Why the biggest threat to your organisation may already be inside

Why the biggest threat to your organisation may already be inside

*by **Mark Walmsley**, **CISO, Freshfields Bruckhaus Deringer LLP** and Chairman of the steering committee for Cyber Security Connect UK 2018*

For many years, the idea of cyber security has been synonymous with defending a network's perimeter from external threats. Over the last 18-24 months, however, we have seen a major shift in the threat landscape, with perimeter protection growing steadily less relevant.

While a strong perimeter is still necessary to protect from the countless low-level attacks hitting companies every day, it is no longer effective against most advanced threat actors. Defences are increasingly bypassed by tactics such as attacking through a supplier or tricking employees with social engineering.

It is also increasingly the case that a security incident will be caused by someone already inside the network perimeter in the form of a malicious insider. The idea of the insider threat covers a wide range of motivations, actions and outcomes, but all boils down to an employee abusing their privileged access to misuse corporate information.

Who is behind the insider threat?

As with most illegal activity, malicious insiders are often motivated by the chance to make money or further their personal agenda. There have been several high-profile incidents in recent years, such scientists stealing high value pharmaceutical trade secrets with the aim of setting up their own company. In another example, a financial services employee stole data relating to thousands of clients and copied it to his home server to use as leverage for potential employers.

Most insiders are not nearly so ostentatious however, and it's more common to find that they have taken work they have completed or contacts they have built up. While much less damaging than cases of thousands of files being stolen, these incidents still often include mission critical data and the user may not be aware of the damage they could cause.

Alongside these more mundane cases, we are also seeing an increase in the use of insiders for concerted cyber-attacks. Adversaries may plant an individual within a large organisation or governmental body or seek to turn an existing employee through bribery or blackmail. Rival corporations, nation states and organised crime groups may all use this tactic to gain an advantage through stealing secrets or by disrupting an organisation's operations.

Security within the perimeter

Whatever shape it takes, defending against an insider threat requires an understanding of what is going on inside the network and should seek out unusual activity that could point to malicious intent. Human actions are much harder to categorise and anticipate than malicious software, and the best way to identify and prevent potentially harmful activity is via behavioural analytics. This approach uses machine learning to analyse our behaviour across the organisation and creates a model of what normal activity should be.

Once this is established, anything that falls outside of expected behaviour can be quickly identified. The best solutions can achieve this almost instantly, while connecting the dots to other activity that might point to a wider pattern of activity. This also makes behavioural analytics useful for spotting signs of advanced cyber attackers who have compromised a user account.

Finding the right solution

Behavioural analytics is a complex field and organisations should not simply rush out and purchase the first solution they see. The need to monitor user behaviour for signs of threats must be finely balanced against legal and ethical rights to privacy. International businesses should be aware of the differences between countries, such as the works councils in France.

Careful consideration is also required when selecting a solution. There are some very powerful tools on the market, and it can be tempting to rush out and invest in the most formidable one available. However, this often leads to the solution going to waste as the company fails to integrate it with the business and uses only a fraction of its capabilities. The equivalent would be buying a top-of-the-line F1 racing car and using it to drive to Tesco once a week.

Instead, companies need to first work out what their business needs are and define the outcome they want to achieve. From here, they should do their research and investigate multiple solutions before deciding. The complexity of the subject means it is often beneficial to take on a consultant or reseller with the knowledge and industry contacts needed to find the best match.

I anticipate the rapidly-evolving insider threat and the challenge of finding the best solution being one of the major areas of focus at the Cyber Security Connect UK event later this year.

---

https://www.cybersecurityconnectuk.com/News/Cyber-Security-Connect-Blog/Why-the-biggest-threat-to-your-organisation-may-already-be-inside

by **Mark Walmsley**, **CISO, Freshfields Bruckhaus Deringer LLP** and Chairman of the steering committee for Cyber Security Connect UK 2018