
WORLD

Home :: Tech Primers

Is it time to start hacking the hackers?

By Sara K. Gates, Founder and CEO, Wisegate, special to Network World

Network World | Aug 29, 2013 3:30 PM PT

RELATED TOPICS

Tech Primers

COMMENTS

INSIDER

In the light of unprecedented attacks by cybercriminals against businesses that span every industry, this question has come to the fore: Is it time to fight back?

As the Founder and CEO of Wisegate, a private, expert peer group for senior-level IT executives, I get to work with some of IT's best and brightest security professionals and have a ringside seat to the discussions that unfold.

RELATED

ERM: Old concept, new ideas

IT security experts share their tips for managing vendors

Verizon Enterprise chief: We're headed for cloud computing's Arlist

on IDG Answers

Can we literally fall in love with our tech devices?

networkworld.com

Is it time to start hacking the hackers?

Sara K. Gates, Founder and CEO, Wisegate, special to Network World

5-7 minutes

By Sara K. Gates, Founder and CEO, Wisegate, special to Network World

In the light of unprecedented attacks by cybercriminals against businesses that span every industry, this question has come to the fore: Is it time to fight back?

As the Founder and CEO of Wisegate, a private, expert peer group for senior-level IT executives, I get to work with some of IT's best and brightest security professionals and have a ringside seat to the discussions that unfold.

Wisegate member Jeff Bardin, Chief Intel Officer at Treadstone 71, says "hacker groups and disruption of business has reached an all-time high and no longer can be ignored. We want to get the 'adversary' to understand that if they launch an attack against a company, there will be costs to pay."

[ALSO: 12 white hat hackers you should know**]**

But members not in favor of going on the offense point to the issue of attribution as a major reason why it won't work: it's too difficult to pinpoint the location and source of many cyberattacks. Yet many security experts say there are some "offense-like" tactics that can

drive up the cost of hacking into a corporate network and, if deployed properly, could discourage hackers enough to have a major impact on the threat landscape.

There are interesting questions being raised about how far businesses can go and what types of attacks can actually be effective, says Wisegate member Martin Zinaich, Information Security Officer of the City of Tampa. “It doesn’t necessarily have to go from nothing to launching a full out assault against cybercrime infrastructure. It could be much more subtle things like feeding the bad guys misinformation or doing your own reconnaissance.”

In fact, many Wisegate members believe there are offensive security measures the good guys can leverage. Misdirection tactics, for example, can be deployed by heavily targeted companies, such as those in the financial or defense sectors.

“We need to start thinking like our adversaries, to look at different approaches and techniques to confuse an attacker,” said Wisegate member Tim McCreight, CISO for the Government of Alberta. “We’re looking at using ethical or ‘white hat’ hackers to check our defenses, and we’re approaching our program like we’re trying to break into our systems. We need to adopt this mindset, and keep focusing on risks.”

Unfortunately, offensive security tactics may have their drawbacks as well. Some companies may want to refrain from specifically targeting hackivist groups since it raises ethical questions and the legality of the practice. In addition, building phony systems and fake credentials may be too costly to deploy.

Wisegate members agree it's hard to agree whether "hacking back" is an acceptable enterprise defense practice when no one can

agree what the term means. Offensive security is huge but relatively undefined and it's compounded by the fact that the laws governing it are vague.

I believe this topic is critical. While hot button issues will be raised and flames fanned by the media, it takes time to think through the best responses to issues our IT leaders are facing. It takes time for the issues to be raised in the trenches and substantive opinions to be developed.

The single most important key to fighting cyber crime will be harnessing the collective intelligence of the good guys in our industry. If we can garner the collective intelligence of these practitioners, all things are possible.

Gates, Founder and CEO of Wisegate, is a respected industry veteran of several start-ups and large enterprise IT companies, including VP of Identity Management at Sun.

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.

Follow everything from Network World