Protect your company from future ransomware attacks

By Lukas van der Merwe

3 Sep 2019

The recent ransomware attack on Johannesburg power utility City Power shows how easy it is for organisations to fall victim to cybercriminals, who often carry out attacks that are financially motivated.

Lukas van der Merwe, Specialist Sales Executive: Security at T-Systems South Africa

In the City Power attack, the utility – which supplies electricity to South Africa's biggest city – revealed that the ransomware virus encrypted all its databases, applications and network.

While the company did not reveal how much the attackers demanded for decrypting its systems, one can imagine that it was most likely a significant amount. In cases like this, there is no guarantee that once the ransom is paid the data will be decrypted nor that the perpetrators will not attack again. It is strongly advised against paying the ransom.

In order to avoid a ransomware attack, it is important to delve into how such an event happens. This type of attack is normally perpetuated using a Trojan. Here, a user is fooled into downloading or opening a file that is received via e-mail, which appears legitimate.

There are, however, notable exceptions like the worldwide WannaCry Worm attack, in 2017, which distributed itself without user interaction.

As the frequency of ransomware attacks is on the increase, organisations should be prepared so they suffer as little downtime as possible in the event of a cyberattack. Obviously, prevention is the preferred option but is still fallible.

Safeguard your network from attacks

1 Aug 2019

An advanced attack, which encrypts data, may be impossible to reverse without having access to the encryption key. To reduce downtime, companies should have a clearly defined remediation or infection control process in place to first isolate any infected devices from the network and prevent further distribution. The next step is data recovery and, since recent attacks also encrypted backups, the remediation process should include remote/offline backups not accessible from the network.

Recovery from a ransomware attack depends on a multitude of factors, including the type of attack, access to recent unaffected backups, the extent or size of the affected data set, performance of the systems in restoring the backups and the type of system affected.

For example, a recent ransomware attack on a South African software development firm was recovered within 24 hours, as no transactional data was affected, and the company simply restored the most recent unaffected backup. Development work performed since this backup and the attack was lost, yet the financial impact of the attack was limited to production time lost.

Should a transactional system be affected, the recovery time will be greatly extended due to the requirement to recover all recent transactions up to the point of failure. The larger this data set, and the more complex the environment, the longer the recovery, and the financial implications or damage could be extensive due to potential loss of transactions.

In short, recovery could be completed in hours or may take weeks.

It's time to take ransomware attacks seriously

Dr. Amin Hasbini 1 Aug 2019

Education is a big part of prevention. Companies should execute regular cyber awareness initiatives to educate their users. Such programs should be supported by the highest levels in the organisation and continued amendment is required for the content to remain relevant. Individuals should be made aware of the severity of such attacks and obliged to participate in the programs.

Users should be vigilant about clicking on unfamiliar links or e-mails. The sophistication of these attacks is rapidly increasing, and a malicious e-mail may appear to originate from a trusted co-worker and even reference a familiar topic or meeting. If you suspect that you may have been affected, disconnect your device from all networks and seek assistance from the relevant support team.

It is possible to reduce the risk of attacks, but any holistic security policy should include rapid and effective remediation. User education is critical. Perpetrators of these attacks are difficult to trace and prosecute.

The impact of an attack is potentially disastrous. IT service providers offer consulting, tools, processes and services to assist organisations in minimising the risk.

ABOUT THE AUTHOR

Lukas van der Merwe, Specialist Sales Executive: Security at T-Systems South Africa.