BIZCOMMUNITY

# Fighting the insider threat

By Anton Vukic

24 Apr 2015

In the past, security efforts were largely focused on preventing cyber criminals from gaining access to the company network. Today, although this threat continues to be a real danger, there has been a growing focus on the threats posed by insiders. Company employees that have access to critical information and either maliciously or carelessly leak that data.

Businesses rely more and more on automated systems, and small USB drives, and these have paved the way for malicious insiders to inflict huge damage, and exfiltrate company data without anyone being the wiser.

**It can happen to anyone**

Moreover, insider attacks can be at least as devastating as external threats, and they can happen to anyone. These threats usually fall into one of the three categories: sabotage, theft of intellectual property or other sensitive data, and fraud.

These threats are particularly prevalent during tough economic times, during which organisations are forced to make cutbacks and retrench staff. This leads to a rise in the number of people who would consider stealing valuable data, and therefore a rise in malicious insider activity.

So what should IT be doing to prevent this sort of threat? The first step is knowing what your businesses' most valuable data is, the data that would damage the company the most should it be stolen - think along the lines of the recipe for KFC's eleven herbs and spices - and make sure security is focussed on that data.

Also, learn from any past attacks, as these will have shown where you are vulnerable, and what you were doing wrong. Understanding the weak points in your organisation will help the technical team put controls in place to watch for similar attacks in the future.

It is also important to understand who has access to your sensitive information. Remember, this list will include third-party business partners as well as internal employees. Make sure that only trusted parties have access, and that no-one has access to anything they don't strictly need to do their jobs. Always enforce the principle of least privilege.

## Eyes open

Next, keep an eye out for any anomalous or suspicious behaviour. The signs are numerous, and will include working unusual hours for no reason, unnecessarily copying data they don't need, disregarding company policies about installing unauthorised software or applications, and trying to access restricted areas on the company network.

Be particularly vigilant when it comes to staff who have resigned or are about to be terminated. Research suggests there is a window during which most insider attacks take place, and that is within 30 days of handing in a resignation, on either side.

Another way to stop the insider threat is to have data leakage prevention (DLP) and other technologies that focus on preventing the leakage, accidental or deliberate of company data. An example of this would be centralised logging tools that are designed to look for any signs that data is being exfiltrated, or emails sent outside the organisation that are of an abnormal file size.

Perhaps the most vital measure businesses can introduce is to have a programme in place to deal with the threat. Get senior managers involved, put best-practices and plans in place to deal with and mitigate these threats. Technology on its own cannot hope to block all these attacks. A combination of proper policies and procedures with awareness and having an action plan already in place, allows companies to quickly prevent or these attacks.

## ABOUT ANTON VUKIC

General Manager at First For Phoenix

- Pros and cons of hosted and on-premise storage - 3 May 2016
- Remain POPI compliant with DLP - 11 Jan 2016
- Home automation: our homes are getting smarter - 2 Nov 2015
- Fighting the insider threat - 24 Apr 2015
- On-the-go power - 12 Mar 2015

View my profile and articles...