'Active defense' benefits public sector more

By Ellyne Phneah | January 16, 2013 -- 11:03 GMT (03:03 PST)

Governments and public sector agencies have more resources and more sensitive information to protect, which is why an "active defense" online security strategy makes more sense compared to private sector entities.

According to Marc Bown, SpiderLabs managing consultant at Trustwave Asia-Pacific, state governments are generally well-resourced and have important data to defend against hackers, and pursuing an active defense strategy is of great value to them.

Active defense generally involves creating "honeypots" that use false information to lure hackers down dead ends and away from the organization's critical information.

Roman Foeckl, CEO of security firm CoSoSys, added that public sector agencies pursuing such a security policy may have suffered serious damage resulting from their networks being breached by hackers in the past. Since they have the resources and traditional security methods have failed them, it is natural for them to seek other options, he said.

Elaborating, Foeckl said active defense requires skilled IT professionals, time for research and attack simulation and money to execute successfully. Private sector entities, in comparison, may not have these resources in place to pursue such an online security strategy, he added.

Both Bown and Foeckl were commenting following a report in December 2012 revealing Juniper Networks was in talks with India's government and CIOs of top companiesto adopt its deception-based cybersecurity system. The system is touted to mislead hackers using false information while keeping organizations' critical information safe, it noted.

However, organizations must beware there can be inherent dangers in using active defense methods, Bown warned.

An attacker's first step is usually to find the weakest link in its target's security and this means most attackers will find their way into a honeypot. However, if the public sector entity focuses too much on creating diversions but fail to secure the rest of its network, then that negates the safeguards created through deception, he explained.

Hackers also prefer to scan huge portions of the Internet looking for weaknesses they understand instead of targeting a few organizations, so by creating honeypots, the agency may attract unwanted attention from cybercriminals instead, he said.

Active defense not a substitute

The security watchers also pointed out that active defense does not replace traditional security strategies.

Foeckl, for one, said while active defense measures such as deception and active response may be more efficient than usual methods, it still depends on the organization's IT infrastructure, security needs and the tools it uses.

If active defense on its own had worked better, companies would have gotten rid of the other defenses such as firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS) and rely [solely] on them instead, noted Luis Corrons, senior technical director of Panda Security's PandaLabs.

At the end of the day, companies have to assess the risk of being a target and the investment they need

to do commit in order to develop an active defense strategy, Corrons said.