Cisco: Careless Atitudes Help Cybercriminals

Written by Marco Attard
23 January 2015

According to Cisco users fail to patch or update their software-- leaving their organisations wide open for increasingly sophisticated attackers able to take advantage of such glaring security gaps.

"Defenders, namely, security teams, must be constantly improving their approach to protect their organization from these increasingly sophisticated cyber attack campaigns," the company says. "These issues are further complicated by the geopolitical motivations of the attackers and conflicting requirements imposed by local laws with respect to data sovereignty, data localisation and encryption."

The Cisco 2015 Annual Security Report says 60% of survey respondents do not patch, and only 10% run the latest version of Internet Explorer. On the other hand 90% are "confident" in their security capabilities, even if it should not be the case. It surveys security executives from 1700 companies in 9 countries, namely the UK, Germany, Italy, the US, India, Japan and China.

Cisco also names the top 3 cyber attack trends of 2014-- Snowshoe Spam (attackers send low volumes of spam from a large set of IPs, avoiding detection and leveraging compromised attacks in multiple ways), attacks via less common exploit kits and malicious combinations of Flash and JavaScript.

Singled out as a particular risk in 2014 are end users downloading from compromised sites. According to the survey such downloads lead to a 228% increase in Silverlight attacks and a 250% increase in spam and malvertising exploits.

What can be done to fix such a situation? Ultimately, defenders need to realise their security readiness is in need of a check, not to mention increase awareness of vital patches and updates. After all Heartbleed might have been the landmark vulnerability of 2014, but 56% of all installed OpenSSL versions remain over 4 years old.

Cisco also lists what it calls a "Security Manifesto," a list of security principles to help boards, security teams and users better understand current cybersecurity issues.

1. Security must support the business.
2. Security must work with existing architecture – and be usable.
3. Security must be transparent and informative.
4. Security must enable visibility and appropriate action.
5. Security must be viewed as a "people problem."

Go [Cisco 2015 Annual Security Report]