnerable – as the House of Commons has discovered.

So how do machines become infected by keyloggers? Traditionally, they were pieces of software installed on a computer through a virus or as spyware. For the criminally-minded, software keyloggers have the significant advantage of being able to infect a massive number of machines and gather the data quickly, easily and remotely.

But IT security systems have done a good job at keeping up with software keyloggers and detecting them. Up-to-date anti-virus and anti-adware tools can prevent Trojans and spyware entering the system in the first place. And should a keylogger slip through the net, standard monitoring tools can detect and remove them.

As software keyloggers are being detected and removed almost as quickly and easily as they were being installed, criminals have done their best to find new ways to breach security measures. This has, in turn, led to the latest breed of hardware keyloggers, which are much harder to detect as they do not install any code onto the machine and cannot be spotted by traditional anti-virus or anti-spyware tools.

The most common form of hardware keylogger is a small device installed at the back of a PC between the keyboard and its connection to the machine. Happily, this type of device is also the easiest to detect visually – provided you know what to look for.

As with all hardware keyloggers, and as in the case of Briannagh, it requires the attacker to have physical access to the computer to install and later retrieve the device, albeit for a matter of seconds. However, as social engineering skills are becoming more sophisticated, this doesn't pose a problem to the determined individual.

Other forms of keyloggers are built into the keyboard, either by the attacker simply replacing the user's keyboard completely, or by dismantling their existing one and installing the device. The former runs the risk that the user will notice that they have a different keyboard, and the latter has the downside of requiring the thief to spend more time at the machine, but for both the chances of visual or manual detection are almost zero.

All is not lost however. Companies can protect themselves, even from hardware keyloggers. They should ensure that regular checks are conducted and comprehensive employee IT training is given to raise and maintain awareness of the issue, including the threat of social engineering attacks and the different forms they can take. Certainly in large organisations it isn't practical for the IT security manager manually to check the back of every single box and every single keyboard. However, if users are able to carry out basic monitoring of their own equipment, the chances of detecting these rogue devices are greatly enhanced.

Another point of consideration is the type of equipment in use. Although not immune from hardware keyloggers, laptop computers with their inbuilt keyboards are far harder to tamper with. However, it is important that the reduced threat from keyloggers is balanced against the other security challenges that arise from the use of mobile devices.

In addition, two-factor authentication devices such as secure tokens have a role to play. Because the token's passcode constantly changes, any data that is gathered by a keylogger is immediately ineffectual. It cannot be used again to gain access to the system.

Organisations should also consider increasing the use of drop down menus for gathering information, as have been adopted by some banks for their online customers. Instead of typing in information with trackable keystrokes, drop downs enable users to select characters or words with the mouse, which a keylogger cannot record.

The final nail in the coffin for hardware keyloggers are the products that have recently come on to the market that can automatically detect their presence. These software solutions can intercept and block communications to the device from the targeted computer, as well as alerting the IT department to its presence.

Hardware keyloggers are growing in popularity. According to Equifax's fraud experts there has, in fact, been a 5,000 per cent increase in fraudsters using hardware-based keyloggers to get hold of valuable information. But although these devices are becoming remarkably prevalent – Briannagh, with the help of the BBC, acquired hers on the internet for around £50 – effective security measures are a lot less common.

Companies have got to re-evaluate their security policies and training, and make sure they are are aware of the changing threats they face. Finding out that they are vulnerable after the event is simply not an option.