theguardian

NSA merging anti-hacker team that fixes security holes with one that uses them

US spies will have to choose between keeping hackers out or acting like them to gather intelligence, going against recommendation of computer security experts

Danny Yadron in San Francisco

Wednesday 3 February 2016 13.15 GMT

A reorganization of the National Security Agency could increase pressure on US spies to choose between keeping hackers out - or acting like them to gather intelligence.

This week, the NSA is expected to announce an internal reshuffling that will merge its defensive and offensive cybersecurity missions, two former US officials said.

The defensive side, called the Information Assurance Directorate (IAD), works with private companies and government networks to plug security holes before they can be exploited in a cyberattack. The offensive side, called the Signals Intelligence Directorate, often seeks to leave such security holes unpatched so they can be used when they hack into foreign systems.

Merging the two departments goes against the recommendation of some computer security experts, technology executives and the Obama administration's surveillance reform commission, all of which have argued that those two missions are inherently contradictory and need to be further separated.

The NSA could decide not tell a tech company to patch a security flaw, they argue, if it knows it could be used to hack into a targeted machine. This could leave consumers at risk.

NSA director admiral Michael Rogers has said a flatter structure is necessary to make the agency, which can get bogged down in military speak and red tape, more agile as foreign hackers become increasingly brazen. The US Office of Personnel Management announced in 2015 it was hit by a breach linked to China, and more recent attacks have included Iran-linked attacks on US critical infrastructure.

NSA hackers could probably work with its defenders on where to look for software flaws, or how to model enemy behavior, former US officials said.

"These core missions are critical as we position NSA to face complex and evolving threats to the nation," an NSA spokesman said of the restructuring, described in an earlier report on 26 January by the Washington Post. "Out of respect for our workforce, we cannot comment on any details or speculation before the plan is announced."

Still, several computer security experts and former intelligence officials acknowledged

the new NSA may face additional tension in choosing between offense and defense. And, like in sport, offense is usually more alluring.

“When a lesser thing joins a greater thing there’s always the threat that the greater thing prevails,” said one former US official, who added he was supportive of NSA’s plans.

In its 2013 report to the White House, the President’s Review Group on Intelligence and Communications Technologies suggested NSA’s IAD be broken out into its own agency.

“We are concerned that having IAD embedded in a foreign intelligence organization creates potential conflicts of interest,” it wrote. In 2014, one of computer security industry’s leaders, RSA executive chairman Art Coviello repeated these claims at the RSA Conference in San Francisco, the industry’s main trade show.

Coviello experienced the tension between the two sides of NSA during the last decade when his company adopted an encryption scheme backed by the defensive side of the agency. Years later, Reuters and others reported that type of encryption relied on a random number generator that could have been cracked by NSA hackers.

By going the other way, the NSA may make private companies - especially in Silicon Valley - less likely to work with the agency on defense. Former US officials supportive of the plan said any companies skeptical of the new structure probably already weren’t willing to work with NSA anyway.

Other former officials said the restructuring at Fort Meade just formalizes what was already happening there. After all, NSA’s hackers and defenders work side by side in the agency’s Threat Operations Center in southern Maryland.

“Sometimes you got to just own it,” said Dave Aitel, a former NSA researcher and now chief executive at the security company Immunity. “Actually, come to think of it, that’s a great new motto for them too.”

More news

Topics

NSA Hacking Cyberwar Computing US military More…