FEATURE

How to Prioritize Threats (Without Spending Big Bucks)

An internally developed risk matrix helps utility company PG&E figure out which vulnerabilities to focus on first

By Robert McMillan

CSO |
APR 17, 2008 7:00 AM PST

Like many other security professionals, PG&E's Seth Bromberger gets up every morning and faces a serious case of information overload. Not a day goes by without the report of some new software bug or security vulnerability. Weekly bug reports have jumped from just a handful of issues a few years ago to more than 400 in a typical week.

But what to do with all this information? And how to decide which problems need to be fixed first? Two years ago, Bromberger, manager of information security and his security team at PG&E, started developing a threat assessment system that would answer this question. It's inexpensive, easy to maintain and--most important--it helps him sleep at night.

Like most organizations, PG&E had a pretty good handle on vulnerabilities, but the utility company didn't really have a great way of measuring threats--evaluating the odds of whether anyone was likely to actually exploit the problem.

[Learn 8 pitfalls that undermine security program success and 12 tips for effectively presenting cybersecurity to the board. | Sign up for CSO newsletters.]

This is a common state of affairs, according to Eugene Schultz, CTO at High Tower Software, a company in Aliso Viejo, Calif., that specializes in security event management appliances. "That's because we don't really understand threats very well, and what we don't understand, we tend to gloss over."Bromberger puts it another way. "There's a question as to whether there's any benefit in measuring the threat," he says. "If you know you have vulnerability, do you really care about the threat?"

PG&E decided that it did, in part, because it had to develop a rational way of prioritizing the vulnerabilities. So Bromberger met with his staff, and over the course of just a few days they hammered out a first draft of a risk matrix for his company. (He guesses it took about 150 hours of labor.) First they identified close to 40 "threat agents." These can be things like disgruntled employees, nation-states, nature itself or even journalists. When a vulnerability is identified, PG&E looks through this matrix and determines which of these agents have the capability of exploiting the issue.

Here's how the matrix works: Bromberger's team rates the capabilities of every threat agent, giving each one a score between 0 and 5. A nation-state would have a "financial" capability of 5, but a "PG&E institutional knowledge" capability of, say, a 1 or a 2. Then when vulnerabilities crop up, the team decides what kind of capabilities are needed to exploit them, using the same scale. If a known threat agent has the capability to exploit a known vulnerability, it gets priority treatment.

The best thing about the system is that even if it misjudges a threat, the security team can adjust the matrix. "Even if the methodology were flawed, we'd be able to reproduce it," Bromberger says. "I wouldn't have to stand in front of management and say, 'We felt that or we thought this.' It is unambiguous."

Next read this

- *10 essential skills and traits of ethical hackers*
- *The 10 most powerful cybersecurity companies*
- *How to test the impact of new Windows DCOM Server authentication*
- *CISOs' 15 top strategic priorities for 2021*
- *The new math of cybersecurity value*
- *7 tenets of zero trust explained*
- *Tabletop exercises: Six sample scenarios*
- *12 security career-killers (and how to avoid them)*

- *5 steps to security incident response planning*
- *10 essential PowerShell security scripts for Windows administrators*

Microsoft's very bad year for security: A timeline