Security tips in the age of data leaks

By Doros Hadjizenonos

18 May 2016

On 3 April 2016 a collective of international newspapers and the International Consortium of Investigative Journalists (ICIJ) dropped a bombshell - they had millions of documents showing the private business dealings of thousands of people, many of whom were famous or politically powerful, and many of which revealed hard evidence of tax evasion.

©spaxia via 123RF

The law firm that helped these people hide their money, Mossack Fonesca, had suffered a data leak like never before seen. In the weeks since, revelations continue to pour out, ruining reputations, sparking political resignations, and prompting further legal and regulatory investigations.

While exposing corruption and tax evasion is obviously for the greater good, it must be acknowledged that a leak on this level is the stuff of nightmares for enterprise security professionals the world over. If there is one thing the Panama Papers has taught us, it is that we are living in the age of data leaks. If the Wikileaks and Ashley Madison scandals (among others) hadn't already convinced you, it is hard to argue with the 2.6 terabytes of data leaked in this instance.

It's not just the embarrassment factor to consider. Even if your company has absolutely nothing illegal or unethical to hide, there are often trade reasons to keep certain information behind lock and key. Furthermore, if you hold customer information, a breach has much broader implications. US retailer Target discovered this to their detriment after thousands of customer credit card details were stolen from them, and those customers understandably began to claim for damages and compensation. So even if you're one of the good guys, you have a number of important reasons to ensure your data is secure.

Here are our top five tips for avoiding a data leak and ensuring the security of your company systems:

1. Integrated threat management

It seems obvious, but is often overlooked or underestimated. You cannot monitor or protect devices you don't know about, and you need to have an over-arching view of your systems for effective management. An audit of your entire system is a starting point. Then, as we've said before, security challenges are increased when there is a lack of proper visibility for incident detection and response. We highly recommend the use of a single, visual dashboard for event analysis, threat monitoring, and mitigation. This important intervention helps you to ensure full-spectrum visibility into threats across the

organisation.

2. Review your weak points

Linked to the above, but at the level of the next layer, we suggest you regularly review your security implementations and solutions to spot any weak spots. If your team is skilled and has capacity, a regular internal review is recommended. An occasional external review from security service providers might also provide a second opinion or different perspective. It is important to approach this task with an open mind, otherwise you may be so focused on securing the C-suites laptops that you forget the boardroom printer that runs off the wireless network with very little built-in security.

3. Unified policy management

What are the policies you have in place in your organisation? How relevant to the new connected ecosystem are they? Do they address cloud or bring your own device? Are they enforceable? When policies are misconfigured or patchy, your business cannot effectively protect (and enjoy visibility across) business segments, and that’s risky for the organisation as a whole. The strength of your security architecture thus relies on the use of an efficient operational solution.

4. The power of auto-pilot

Given the complexity and breadth of our systems today, relying on manual intervention on all IT matters across all levels is setting yourself and team up for failure. Certain operations and responses can and should be automated, freeing up your human resources to focus on critical systems and high level threats.

5. Consolidate solutions

With a proliferation of new solutions coming to market, many with a single case or niche focus, it is easy to complicate your protection to the point of becoming wholly unmanageable. Security complexity can be addressed through consolidation. Bring all your security protections and functions under one 'umbrella'. A consolidated approach, supported by a single platform, should give you more control over your security, as well as offering insight into their security health. Finally, a consolidated solution also enables agility and threat responsiveness across the environment.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...