BIZCOMMUNITY

Are we safe and secure?

By Johann van Rooyen

28 Jan 2019

The world used to be a dangerous place. From roaming animals to unsafe food, untested products and cars without seatbelts or hardly any safety features at all. Riding motorbikes without a helmet was the most natural thing and most of us reading this can remember riding our bicycles without a helmet. You never see a kid without a helmet on a bike anymore. We can't deny it, the world has become much safer ever since safety and security became a selling point, thankfully.

Johann van Rooyen is cybersecurity specialist at Green Enterprise Solutions

Products are now rigorously tested and require a certain rating or certification to be allowed to be sold to the general public. These rules and regulations even stretch to ICT. There are rules and regulations that keep your data safe. Companies are required by law to have robust safety features like firewalls, anti-virus software and back-ups in place.

Last year’s General Data Protection Regulation (GDPR) is a prime example of companies, organisation and government entities needing to protect users data. However, this is costly and does it really matter in Namibia? It does, imagine your banking data, or even your billing information for your mobile phone or electricity being available to a hacker, or medical information.

Besides, most companies and organisations believe they have everything in order. However, as we know, an organisation or its security and especially online is only as strong as its weakest link. That’s where something like penetration testing comes in. Penetration testing is essentially trying to figure out to how to penetrate your own ICT-environment. Basically trying to hack or enter into your ICT-network by exploiting security loopholes found through various means. This is also called ethical hacking because it necessitates permission from the target.

Penetration testing surveys and analysing weaknesses that might be used and exploited by criminals to steal data, money or perhaps blackmail an organisation. Everyone’s information is online somewhere if it’s not properly tested it can fall into the wrong hands. A simple analogy might be installing a home security system. You would only want to install a tried and tested successful system. Safe, secure and reliable, so that you and your family are safe.

Companies need to take this level of care and responsibility when it comes to their ICT-environment in the broadest terms. This includes mobile applications, devices as well as third-party access, applications, networks, and computer systems. You can use tools that both run automated checks and conduct manual penetration testing, which incorporates human expertise alongside penetration testing software. This will check compliancy boxes and strengthen your overall security and safeguard you against possible liabilities, litigation or penalties.

There are further benefits too. Penetration testing helps with; discovering security policy blind spots, reveals compliance with security policies, helps improve security itself, it gauges and tests staff knowledge when it comes to ICT-security, online habits and it gives a blueprint as to what the most essential risks are that need to be addressed by the organisation. It also gives the company lawyers and the CEO peace of mind, which is essential.

All in all, penetration testing is done to ensure that the ICT-environment is as safe and impenetrable as possible before someone with bad intentions realises they can access your system and use it for illicit means.

ABOUT THE AUTHOR

Johann van Rooyen is cybersecurity specialist at Green Enterprise Solutions