A mindset change required to mitigate cyber attacks

2017-01-25

Network security is a global risk and enterprises are spending millions on securing their corporate networks, yet they are still being attacked. Greg de Chasteauneuf, chief technology officer at Saicom Voice Services takes a look at why there needs to be a mindset change. “The cybersecurity industry as a whole needs to ask itself what the most significant development over the past twenty years has been, because the reality is that companies are being compromised and held to ransom more frequently,” says de Chasteauneuf. The current mindset is very much that of perimeter security - a firewall boarding the trusted and untrusted networks. Most companies believe this is enough, the reality is that it is not. Today’s threats come from everywhere, not just the untrusted networks, and many of these attacks render the traditional perimeter firewall useless. Haroon Meer of Thinkst Applied Research agrees. “Firewalls have had a good run but they offer very little to protect companies against phishing or application layer attacks. For most of the more common attacks seen today, firewalls are no roadblock, in fact they barely count as a speed bump.” Human beings are often the weakest link and it is a company’s own employees who can punch holes in its network. It can be unsuspecting employees opening emails that have been socially engineered to fit their lifestyle profiles or a disgruntled staff member with an axe to grind who shares confidential information. Anyone can buy an inexpensive cellular modem device and plug it onto a network, and this causes a big vulnerability. The point is, if someone is snooping on a company’s network, it needs to know about it. “This is where deception technology steps in. The industry will see an important move back to host security and honeypots to detect and mitigate lateral movement within the trusted local-area network (LAN)” says de Chasteauneuf. Gartner identified deception technology as one of its top ten technologies for information and security in 2016. Deception technologies create fake assets, for example a password file, a customer list or a payroll document and if an attacker tries to attack these files, it is a strong indicator that an attack is in progress. Deception technologies exist for network, application, endpoint and data with the optimal systems combining multiple techniques. Next generation tools like Thinkst

Canary reliably set off an alarm when an active attack is discovered. They are simple, effective and alert a company when it needs it most. “Companies have spent millions of rands on security tools that have achieved almost nothing, except for giving them a false sense of security. A quick look at recent headlines shows that those companies are now paying the price for it. Thinkst Canary forces attackers to reveal themselves, allowing companies to quickly discover an attack when their other security controls have failed,” says Meer. Enterprises should look at deception technology tools that are simple and quick to deploy, require no firewall or infrastructure changes, are scalable and have zero administrative overheads. Companies expect that hugely complex solutions are needed because of the enormity of the problem, but sometimes it is the simplest of solutions that are the most valuable. “Canary works like an alarm system that can be setup in minutes and offers companies peace of mind. This allows them to remain focused on their core business,” adds Meer. Once an active attack is discovered it then leads to the next phase - managing and responding to the attack. This is where managed security services like Saicom Voice Services will play a role. PwC’s Global State of Information Security Survey 2017 found that 62% of survey respondents use managed security services for cybersecurity. The reality is that very few organisations will have the commercial means to deploy and maintain a cybersecurity task team, as such, outsourcing of this function will be the norm. “Security will continue to be high on the CIO’s agenda in 2017 and in time will become the most important requirement when making any IT decision in the future. Forward-thinking organisations will start to deploy deception technologies and adopt managed security services to monitor and mitigate risks,” concludes de Chasteauneuf. ***Post written by Greg de Chasteauneuf Chief Technology Officer (CTO) – Saicom Voice Services***