BIZCOMMUNITY

Are you leaving the front door open for cyber criminals?

By Aaron Thornton

16 Oct 2019

Are you careful about keeping your front door locked and garage securely closed? Do you switch the home alarm on at night before dozing off? Yep, we thought so. Crime is an ugly reality that we all have to face daily, and most South Africans are extremely cautious and vigilant about their home security. Pity that the same cannot be said for internet and data security...particularly given the fact that current cybercrime statistics are just as shocking as 'physical' crime stats!

Aaron Thornton, managing director, Dial a Nerd

Not convinced?

The global Cyber Exposure Index ranks South Africa sixth on the list of most-targeted countries for cyberattacks, while PwC's 2018 Global Economic Crime Survey ranked cybercrime as the second most frequently reported type of fraud (and identified it as the most disruptive and serious economic crime expected to impact organisations in the next two years). Now, this is where we can hear small business owners and home-based professionals mutter to themselves, 'ah but I'm a small fry...hackers have no reason to target me, I wouldn't be on their radar.'

Are we right?

Thought so, and this is why your approach is so wrong!

Hackers are well aware that SMEs and home users don't have the same IT security resources as their bigger counterparts, which makes them easy targets. Furthermore, many of today's cyberattacks are automated (and there is no hooded hacker with a funny accent sitting in a dark room focused on you…instead, millions of infected emails are being spammed into the World Wide Web every minute of every day).

So, if someone within your business (and obviously on the network) clicks on what they think is a legitimate attachment to an email, they'll unwittingly allow malware - often in the form of ransomware - to run.

In fact, Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every 14 seconds this year, and every 11 seconds by 2021. For the uninitiated, ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.

Sadly, while SMEs and home users spend scarce resources on electric fences and security guards, they invest next to nothing in IT defences and data security (and leave themselves shockingly vulnerable to crimes that can cripple the business with one dodgy link!).

Rethink your 'security' equation

Now that you've been sufficiently scolded, we hope that your next move will involve giving your IT setup a rethink! Yes?

The smartest approach is always a proactive one. Moreover, IT and data security is not a quick, once-off box to tick. It requires a thoughtful and professional strategy, as well as continuous 'maintenance' and double checking.

As a fundamental guideline, every business should adopt a 'layered security' approach to their IT system and user network. This is a gradual and systematic approach that is made up of many layers. When properly and professionally executed, it creates a robust system of defence that is effective in mitigating the severe risks that cybercrime presents today.

Of course, every home and business has a budget to operate within, so we do understand that resources have to be managed. That said, we do strongly suggest that you try to implement every layer detailed below (each layer is equally important) in order to keep the business, its employees, and its data, safe:

- **Endpoint Security**: Only use licensed software, and keep all software up to date! This will ensure that security flaws and "back doors" are controlled and patched by the creators of the software. Use a reputable anti-virus and make sure that all devices on the network have robust anti-virus protection.

- **Education & User Guidance**: Proactively educate and train all users and employees to ensure that they understand the cyber risks (and the importance of adherence to rules). Training should help users to identify and avoid threats. In addition, implement professional policies and procedures around data security that oversee how data is stored, shared and used within the network.

- **Network Security**: Hardware such as firewalls and other tools that manage access to IT infrastructure are critically important and cannot be overlooked.

- **Contract Support**: In many instances, businesses now require 24/7 helpdesks and IT support in order to properly address crises such as data breaches and ransomware attacks.

- **Server and/or Hosted Security**: Use internationally recognized cloud platforms such as Microsoft's Office 365 to

house and control your email, document collaboration and data repositories. Microsoft continually upgrades and invests in spam filtering, phishing detection and other cyber attack defences.

- **Disaster Recovery**: Something will go wrong eventually; with the support of your IT partner, have a plan in place that will mitigate risk, reduce business downtime and get systems back up (with data accessible) in a timeframe that is suitable and affordable.

Stay compliant

While your business or home network might not have suffered a data breach or attack to date, it is sadly just a question of 'when' (not if!) you will be targeted. You simply cannot afford to ignore the risks, no matter how tough the current economy may be!

Indeed, business owners also have to consider the legalities around data protection, with new legislation such as PoPI (SA's Protection of Personal Information Act) and Europe's GDPR presenting severe penalties for entities that do not comply.

So the next time your house alarm goes off (or when you hear those armed guards investigating next door's alarm), let it be a sharp reminder to check your IT security and make sure that your virtual front door is secure!

ABOUT AARON THORNTON

Managing Director at Dial a Nerd
- #BizTrends2020: SME technology in 2020 - a path to efficiency - 6 Jan 2020
- Are you leaving the front door open for cyber criminals? - 16 Oct 2019
- Why tough times call for technology-led innovation - 10 Sep 2019
- What every business owner should know about migrating to the cloud - 3 Aug 2018
- Three security issues to consider when using public Wi-Fi - 20 Apr 2015

View my profile and articles...