HealthManagement
Promoting Management and Leadership

Staff Download Malware Every Four Seconds

A leading IT security company has found that there has been a 282 percent leap in costs related to healthcare breaches since last year. In spite of this only 54 percent of healthcare organisations have put their data breach response plans to the test a Healthcare IT News report says.

An increasing quantity of malware is being inputted into the IT ecosystem that traditional security techniques do not have the power to prevent, says said Check Point President Amnon Bar-Lev.

The rise in malware attacks is largely down to employees accidentally installing malicious software onto the company network. More worrying is this happens at a rate of every four seconds claims a recent Check Point report on security.

Worked out by the hour, this adds up to 971 unknown malware downloads per hours compared to 106 per hour in 2015. Common routes for network breaches are through staff mobiles or malicious Wi-fi.

See Also: **Comparing Countries' Approach to HIT**

Fr its latest report the company analysed more than 31,000 Check Point gateways to pinpoint malware trends and threats being faced by organisations, the effect of successful breaches on organisations and the financial impact beyond immediate remediation costs.

Check Point researchers discovered healthcare records have the highest value on the black market compared to credit cards. Furthermore, healthcare security incidents rose 60 percent in 2015 which triggered the 282 percent increase in costs connected to breaches.

The Check Point report said that while compliance protections for doctors, nurses and administrators with access to data but limited knowledge of cybercrime techniques was important, the focus needed to shift to IoT and access control protections.

The most common characteristics of breaches were:

- Hacking via email (75 percent);
- Bypassing gateway firewalls (39 percent);
- Undiscovered until after breach (85 percent).

"Innovations like cloud, mobility and IoT are changing the way we deploy, the way we consume, and the way we secure technology," Amnon Bar-Lev, Check Point's president said in a statement. "More and more malware is being put into our ecosystem that traditional security techniques are powerless to prevent."

"Given this, staying a leader requires being one step ahead of things you cannot see, know or control - and preventing attacks before they happen," he added.

Source: HealthcareITNews

Image Credit: dnaindia.com

Published on : Tue, 27 Sep 2016