Who's stealing whose software?

Published: 5 February 2016
Published by: https://digitalisationworld.com/subsection/28
By: Mark Warren, Perforce Software

Some steps towards protection against IP theft.

Much has been written in recent years about the security risks that the 'insider threat' presents, such as introducing viruses and obtaining financial information or funds. Now there's a new worry: using cyber-attacks to steal IP (intellectual property). Statistics suggest this is a very real threat. For instance, a Kapersky Labs survey across 27 countries found that just over one in five global organisations had experienced a loss of intellectual property during a cyber-attack.

The impact of software IP theft can be huge, whether you are a computer games company that has had its code stolen by a rival in China, or a financial company about to introduce a new service, or a manufacturing firm that was about to launch a product but finds out its engineering assets have been replicated by someone else.

A case in point is one of the world's largest chip manufacturers, which knew it had a security breach but couldn't prove the source, even though it had spent $1 million with a global IT consultancy to get the bottom of the problem. The answer finally lay in applying behavioural analytics to the company's code records.

More on that later, but back to what the challenge is here. Traditional software tools are typically focused on the perimeter, in other words, 'keeping the bad guys out', but there needs to be a realisation that it is impossible to keep the corporate walls 100 per cent infallible. Developing a better understanding of what is happening within the organisation is also vital, particularly because such a high percentage of security breaches – whether to obtain IP or for other nefarious reasons – are caused by insiders, whether accidentally or deliberately.

Privilege management – in other words, who has access to what – can contribute to the problem. Some employees tend to have access to more confidential data than others, including the software development teams, the very people who are creating those incredibly valuable software IT assets. Most existing SIEM tools find it hard to investigate what is going on in the software development environment, largely because of the isolated way in which these individuals work, with processes and tools that are not shared with the rest of the organisation. Plus, code repositories typically do not lend themselves to close scrutiny.

This is why more organisations are not only taking this area of risk more seriously, they are also approaching the problem in more creative ways. In particular, they are looking at the behavioural and activity patterns of people, rather than focusing on the data. Let's go back to that well-known chip manufacturer: once it applied behavioural analytics to the company's version management (a.k.a. source code) log files, within two weeks, it was able to confirm the

two suspects and in addition, identified a further 11 software developers who had also been stealing code from their employer.

Behavioural analytics sorts through all the security 'noise' and calculates where are the most likely risks residing, or more accurately, who are the most risky employees, whether in software development or another department. This technique scrutinises two factors: unusual patterns of activity and personality types. For instance, behavioural analytics tools will automatically pickup when someone is checking out code files at odd times outside the normal working day, or checking out large files and then not checking them back in, or someone who does not need that kind of information as part of their job.

Behavioural analytics also evaluates whether this person has any other risk factors, for instance they might be about to leave the organisation (a Symantec study found that 56 per cent of workers believe it is acceptable to take data with them and use it at a competitor), or have recently been passed over for a promotion.

Of course, many security incidents are the result of someone hacking or impersonating a legitimate employee without their knowledge. Careless employees who move data to insecure working locations are renowned for creating security holes and have allowed a piece of malware to be downloaded. There is a good chance that before long, an external third party is in the system, but the good news is that they will probably trip themselves up, if behavioural analytics are applied.

Of course, traditional security tools are still needed and more organisations are applying a multi-layered approach to managing security risks, looking at a gamut of tools, rather than a single solution. While it is early days for behavioural analytics, indications are that it is set to earn its place in the security landscape as part of a more robust approach to managing the insider threat.

Submitted by: Ruth Edge – Cardinia Shire Council