The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. The views expressed in this column are the author's and do not reflect the position of the ISSA, the ISSA Journal, or the Editorial Advisory Board.

It Is Time for New Thinking and Different Approaches to Cybersecurity

By Zuly Gonzalez

Humor can be a great way to communicate with people about serious subjects. One good example of this is the series of TV ads currently being run by a big identity theft-protection company.

We have all seen these ads. One shows a guard in a bank during a robbery. One of the customers lying on the floor says to him, "Do something." His response: "Oh, I'm not a security guard; I'm a security monitor. I only notify people when there's a robbery. There's a robbery."

Besides being clever and funny, the company's ad captures a shortcoming in traditional security products and communicates it very clearly. Then the narrator asks the question: "Why monitor a problem if you don't fix it?" Perhaps the more important question to ask is "Why monitor a problem, when it makes more sense to prevent it?"

This is the very same question that we in information security should be asking today, especially cybersecurity. It's time to start thinking differently about new ways to solve these classic problems.

Why now? Do we not have a decent handle on cyber threats and attacks? The answer is a resounding "No!" as is made clear by even a cursory look at recent industry statistics and trends. Security spending is already substantial and continuing to grow rapidly, yet attacks are growing at an even faster pace and succeeding quite often. The reality is that traditional, detection-based security approaches are not working well.

Today's pervasive detection-based approaches are largely reactive. That is to say, they provide solid protection against yesterday's known attacks, but they are essentially useless against the new attacks of today and tomorrow. Reactive, detection-based approaches can only protect you from what they already know is bad. Additionally, taking a reactive approach means that malware is detected only after it has already penetrated an organization. At that point it is too late.

That is why we need some "the-world-is-round" type of thinking around cybersecurity. To put it another way, it is time we recognize the obvious and irrefutable fact that we need new and more effective ways to combat new and unrecognized attacks.

This is especially true in the web browsing realm, which is the source of around 85 percent of all malware today.[1] Trying to discern which websites are good or bad, or which parts of those websites are safe, is an endless game of catch-up that the good guys just cannot win.

Isolation: A new approach to an old problem

Instead of focusing on hunting down the possible evil, a better approach is to prevent ALL web code from ever reaching a user's computer. That is the idea behind isolation-based security, specifically browser isolation.

Browser isolation essentially creates a terminal point that is the end of the line for all website content. It is a place safely removed from the network being protected. None of the web content goes any farther than that terminal point, which is an isolated virtual machine either hosted in the cloud or in an on-premise server. What does continue on to the final destination – the users' computers – are graphic representations of that content. To the end user, those representations look, act, and respond exactly like the actual website does, but no website content ever reaches the user's computer. When a user's browsing session ends, the entire virtual machine, and any malware it may have encountered, is completely destroyed.

The elegance of this approach is that it eliminates the need to try to determine whether a website or specific web content poses any threat. Browser isolation treats all sites and all content as potentially dangerous, and stops any of it from reaching the user's computer. With this approach, users can view and interact with web content as they normally do – without the potential risk of compromising endpoints.

Why detect threats when you can stop them?

Browser isolation is a radically different but highly effective way to mitigate the significant web-based malware threat. To gain this protection for their organizations, leaders need to be open minded about new, innovative approaches to classic problems that have been plaguing the security industry for decades.

As the bank customers in that TV ad might say, "Don't just recognize the problem. Fix it." With browser isolation, organizations can do just that.

About the Author

Zuly Gonzalez is co-founder and CEO at Light Point Security. Previously, she was a program manager at the NSA. She has decades of experience in cybersecurity and national security as both a practitioner and a manager. She may be reached at zuly.gonzalez@lightpointsecurity.com.

[1] Chris McCormack, "The Four Rules of Complete Web Protection," Sophos, Dec. 11, 2011 – https://www.sophos.com/en-us/medialibrary/Gated Assets/white papers/sophos4rulescompletewebprotectionwpna.pdf.