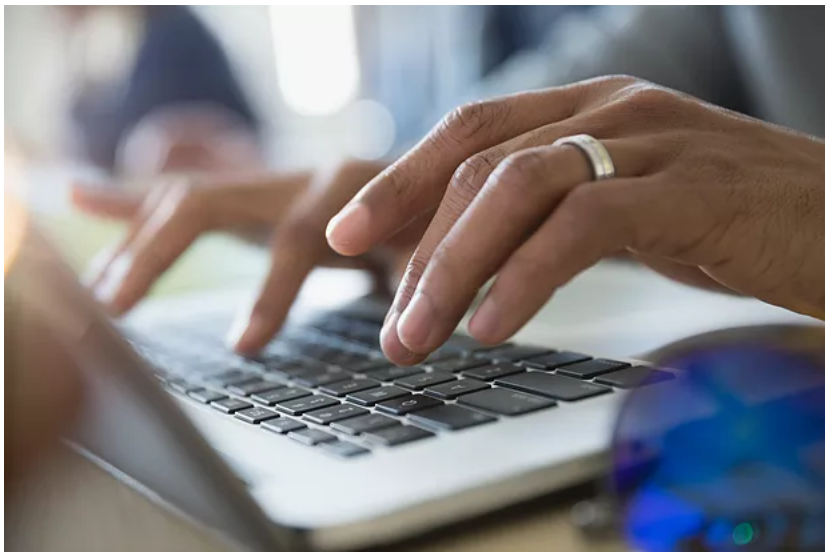
Cyber security | Predictions

Centrify predicts how to turn the ANZ cyber security tide in 2018

December 12, 2017 | Richard van der Draay



Centrify has identified seven trends that it says will shape enterprise security in Australia and New Zealand during 2018.

Centrify Corporation Senior Director APAC Sales Niall King said the major data breach revelations that had marked the past year would continue in 2018 as organisations struggled to recognise that unmanaged trust was at the core of their cybersecurity vulnerability. "While during 2017, Uber and Equifax opted to hold off reporting their respective data breaches, this is not an option in Australia where mandatory data breach reporting legislation takes effect from February 2018," he said.

Based on its industry research and deep dive discussions with customers, the firm has highlighted seven trends that will impact cybersecurity during 2018.

1/ The dark trend in ransomware will continue to explode in the coming year
According to the FBI, 2016 ransom payments totalled about US$1 billion, up from US$24 million in 2015. Centrify expects this lucrative illicit trend to continue for years to come.

2/ Blockchain will emerge as a potential disruptor across many areas of technology
While Centrify expects blockchain to emerge as a potential disruptor across many areas of technology in 2018, it will take several years to address blockchain vulnerabilities before the technology is sufficiently mature to act as a basis for enterprise security. That means blockchain technology may add to security risk before it starts to reduce it.

3/ Automation frameworks will make it easier for DevOps to adopt AWS securely
Security vendors will continue to embrace Amazon's shared responsibility model for AWS during 2018, resulting in the rise of DevOps, a fast-growing segment required for successful automation. Centrify says baking security into the process will allow for further adoption of cloud-based services.

4/ Increasing identity-related breaches and vendor fatigue will force organisations to

RELATED POSTS

Centrify unveils six steps to beef up security in 2018

re-evaluate their security postures — architecture, budget and project priorities
Despite Verizon's 2017 Data Breach Investigations Report (DBIR) reporting that compromised identities were responsible for 81 per cent of all data breaches, companies spend just 4.7 per cent of their total security budgets on identity and access management (IAM) - the very technology that could help prevent four out of five breaches. Centrify expects that a combination of increasing identity-related breaches and security vendor fatigue during 2018 will force companies to re-evaluate their entire security posture from the ground up, to put protecting identities at the centre of their security.

5/ Organisations will respond to the current threat landscape with a Zero Trust Model
After the huge corporate impact of data breaches such as Equifax and Uber, Centrify expects companies to respond to increasing cybersecurity threats by implementing Zero Trust security models, which shift access controls from the perimeter to users and individual devices and grant access to services based on what is known about a user and their device.

6/ The security market will incorporate machine learning to address identity-related breaches
Last year, companies such as Centrify integrated machine learning to ascertain the risk level of individual transactions and decide in real time whether to allow them. Centrify expects to see wider adoption of this approach, which pivots identity security away from detect-and-respond alerts and towards more automated preventative controls.

7/ The rapid move to the cloud will increase the adoption of Zero Trust network models and modern microservices architectures that mandate the use of least privilege
During 2017, companies moved large segments of their infrastructure into the cloud, which still requires authentication and privilege management. Centrify anticipates widespread adoption of technologies that manage privileged identities with fine granularity. Least privilege will become an increasingly common term around the data centre.

Mr King said the immediate cybersecurity outlook for 2018 was ominous. "While the risk is that things will get worse before they get better, Centrify is confident that emerging security models such as Zero Trust will enable organisations to rethink their cybersecurity," he said.

"Embedding security bulwarks such as least privilege access, multi-factor authentication and machine learning-based risk assessment into standard corporate workflows will increasingly focus organisations on securing identities to follow a proven path that can turn the cybersecurity tide."

Tags: Centrify

Telecom Times ABN 29 4077 68729
Editor: Richard van der Draay
Tel.: +61 (0) 422 053 989
PO Box 953, Gladesville, NSW 2111 Australia

About us