Publication : Computer News Middle East
Date : Feb issue
Headline : State Secrets – Government Security

Abdulnabi points to an IDC report on security spending by governments. According to the report, overall security spending has been trickling upward at an average rate of about 4 percent per year, with the US federal government alone expected to spend $7.3 billion on cyber-security in 2017.

According to Alain Penel, Regional Vice President, Middle East, Fortinet, the government sector accounts for 35 percent of the vendor's total revenue for the Middle East. And it's easy to see why governments are so caught up with security. Aside from the spook caused by Stuxnet, Penel points towards other threats that governments are keen to mitigate against as factors in increase spending.

"Government spending is on the rise and will continue to increase. This largely corresponds to the increased threats to sensitive data being compromised by organised hacker groups," he says.

Hacker groups such as the Syrian Electronic Army are now recognised as a force to be reckoned with—the group has compromised the websites of several high-ranking organisations over the past 12 months. Other hacktivist groups have also garnered headlines, so government organisations are doing all they can to protect themselves.

And according to Natalya Kaspersky, CEO, InfoWatch Group of Companies, it's not just the threat of hacktivism that has governments on their toes—some countries in the region may see their critical infrastructures being threatened.

"Some countries in the region still have IT infrastructures that are supplied with worldwide monitoring capabilities, which can influence the processes in these receiving countries. This influence can be realised as infrastructural attacks like, for example, the Stuxnet virus targeted at Iran nuclear sites. Or as imposing certain information to cause disorders like was the case in Egypt, for instance," she says.

"When we talk about the necessity for protection, it depends on a country's threat model. If a country considers such access to its infrastructure a threat then there is a strong necessity for protection."

Natalya Kaspersky, CEO, InfoWatch Group of Companies

The government sector accounts for **35%** of Fortinet's revenue in the Middle East

"So when we talk about the necessity for protection, it depends on a country's threat model. If a country considers such access to its infrastructure a threat then there is a strong necessity for protection."

Indeed, according to Abdullah Hashim, Senior Vice President, ICT, Etisalat, a government's first priority is to protect against damage to critical infrastructure.

"A targeted cyber-attack on a country's information infrastructure can cripple communications, deny access to public services and cause massive economic losses. The first priority for governments is to defend their critical infrastructure assets, including communications, energy and utilities, oil and gas, citizen services, and banking and finance infrastructures, as those are the primary targets for compromise," he says.

Naturally, governments are also worried about ensuring the privacy of their citizens' data, and they're keen on cracking down on cyber-crime, too. To this end, some governments have been taking a more proactive approach when it comes to cyber-security. For example, the UAE recently formed the National Electric Security Authority (NESA)—a clear indication that the country's government is taking cyber-security seriously, according to Glen Ogden, Regional Sales Director, Middle East, A10 Networks.

"NESA's inception clearly, shows how important a credible and properly regulated defence against cyber-attacks is to any region's national security," he says.

However, he also advises that individual government departments need to take responsibility for their own networks. A centralised agency can only do so much, after all.

"Whilst entities like NESA help to raise the profile of threat defence, each government or ministry still needs

"Entities like NESA are key to co-ordinating efforts to enhance cyber-security by bringing together the various clusters and agencies within governments."

Muhammed Mayet, Chief Technology Officer, Security, Dimension Data MEA