Securing identity, access management against cyber criminals

Following global cyber attacks, organisations need to ensure that identity and access management (IAM) is as well managed as firewalls and security controls.

© Igor Stevanovic – 123RF.com

“In our ever-increasing digital age, we are finding that we need to work even harder at governing and protecting data and information,” says Philip Yazbek, industrial psychologist at consulting firm Bizmod. “How we govern and protect starts with who and how we access data and information.

“The global cyber-attack that hit 150 countries worldwide (South Africa included) in May should be a wake-up call to not only organisations but to our government agencies as well, confirming that our information security is still very vulnerable.

“Organisations can have all the necessary firewalls and security controls in place, but if they are not controlling and monitoring IAM, they are leaving the doors open for cyber criminals.”

He cites recent cyber security research that reveals some startling information.

- In South Africa, data breaches costs SA firms R28.6 billion per annum. (IBM & Ponemon Institute, 2016)
- Breaches are usually discovered long after they have occurred. In 2015, the average amount of days it took from when the incident occurred until it was discovered was 146 days (Mandient Consulting, 2016)
- In most breaches, legitimate user credentials were used, where 63% involved weak, default or stolen passwords. (Verizon DBIR, 2016)
- Employees can be your biggest risk. It was found that 43% of data loss was internal, half being intentional, the other half accidental. (Intel Security Report, 2015)
- 90% of ex-employees retain access to their former employers' software applications. Another 49% were shown to have logged into a company account after no longer working there. (Intermedia, 2014)

Open networks increase risk

"Employees move around in an organisation; they may move across roles or up in the ranks and by doing so accumulate access rights along the way. It may even become a form of entitlement to be a super-user with avant-garde access.

"In the past, before the advent of smart devices, cloud networking and VPN access, IAM was simpler because systems were mainly computer based and were easily controlled in closed networks. Now, people are connecting on different platforms – PC, mobile devices to the cloud – and various operating systems (Android, IOS, Microsoft), so the architecture has had to evolve to cater for this, making IAM and how it is governed more complex.

"While we assume that people have the integrity to not abuse their privileges and only use the access they need, the onus is on the organisation to ensure this is controlled," concludes Yazbek.