BIZCOMMUNITY

How to avoid disaster in the wake of Spectre and Meltdown

By Colin Thornton

23 Jan 2018

Earlier this month, while the majority of South African business owners were still enjoying their summer holiday, the global technology industry suffered a rather devastating blow. Two major security vulnerabilities, dubbed Meltdown and Spectre, were discovered in the central processing unit (CPU) chips that power most of the computers in the world.

Essentially, these hardware vulnerabilities allow programs to steal data that is currently being processed on computers. While programs are typically not allowed to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of sensitive information stored in the memory of other running programs.

This might include, for example, your passwords stored in a password manager or browser, photos, emails, instant messages – and valuable intellectual property that sits within a business.

Bugs in modern computers leak sensitive data

9 Jan 2018

According to researchers, there is no simple fix for Spectre, which could require redesigning the processors. With regards to Meltdown, the software patch needed to fix the issue could slow down computers by as much as 30% — which is not the news that time-strapped business owners want as they settle into a new year of work…

Is your technology ‘house’ in order?

While it is certainly bleak news, the Meltdown/Spectre debacle serves as an important wakeup call for business owners and managers everywhere.

The reality is that any business can be affected by any vulnerability - at any time. This applies to businesses that employ less than five people and extends to multinational corporations.

So, while Meltdown and Spectre are hot off the press, new vulnerabilities and flaws are actually being uncovered all the time.

The critical takeout here is to constantly invest in robust internet security. It is useful, perhaps, to compare your business to your residential home. As a homeowner, you probably take basic precautions and invest in things such as burglar bars, alarms, armed response, security guards - and of course – insurance!

Booby-trapped messaging apps used for spying

22 Jan 2018

Your business requires the same approach - and you can do this for your enterprise systems and infrastructure in various ways. For example, next-generation firewalls such as SonicWALL are the technology equivalent of burglar bars. They are a serious deterrent, and your first line of defence against intrusions from outside (or even inside) your IT network.

Secondly, anti-virus systems like ESET Nod 32 are similar in nature to home alarm systems. They notify you when a vulnerability has been detected, and then hold it in quarantine until you decide what to do next. Thirdly, patch management can be likened to home security guards. When a vulnerability is documented, the installation of patches ensures that your systems are no longer vulnerable. And last (but not least), backup software like RedStore or Symantec backups serve as your insurance. They allow you to recover your data more easily after an attack or incident, and to minimise any downtime in the interim. Without the insurance of a backup, your data will be lost – which often has a crippling effect on a business.

Internal awareness and education

> *In addition to investing in the right internet security tools and platforms, driving awareness and education within your business is imperative.*

Ultimately, employees and staff are the real frontline soldiers. Often, they are the ones to fall victim to spam and malware – and are very likely to be targeted more frequently than owners and managers.
As a result, savvy business owners must invest in the education of employees and managers around internet security, ensuring that they fully understand the threats – and how to identify them.

Looking ahead, here are some quick tips to ensure that you enter the year with robust security in place.

- Ensure all software and anti-virus programmes are up to date
- Pay attention to detail! (Does the email look trustworthy? Is it threatening in nature? Can I verify the sender?)

- Ensure that backups are *always* up to date
- Bookmark your favourite (and important) websites to ensure that you don't click on a link that is not real
- Beware of enticing 'pop-ups'

Finally, it is important to note that businesses that do not have an existing engagement with an IT company/consultancy will definitely be at a higher risk of falling victim to attacks and/or hardware vulnerabilities.

Regular engagement with IT professionals keeps business owners abreast of key trends and threats within the technology environment. This doesn't necessarily mean that you need to take on a support SLA, but it does mean that an engagement (at the very least) bi-annually is required with a company which can complete a security assessment and provide objective reports on the risks within your business.

ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SME's is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...