Hotels increasingly vulnerable to ransomware attacks

According to Grant Thornton, South African businesses need to act now to ensure that their digital systems are protected and that critical systems are taken offline as they are increasingly vulnerable to the 400% growth in global ransomware extortion attacks.

©Brian Jackson via 123RF

Simple ransomware attacks are relatively straightforward – victims receive an email with a link that contains software that encrypts files on their computer. These victims are then held to hostage until they pay a ransom.

Recently an upmarket hotel in Austria had its electronic key system compromised by hackers who locked management out of its own computer system. Guests were unable to access or leave their hotel rooms and this led to the hotel being forced to pay a ransom of two Bitcoins – an electronic currency that is difficult to trace – equivalent to about $1,800 (R20,000) to gain access to their system.

Hotels doubly vulnerable

Martin Jansen van Vuuren, director: advisory services at Grant Thornton says that the Austrian attack indicates just how easily hotels' systems can be infiltrated from cyberspace.

Jansen van Vuuren says: "Hotels are doubly vulnerable because ransomware attacks may not only impede their systems

but they also could seriously impact on their guests by preventing them from using the hotel's facilities. Part of hotel management's risk mitigation should be to work out exactly how these malicious cyberspace attacks can affect their operations and even their customers."

"The security of convenient computer-driven systems is vital, because everything from air-conditioning and room management to sprinkler systems, suddenly become vulnerable to external attacks. There is a need to give particular consideration to these risks as we become more reliant on technology in the guest experience."

Jansen van Vuuren says mobile phones, used as keys in many hotels these days, are also vulnerable as they often do not have the same level of security as a desktop system. Hackers could steal "door keys" via cyberspace or simply disable keys causing huge inconvenience. Open Wi-Fi systems, that are by their nature made easy to access for hotel guests, are another potential source for hackers if they are linked to systems which can be used to gain entry to devices and then to lock out users or steal data.

The biggest weakness for hotels

"The biggest weakness for hotels is their public interfaces such as booking systems that need to connect the internal systems and users to third party applications and ultimately customers. The booking system is therefore particularly vulnerable to ransomware attacks and hackers," said Jansen van Vuuren.

"Many hotels do not have on-site IT support and rely on the hotel chain's head office or an external service provider to attend to IT issues. This centralised approach places individual properties at additional risk of attack, as a cyber-attack may not be picked up quickly enough leading to a delay in combating the cyberattack" he says.

Ransomware attacks quadrupled in 2016 to 4,000 a day

Grant Thornton's director of IT advisory services, Michiel Jonker, says that while the hotel industry is in the public eye, following the most recent high-profile attack, it has to be borne in mind that every industry is at risk.

According to data from the United States Justice Department, ransomware attacks quadrupled in 2016 to an average of 4,000 a day. The FBI said the costs to victims of such attacks rose to $209m (R2,7bn) in the first three months of 2016, compared with $24m (R312m) for the whole of 2015.

"Ransomware syndicates are extremely sophisticated, even hosting their own 'call centres' which assist you to access your decryption key and undertake not to attack you with the same ransom. They even use algorithms to determine your particular industry, and the ransom price is based on your industry's perceived 'wealth'," says Jonker. "You can't really prevent these attacks, you can only reduce your attack vulnerability to some extent. Preventive controls are not enough. Organisations will have to rely on corrective controls, most notably backups and disaster recovery plans."

Minimise the risk

He says corporate executives have to start seriously considering how their companies will respond to malicious attacks and whether their systems – both critical and simple – are designed to minimise risk to the impact of hackers and ransomware.

He says that Grant Thornton's IT Advisory team advises clients to take, among many other things, the following steps in order to minimise the risk to some extent:

- Remove admin rights for laptop users to prevent users from inadvertently downloading malicious software;
- Ensure that all systems undergo well-structured backup processes and that they are recoverable;
- Segregate networks so that different network segments are limited to different groups of authorised users;
- Provide database access only to those people who require access; and
- Install antivirus software on all devices including laptops; smartphones and other wearable technologies;

• Use low-code programming platforms to develop apps, as we do, where security has already been incorporated into the platform.

Off the grid

Jonker says that while prevention is better than dealing with the effects of a cyberattack, it is best practice to isolate certain high-risk and critical (especially national) infrastructure networks and systems, so that they are off the grid and entirely inaccessible from cyberspace. They only ever link intermittently via a small ‘sterile’ middle system, with neither linked system connected at the same time – a bit like an airlock in a submarine. So a hotel’s external public reservation system might interface hourly via such a sanitised link only.

“At the end of the day you balance security with the need for convenience, availability, functionality and innovation,” says Jonker. “To produce leapfrog new technology most developers are focused on building systems that work, not systems that are secure. We need to change mindsets so that we don’t focus exclusively on functionality but ensure that we build systems that enhance security and privacy in equal measure.

“We believe that technology advances can be hugely beneficial for hotels in creating great guest experiences, but the systems must always be developed with security considerations fully understood and mitigated,” Jonker concludes.