Drones - a new threat that needs to be included in your cybersecurity strategy

With estimates that between 30,000 and 50,000 drones are currently being operated in South Africa, security experts advise that unmanned aerial vehicles have punched a gaping hole in existing physical and IT security strategies.

Pieter Scholtz, DSM Expert: AO/Data Centre Services at T-Systems South Africa.

Interpol warns that the potential use of drones in a terrorist incident or attack against critical infrastructure and soft targets is a growing concern for law enforcement, as the availability of drone technology becomes more widespread globally.

Furthermore, as drones become less expensive and their potential applications continue to expand, it is expected that countries across the globe will see a rise and evolution of this threat.

A report by Goldman Sachs estimated that the total drone market could reach $100 billion by 2020, playing a significant role in every sector of the economy, from agriculture to entertainment and everything in between. However, the report also cautions that for security professionals, the scope of the threat is huge and evolving.

Every enterprise and every individual protected by a traditional fence now requires an aerial equivalent, according to Pieter Scholtz, DSM Expert: AO/Data Centre Services at T-Systems South Africa.

“Drones are bypassing all the traditional security measures that have been in place for years and are breaking all the rules regarding physical access and countermeasures,” he says.

Scholtz notes that what compounds the threat is that drones are relatively inexpensive, easy to operate and can carry heavy payloads that can perform surveillance, capture data, or disrupt networks.

Expand cybersecurity policies

“One of the main things that organisations need to do is to expand their cybersecurity policies to include the threat posed by drones. The nature of drones means that they present a very cheap and easy way to do industry espionage or network hacking. These threats should be taken seriously,” Scholtz says.

He cites an incident in which a German company found a drone parked on the roof of its data centre, where it tried to hack into the centre’s command and control network.

“Hacker drones can eavesdrop electronically on conversations, can perform network attacks, or can create fake wireless access points that can trick an organisation’s employees to connect to it, instead of the corporate LAN,” Scholtz says.

A host of other threats are posed by surveillance drones, which can be used for corporate espionage, invasion of privacy and intelligence gathering for a physical attack, as well as by smuggler drones, which can be used to deliver contraband to restricted areas, such as prisons. Weaponised drones can bring about a variety of physical threats, either by carrying a payload of weapons or by being used as a weapon itself.

Drone detection technology needed

Sam Twala, business and technical director at NTSU Aviation Solutions, says that regulations alone will do little to discourage criminals exploiting drone technology for nefarious purposes. Instead, he says that organisations need to rely on drone detection technology to protect themselves.

“Terrorists or people with malicious intent do not read regulations and comply prior to carrying out their plans. Hence, it is important that organisations develop defence models that will help to protect them against drones,” he says, adding that, unfortunately, there is ‘no one-size-fits-all’ solution.

“The variance in threats delivered by drones means many different types of facilities are vulnerable. You will need a solution that can fit each environment.”

However, because the threat posed by drones is evolving at the speed of cybersecurity, it is security specialists that are facing a challenge to keep up, says Jaacie Visagie, special project manager at UAV & Drone Solutions.

“At the moment, it’s a cat and mouse game. We are discovering new things every day because this is a relatively new industry – but it will come,” he concludes.