Cyber failures spark search for new security approach

May 24 2014, by Rob Lever

With cybersecurity's most glaring failures in the limelight, many experts say it's time for a new approach

With cybersecurity's most glaring failures in the limelight, many experts say it's time for a new approach.

In recent weeks, the security community has been rocked by news of a massive breach at online giant eBay affecting as many as 145 million customers, following another that hit as many as 110 million at retailer Target.

A US indictment earlier this month accused members of a shadowy Chinese military unit for allegedly hacking US companies for trade secrets, a charge denied by Beijing.

The incidents highlight huge gaps in cybersecurity, or the ease in which malicious actors can break into a single computer and subsequently penetrate a network or cloud.

"The old model (for cybersecurity) doesn't work," said James Lewis of the Center for Strategic and International Studies.

"It is getting worse and getting out of control... One of the dilemmas is that when people have a choice between security and utility, they often choose utility."

A survey released Wednesday by the security firm Trustwave said it identified 691 breaches across 24 countries last year, with the number of incidents up 53.6 percent over 2012.

"As long as criminals can make money by stealing data and selling that sensitive information on the black market, we don't expect data compromises to subside," the report said.

Much of the problem stems from so-called "phishing" attacks in which emails are disguised as coming from a trusted person.

When links are opened, hackers can install malicious software allowing them to control a computer, and potentially an entire network.

A report by security firm Symantec found a 91 percent increase in targeted "spearphishing" attacks in 2013 and said more than 552 million identities were exposed via breaches.

IBM recently unveiled a new cyber defense system aimed at thwarting attacks before they happen, with predictive analytics.

Symantec suggests a similar approach touting its platform "that aggregates and correlates unfiltered alerts from a diverse set of technologies, harnessing global threat intelligence to detect traffic patterns associated with malicious activity," according to a blog post by Symantec's James Hanlon.

Hardware security approach

But others in the cybersecurity community dispute that approach.

The idea of predicting and halting attacks "is utter nonsense," said Simon Crosby co-founder of the security firm Bromium, which uses a hardware-based solution that isolates computers to prevent the spread of an infection.

Crosby told AFP he views as unlikely "the ability to pick through the noise to find a bad guy before he does bad things."

He said Bromium offers a better solution "by making the system defend itself by design."

Johannes Ullrich, a researcher with the SANS Institute, said hardware isolation "is a solid approach," but just one of many new options being explored.

Ullrich said that in hunting for malware, "you cannot come up with a list of everything that is bad, but what you can do is enumerate what is supposed to be there."

This "white list" approach has a higher chance of success, Ullrich said.

'Hunting ghosts'

The old notion of using anti-virus software, which updates itself based on new malware "signatures," is rapidly losing credence.

A 2012 study by the security firm Imperva said most software only detected around five percent of malware. Another firm, FireEye, concluded last year that 82 percent of malware disappears after one hour and 70 percent exists just once.

"With the half-life of malware being so short, we can draw the conclusion that the function signature-based AV (anti-virus) serves has become more akin to ghost hunting than threat detection and prevention," said a blog post by FireEye's Zheng Bu and Rob Rachwald.

Ullrich said that over time, companies need to invest more in information security and develop strategies before the problems subside.

"Security will never prevent every single breach," he said. "You want to keep it at a manageable level, to stay in business. That's what security is all about."

Citation: Cyber failures spark search for new security approach (2014, May 24) retrieved 26 April 2024 from https://phys.org/news/2014-05-cyber-failures-approach.html