BIZCOMMUNITY

The 10dot cyber security 2017 forecast

By Jared van Ast

17 Feb 2017

Ever wish you could see into the future? Sure you have. We can. You will be hacked this year. Your servers will be compromised, and your personal and proprietary information posted for all to see. Fact. And we don't even need a crystal ball to tell you so.

In 2017, over 700 million cyber crimes have happened around the globe. Statistically, that means at some point during the next coming months you are likely to be hacked.

Cyber-attack methods to watch out for:

- Phishing – Always popular and getting more sophisticated. This is when you click on dodgy yet legitimate-looking links in emails, and you are prompted to input personal information. It's tempting, but don't click it!
- Ransomware – where cyber crooks lock you out of your network and hold access to your data for a ransom that usually takes the form of Bitcoin payments. This threat tech will evolve and we may start to see "viral" ransomware attacks. Gone are the sniper rifles, enter the age of the shotgun approach.
- IoT Manipulation – "Dumb" devices will continue to be hijacked and transformed into botnets, capable of crashing large-scale server infrastructure. DDOS attacks will continue to target platform providers, and government systems.

Most-vulnerable industries

In South Africa, there have been around 2260 reported cyber crimes. We anticipate that thousands more attacks will happen, but with no formal governing body reporting these incidents, it is difficult to monitor the true threat.

If we analyse the global trends, we can expect the following industries to be most vulnerable:

- ### Political institutions

  As hack groups start to formalise their socio-political agendas, we'll start to see many more attacks on political leaders and institutions under the guise of "Hacktivism". Enter the age of cyber propaganda. Just look at the group Anonymous declaring war on ISIS.

- **Fintech**

  This is a fast-growing industry, and although benefitting from loads of cash being invested into security tech, the promise of windfall returns is just too great for money-grabbing cyber crimes to ignore.

  Ransomware will continue to be the tool of choice to expropriate capital from this sector. The smaller players should be extra vigilant in securing their networks and educating staff on good email practice, and other “conscious” online behaviour.

- **Healthcare**

  Access to basic, affordable healthcare is still a privilege of the few, especially in South Africa. These institutions and networks also hold massive data pools that are valuable to malevolent parties out there. More importantly, most of this data lives on legacy networks that have multiple integrations with peripheral systems, such as medical aid providers and other financial institutions. This broadens the risk of exploitation, even for more sophisticated networks.

- **IoT**

  The October 2016 Dyn DDOS attack set new records. Security strategy will need to adjust to incorporate “dumb” devices online. At 10dot, we are working closely with local IoT thought leaders in order to build security tech specifically designed for the IoT movement.

If cyber threat is imminent where will people put their cash in 2017? There is an ongoing debate around prevention vs. predictive analysis and response. This may be slowly gaining traction in first-world markets, but locally, our adoption of next-generation technology remains slightly subdued due to our maturity phase. The Fintech vertical will likely drive this adoption going forward.

Locally, we forecast that “good old fashioned” perimeter prevention tech like firewalls will continue to sell well. This is trusted technology with broad product streams and is comfortable to consume. International, post-industrialised markets will start to drive uptake of fully outsourced, managed services. Semi-industrialised markets will likely adopt a similar strategy to our own – prevention, semi-managed, with granular visibility and control.

An entrenched business driver

A mobile workforce is an entrenched business driver in this day and age. Look out for uptake in sandboxing and end-point technology, and other network segmentation tech, that is geared to enhance the security of a mobile workforce and ever-widening corporate network.

Managed services will continue to enjoy 50% of overall investment in cyber security tech worldwide. This is due to scarcity and cost of cyber security skills, and companies needing to run leaner outfits in order to remain competitive. Outsourcing will continue to deliver a robust value proposition to a stifled and cost-sensitive market.

In conclusion

Our forecast for the cyber threat landscape 2017 includes continued exploits through phishing, ransomware, hacktivism, and data breaches through shared server compromise.

Our advice is to employ the advice of experts to craft a cyber security strategy, and help you plug the gaps. Frequently update your firmware, and other anti-malware programmes, and most importantly, educate your people so they aren't the cause of a cyber threat.

ABOUT THE AUTHOR

Jared is the founder & managing director of 10dot Cloud Security. Frustrated with diluted value propositions. Loves to do things properly. Suspicious by nature and habitually pragmatic. Focused on network security, 10dot works to lock-up business networks and help them grow. Over 15 years' experience in IT & ISP sectors. Jared is hell-bent on enabling companies to focus on core business. 10dot Cloud Security – The Network Security Specialists. [[www.10dot.com]].