The Insider Threat

Monday 22 February, 2016

Media:

Related Sectors:

Computing & Telecoms ::

Related Keywords:

Data Security :: Computer Security :: Data Loss :: Data Protection :: IT Security :: Information Security :: Inside Threat ::

Scan Me:

It can safely be argued that data is one of the most important assets of any organisation, and it is for this reason that companies should invest resources in protecting it.

In 2015, 90% of large organisations reported that they had suffered a security breach, up from 81% in 2014. In a similar trend, 74% of small organisations also recorded a data security breach, also an increase on the previous year's figures.

What are the consequences? Data loss or theft can lead to reputational damage, legal issues and in the worst possible cases destroy a business. The financial damages associated with a data breach, depending on its nature, can include loss of assets, business disruption, missed sales, fines and compensation and various other costs. The average total figure for a large organisation as a result of a bad security breach can range from £1.46m to £3.14m.

The danger within

Whilst external threats such as malicious software and hacking still continue to be a risk, internal personnel are just as likely to cause a breach. 75% of large organisations suffered a staff-related breach in 2015.

Although most organisations strive to employ honest and trustworthy individuals, there is always a threat of insiders contributing to or causing a data breach. The breach can be either deliberately malicious, such as fraud; or result from negligent behaviour, fostered by a poor training, weak policies and the lack of a strong security culture. Half of all organisations who reported an inside breach attributed the cause to inadvertent human error and a lack of vigilance.

But what do companies really do to protect their information? Antivirus, Firewall – traditional security elements are not enough, and both internal and external threats must be taken into consideration. With constant technological innovation comes new risks, and technology designed to increase productivity and collaboration may cause or enable a data breach. Malware infection and data breaches can arise despite defences such as firewalls, anti-virus and intrusion prevention systems. Businesses need to stay ahead of the curve and manage the risks associated with this new technology, which includes educating staff and investing in thorough data security solutions. Without effective training and policies, mistakes and inattention can expose the organisation to countless risks.

Common techniques staff can fall victim to

- **Data loss:** Attackers can lure computer users into giving up their passwords or other sensitive information. Due to ineffective security policies and the lack of tools such as access control and encryption, control of data becomes problematic
- **Infected data devices or un controlled usage:** such as USBs, external hard drives or CDs can cause malware infection or allow staff to copy confidential or inappropriate company data
- **Mobile devices:** This is an ongoing concern for IT teams, as sensitive information can easily be transported and lost. Many mobile devices are connected to corporate networks, resulting in a lack of control over where data is being stored. 53% report there is sensitive customer information on mobile devices, and 15% of large organisations had a data breach in 2015 involving smartphones or tablets

EgoSecure is a leading provider of integrated data protection solutions.

Our data protection secures data wherever it is stored: on computers, in the cloud, on external storage media, on smart phones, tablets etc. Solutions are implemented with minimal effort and costs whilst achieving a maximum level of data security.

After analysing the data flow and identifying the weak links with our Insight Dashboard, the protective measures can be configured individually with 15 protection modules. All modules are integrated into one solution, access only one database and are controlled via a central management console. There is only one installation, after which the modules can be activated in accordance with the protection requirements. After installation, Insight continues to provide information concerning the level of protection

and therefore detects the need to adapt security measures.

The licensing model is simple, you only switch on the modules you need for the areas of risk that Insight identifies and you prioritise, and if you switch on the Green IT module the software can pay for itself

Statistics and facts come from the below sources

https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-digital.pdf

Company Contact:

Egosecure

T. 07912 097542
E. admin@egosecure.co.uk
W. https://egosecure.co.uk/

View Online

Additional Assets:
http://egosecure.co.uk/

Newsroom: Visit our Newsroom for all the latest stories:
https://www.egosecure.pressat.co.uk