What cybersecurity experts think about Transnet's hack crisis

State-owned rail, port and pipeline company Transnet appears to be in crisis mode after a cyberattack hit the company last week. Two cybersecurity experts weigh in on the matter below.

Anna Collard, senior vice president of content strategy and evangelist at KnowBe4 Africa:

“I suspect this was a ransomware attack. Ransomware groups or affiliates targeting large organisations or critical infrastructure are also called 'big-game hunters' because they know that the stakes are high and it's very likely these companies will pay the ransom.

With the United Stated declaring ransomware a national threat, more criminals will shift their attention towards the emerging economies and South Africa is quite attractive, because, on the one hand, we have developed infrastructure, a high degree of digitisation but at the same time, not enough government capacity to defend against this on a national level.

This is really just speculation now, but with what has been going on in the last two weeks, some industry experts were speculating if this attack may even be politically motivated.

ICT

Transnet hit by cyberattack - Operations disrupted nationwide

22 Jul 2021

The concerning point is what are we going to do in South Africa if and when more of our critical infrastructure is under attack. It's absolutely crucial that we - industry, public and private sector - need to collaborate and assist each other in cases like that and defend our country against this inevitable threat together," she concludes.

Stephen Osler, co-founder and business development director at Nclose:

"We have recently seen another flurry of South African victims of the rampant ransomware attacks. According to sources, some well-known ransomware victim lists there have been over 1,000 businesses compromised this year which is a massive increase from the same period of last year.

Unfortunately, no one is spared, and organisations need to ensure proper controls are implemented to either stop the attack or reduce its damage.

It's not a matter of if it's a matter of when. Unfortunately, as soon as a government organisation is compromised in this fashion it's assumed they didn't have appropriate security controls. However these ransomware attacks are happening to blue-chip organisations with large security budgets, so no one is spared," he concludes.