CSO

NEWS

Layered defenses largely fail to block exploits, says NSS

Research lab finds a mix of products from different vendors is best for 'defense in depth'

By John P. Mello, Jr. | Follow
CSO | May 24, 2013 8:00 AM PT

Security experts have long touted a layered approach to cyber security as the most effective way to thwart network intruders, but the strategy can be less effective than the industry would like organizations to believe, according to a report released this week by NSS Labs.

A comparison of cyber defense technologies -- next-generation firewall, intrusion prevention systems and endpoint protection -- shows a "significant correlation of failures to detect exploits," noted the study, authored by NSS Labs Research Director Stefan Frei.

"Such detection failures present a serious challenge to the security industry as they allow an attacker to bypass several layers of defense using only a small set of exploits," NSS reported.

[See also: Three steps to properly protect your personal data]

When security products are layered, it's expected that the combined effect provides a more effective shield. While NSS's research shows security can improve, there's a wide variance as to how much better it gets.

In its study, NSS looked at 37 security products from 24 vendors and layered them in pairs, creating 606 unique combinations. Only three percent of those combinations were able to detect the 1,711 known exploits used in the test.

"Layered defense is still good to do," Frei said in an interview. "However, what we found was the products that you combine is of paramount importance. ...You need to really know what products to combine."

One pitfall to avoid with layered security is using products from the same vendor. That's because all of a single vendor's products are based on the same technology and security intelligence.

"Failure correlation between products from the same vendor is extremely high," Frei said. "If you want to benefit from layered security, you have to mix different products from different vendors."

The problem with introducing multiple vendors into an environment is you're also introducing additional complexity. "Naturally, the more complex it is, the more you have to understand your environment," McAfee Executive Vice President and CTO Michael Fey said in an interview.

For example, you need to know the detection methods used by the products you're layering so you don't duplicate them across the layers. "You're wasting your money if you use the same detection type multiple times," Fey said.

"If you're using something like blacklisting multiple times," he continued, "you're not getting anything for that extra effort."

"You have to make sure your layered model actually does diversify your defenses," he added.

Careful attention must also be paid to an individual vendor's technology because all vendors aren't created equal. "You have to be very careful to choose vendors that put the best intelligence into their products," Joe Stewart, director of malware research at Dell SecureWorks, said in an interview.

Shared threat intelligence plays a role in the dismal performance of many of the product combinations tested by NSS, according to the report.

There is a significant correlation of failures to detect exploits between security products. "This is because most vendors use the same sources of threat intelligence and the same vulnerability research feeds as each other, and this means that they will, more often than not, have the same deficiencies in their coverage," NSS reported.

John P. Mello, Jr. — *Contributor*

John Mello writes on technology and cyber security for a number of online publications and is former managing editor of the Boston Business Journal and Boston Phoenix.