South Korea raises cyber attack warning amid heightened regional tensions

Following the North Korean long-range missile launch and the subsequent closing of the Kaesong Industrial Complex, South Korean government offices have again raised the InfoCon cyberthreat warning level.

By Philip Iglauer | February 16, 2016 -- 04:42 GMT (12:42 GMT+08:00) | Topic: Security

South Korea increased its cyberthreat level for a second time in less than a month on Sunday in response to what it said was a growing danger posed by North Korean cyber attacks.

Three government offices that track cyber threats -- the Ministry of Defense; the National Information Service; and the Ministry of Science, ICT and Future Planning -- raised the cyberthreat level as tensions on the Korean peninsula ratchet up.

"We believe there's a larger possibility that North Korea may launch cyber attacks on the South, and recently upgraded our Information Operation Condition (InfoCon)," a defense ministry official was quoted as saying in the local media.

The Defense Ministry raised the InfoCon warning one notch to level three. The five-tier threat level system is used by the military to assess threats to the government's IT network.

South Korea's Ministry of Science, ICT and Future Planning (MSIP) also increased its cyberthreat assessment one notch from "moderate" or level one, to "substantial", the equivalent of level two, following a week of escalating tensions in East Asia after North Korea launched a space rocket on February 7 and put a small weather satellite into orbit.

nation increased from moderate to substantial for private sector websites, ecommerce sites, and email addresses "because of [the] North Korean long-range missile launch and closing of Kaesong Industrial Complex".

"In substantial cyberthreat level [to the] private sector, KISA and MSIP recommend that every corporation raise cybersecurity monitoring, people update their PC software, and don't open unknown emails," a KISA official said.

South Korea's National Intelligence Service, its spy agency, could not be reached for comment on its cyberthreat assessment.

(http://www.zdnet.com/article/india-anti-colonial-to-its-economic-detriment-marc-andreessen-in-incoherent-twitter-rant/)

LG Pay will be a no show at MWC: Report
(http://www.zdnet.com/article/lg-pay-will-be-a-no-show-at-mwc-report/)

Singtel shrinks net profit by SG$16m
(http://www.zdnet.com/article/singtel-shrinks-net-profit-by-sg16m/)

Facebook withdraws Free Basics project in India
(http://www.zdnet.com/article/facebook-withdraws-free-basics-project-in-india/)

Samsung to provide public safety network in South Korea
(http://www.zdnet.com/article/samsung-to-provide-public-safety-network-in-south-korea/)

On February 11, North and South Korea cut off an emergency "hot line" between the military of the two countries as hundreds of staff were repatriated to the South, days after Seoul announced it will withdrawal its participation in the Kaesong Industry Complex, the last remaining inter-Korean economic cooperation project.

Late last month, the science ministry increased the cyberthreat level (http://www.zdnet.com/article/south-korea-raises-cyberthreat-level-against-north-korea/) from normal to "moderate" about one week after computers in South Korea received a barrage of malicious emails, around the same time North Korea tested a nuclear device.

The Defense and Science ministries both said that no new series of cyber attacks have been detected this time around. "We believe North Korea is more likely to launch cyber attacks than before and we're keeping close tabs on potential signs," said one Defense ministry official, according to local media reports.

South Korea is the target of many cyber attacks, and in particular, its government offices, financial and IT sectors, and the accounts of its personnel get hit by advanced persistent threats (ATP), phishing, and smishing attacks frequently.

The last time the cyberthreat level was this high was in 2013, following a wave of attacks that downed scores of government, banking, and media sites including the website of the presidential office. That attack took place on the 63rd anniversary of the start of the Korean War, on June 25.

Malware used in the 2013 attack has been dubbed by cyber professionals as DarkSeoul. The attack was tracked by officials who linked it to a single IP address in China. South Korea blames the North for that attack.

North Korea was also blamed by South Korea and the US for the Sony Pictures hack in November 2014, which forced the company to pull its film (http://www.zdnet.com/article/hackers-rejoice-sony-pulls-korea-film-bows-to-criminal-pressure/), *The Interview*, from theatrical release. But conclusive evidence that the country was indeed behind the attack remains to this day scant at best. That incident employed a phishing attack.

Source: ZDNet.co.kr

NSW Justice CIO: Getting into bed with your service provider

The New South Wales Department of Justice's CIO has likened the department's attitude towards an as-a-service model to a relationship, saying that some services should be procured like a one-off hookup, and others like a marriage.

