Researcher Puts Quantitative Measurement on Information Security Threats

Editor's Desk: Score One for Threats

A power company's security researchers shed new light on prioritizing threats though quantitative analysis.

Microsoft and Oracle are generous enough to regularly provide severity ratings on vulnerabilities. And automated vulnerability assessment, configuration and patch management tools have made flaw-fixing run of the mill.

That's a good thing.

But we're all resource-strapped, right? And we know those severity ratings aren't universal. My critical flaw is your moderate it-can-wait-until-next-month bug. Can you afford to solely rely on a generic vulnerability scanner to prioritize how your security organization patches systems?

Maybe it makes sense to concentrate more on the threat portion of the risk equation (you know the one: risk = asset value * vulnerability * threat). What if you could put a quantitative score on threats specific to your environment? What if those scores were based on relevant intelligence from law enforcement and some of the best minds in security?

Well, in another testament to the notion that some of the brightest security research is coming out of the nation's critical infrastructure operations, researchers at Pacific Gas and Electric Company in San Francisco have done just that.

Seth Bromberger, manager of information security at PG&E, and his team of security experts have fine-tuned a homegrown methodology for quantitative threat analysis that enables them to prioritize and trend where threats are coming from--something most companies do informally today, mostly on a gut instinct.

Bromberger's motivation at the outset was a better understanding of the threat landscape for critical infrastructures, and a solid score on the NSA's INFOSEC Assurance Capability Maturity Model, or IA-CMM (PG&E earned the second highest rating ever given by NSA). Ultimately, he's developed a threat model that could apply to any organization.

PG&E's methodology begins with a standard definition of a threat agent--which aligns with that used by the DoD--as any person, process or entity that wants to do your organization harm. The secret sauce in this recipe is the proprietary and confidential intelligence from federal and local law enforcement and security experts feeding the methodology.

Threats are divided into broad categories, including insiders, script kiddies, nation-states, terrorist groups and forces of nature, among others. Threat capabilities are then considered, with assigned scores ranging from 0 (no known capability) to 5 (no threat more capable). Areas of capabilities are also applied, such as an attacker's institutional knowledge, technical proficiency, group size and funding, and levels of access.

"The benefits are not only immediate and enable us to refine our prioritization of remediation activities, but now we're beginning to see a huge advantage in longer-term trending," Bromberger says. "Last year, we may have been worried about five particular threat agents; this year, it's five others. This enables us to more precisely target the implementation of our compensating controls."

Gene Schultz, CTO of High Tower Software, has advised Bromberger on the project. He says most threat modeling is more theoretical and academic. "What makes what Seth is doing so valuable is they consulted with people and organizations who are experts on threats to really understand how threats are manifesting themselves," Schultz says.

If there are points to challenge with this methodology, you could start with the fact that the intelligence gathered on threats has a shelf life and must be updated regularly. Also, you must consider the weekly labor-intensive demands of processing hundreds of pieces of updated vulnerability intelligence.

"It's difficult; this is only as good as the qualitative data you feed it," Bromberger says.

Bromberger says, with management's continued support, PG&E may publish the methodology once it has been subjected to more peer review.

"One advantage to this methodology is the cost of development and implementation; this is labor. It's about brainstorming and bringing people together," he says. "It's just a matter of rigor, and if it demonstrates a level of security that gets you a 3 on IA-CMM, I'd say that's worth it."

This was last published in March 2008

Dig Deeper on Enterprise Risk Management: Metrics and Assessments

ALL NEWS GET STARTED EVALUATE MANAGE PROBLEM SOLVE

- Information Security Science
- Information Security Analytics
- IBM's Watson for Cyber Security puts a new face on machine learning
- How to use threat intelligence metrics to attain relevant data

Load More

Start the conversation

Send me notifications when other members comment.

Add My Comment