BIZCOMMUNITY

What can we do to stop ransomware attacks on governments?

By Simeon Tassev

16 Dec 2019

The City of Johannesburg recently became the latest victim of high-profile ransomware attacks specifically targeting government departments. A network breach was detected and all e-services were shut down.

Simeon Tassev, MD and QSA at Galix

This follows on from the City Power attack in July, which encrypted databases, applications and networks, and resulted in users unable to purchase electricity units for prepaid meters.

Ransomware attacks targeting the public sector have become a trend, not only in South Africa but across the globe, for a number of reasons. In order for the public sector to ensure that they can protect themselves from future attacks, they need to reconsider their security protocols and practices to make themselves less of a target and prevent repeated attacks from occurring.

Why are governments being attacked?

The simple answer: because they are seen as ideal organisations' to target. Cybercrime is all about the money, and the public sector is potentially highly lucrative. Despite its name, ransomware is often not only about holding data to ransom, but there is also typically a time bomb attached that will destruct the data if the ransom is not paid.

Governments are in possession of large volumes of data and provide critical services and cannot afford to simply lose their data or have it exposed. Recovery is often difficult and costly – so much so that the ransom demands are seen as the lesser of two evils, so a successful attack is more likely to yield profitable results. These attacks are not limited to South Africa, nor is it a new occurrence.

The attack on the National Health Service (NHS) in the United Kingdom in 2017 seems to have ushered in an era where threats of this nature are a frequent occurrence across the globe. In fact, according to an article in the *New York Times*, "More than 40 municipalities have been the victims of cyberattacks this year".

In addition, the article states that 22 cities across Texas were simultaneously held hostage for millions of dollars after an attack infiltrated their computer systems and encrypted their data.

Investment into security is the only solution

Attacks on public sector organisations are quite clearly on the rise, and ignoring the threat is no longer an option. Once a successful attack has been perpetrated, it is highly likely that hackers will attempt the same tactic again because it is a low-risk strategy with high potential reward. The only solution is to invest further in security to close loopholes and potential vulnerabilities.

Often, cyberattacks gain entry as a result of human error, most commonly by an employee clicking on an infected link or attachment. Consequently, stricter controls need to be put into place and greater effort placed on education and security awareness.

Data itself needs to be protected via encryption to make it more difficult to steal or to use once it has been stolen. Effective backup and recovery solutions also need to be in place, along with best-practice security processes, tools and maintenance. All systems must be kept up to date with the latest patches, updates and definitions.

Once an attack occurs, a post-mortem analysis is a critical step in understanding how the incident occurred and what vulnerabilities exist that need to be addressed. This is the only way to work toward preventing an attack from occurring again.

While every attack is different and its anatomy and methods may change, it is essential to ensure that the same attack strategy cannot be used again otherwise the risk of multiple attacks is high.

Ultimately, data is the target in ransomware attacks. It is imperative to understand what data exists, where it is stored, what it is used for and what the impact is if it is stolen or compromised. If data is not being effectively managed then a breach will likely send any organisation into a tailspin as they scramble to understand what data has been affected and what the impact is.

Prevention is definitely better than the cure.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa

- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...