By Asha Barbaschow | February 16, 2016 -- 01:02 GMT (09:02 GMT+08:00) | Topic: Cloud

According to Aaron Liu, CIO for the New South Wales Department of Justice, the key to successfully implementing a businss service is the relationship with the vendor.

Speaking at Criterion's Implementing an As-a-Service Model conference in Sydney on Tuesday, Liu seperated a businesses relationship into two halves: A quick hookup, or a marriage.

"In some ways it's like getting in bed with your service provider, whether that's cloud or managed service, or even internally," he said. "Is it a hookup? Or is it a long term marriage -- a much deeper composition?"

Liu said that on the one-off implementation side, it is usually the hyperscale commodity items such as infrastructure-as-a-service, platform-as-a-service, email, non-production systems, and other things that he said a business would prioritise its agility over its risk.

LATEST AUSTRALIAN NEWS

IBAC probes Victoria's Ultranet corruption claims (http://www.zdnet.com/article/ibac-probes-victorias-ultranet-corruption-claims/)

Cabinet reshuffle adds rural communications and 'digital transformation' (http://www.zdnet.com/article/cabinet-reshuffle-adds-rural-communications-and-digital-transformation/)

Optus announces AU$227m quarterly net profit (http://www.zdnet.com/article/optus-announces-au227m-quarterly-net-profit/)

What the Dallas Buyers Club ruling means for piracy in Australia (http://www.zdnet.com/article/what-the-dallas-buyers-club-ruling-means-for-piracy-in-australia/)

"In some ways this also branches out into experimental systems and innovation, and although that might be ... high risk, it's balanced off by the need for agility," he said.

Tasmanian council seeks refund on 'underwhelming and exorbitant' NBN FttP estimate
(http://www.zdnet.com/article/tasmanian-council-seeks-refund-on-underwhelming-and-exorbitant-nbn-fttp-estimate/)

On the marriage side of the equation, Liu said that a business is looking at things that are traditionally being provided in-house or as managed services, those that are not subject to significant change -- they're more a long-term proposition or investment, such as ERP and CRM systems.

Liu said the answer to tackling the move to as-a-service is about managing risk and putting the right commercial, technical, and service level controls around it to warrant which side of the relationship spectrum a particular item sits under.

"The market maturity and competitive nature [of those on the hook up side], where you can switch providers is almost as easy as swiping left or right," he said. "The other side's a prenup, a divorce, and potentially a much more protracted barrier to exit."

According to Liu, having everything as a service does not mean outsourcing everything; rather it means taking a service-based approach to design a service.

He said a business also needs to intimately understand its business risk, which is to wholly understand what the business is going to use something for, as opposed to just the IT risk.

"It works both ways and helps if the vendor also understands your business risk," he said. "Sometimes security is used as an excuse not to move towards as-a-service. It's about understanding both sides of the risk equation."

Additionally, Liu said that before signing a service provider, a business should have an exit plan.

"One of the things around that marriage thing is that having it is sticky, and it's very hard to get out," he said. "So approach it like you could a marriage -- depending on how you approach marriage -- but you might want to have that prenup put in place. Service providers that are in there for the long haul will respect that."

He said if a service provider is doing that right, it is not going to be a monogamous marriage, rather a polygamous one, adding that the more strategic partners a service provider has, the better.

Liu said the NSW Department of Justice covers everything from the Sydney Opera House to the Long Bay Correctional Facility, saying the portfolio sees the department becoming a fairly vast and complex organisation.

Speaking of the department's transition into digital, Liu said that whilst digital is being utilised, the department is not fully there.

"About half a million simple forms are now filed through an online portal, as opposed to someone physically performing the tasks," he said. "We are making some inroads, but there's still a long way to go and we've still got parts of the business that are still fairly manual."

Liu said the department's strategy is essentially to push digital services. He said this involves moving to as-a-service, and to get better outcomes for citizens but also to get a better value out of the department's IT investments.

"Part of our journey in coming together as the Department of Justice is to consolidate and optimise some of the fragmented environments that we have, and in doing that you've got to get a plan," Liu said.

"Strategy and planning comes first, and one of the key principles in that plan is to adopt everything as-a-service.

"The cloud can sometimes turn into a storm; there are some characteristics of cloud-like operating models that have inherent risks such as vendor lock-in, one size fits all, forced upgrades -- a lot of negatives to deal with in that journey."

JOIN DISCUSSION