Software watchdog working on enterprise security metrics

Ellen Messmer

11 Sep 2008 • 00:00 • News • General

The Center for Internet Security is devising new metrics that companies can use to evaluate their security status, including measuring how many systems are properly patched and how long it takes to recover from a security incident.

CEO Bert Miuccio says the non-profit group, which crafts software implementation benchmarks, intends to publish its enterprise security metrics by year-end.

'There have been metrics defined in the security community in the past, usually lists of things to be measured in terms of security, such as technical [attributes], people and processes,' Miuccio says. 'But there's still a struggle to understand the value of security investments, in terms of outcomes, to determine the security status of an enterprise.'

Miuccio says the security benchmarks the Center for Internet Security is working on will be 'unambiguous.' They'll revolve around eight principal topics:

"¢ Mean time between security incidents.
"¢ Mean time to recover from security incidents.
"¢ Percentage of systems configured to approved standards.
"¢ Percentage of systems patched to policy.
"¢ Percentage of systems with antivirus.
"¢ Percentage of business applications that had a risk assessment.
"¢ Percentage of business applications that had a penetration or vulnerability assessment.
"¢ Percentage of application code that had a security assessment, threat model analysis, or code review prior to production deployment.

Miuccio adds that the Center for Internet Security will continue its work producing benchmarks for software security. New benchmarks for secure configuration of Microsoft Office and SharePoint, print drivers, the open source Tomcat application and the three Web browsers Internet Explorer, Opera and Firefox are to be published in the fourth quarter as well.

Some organizations view security metrics as a way to show evidence of secure practices to both themselves and business partners.

'The purpose of the IA-CMM is to gauge an organization's effectiveness in delivering security to its clients, meaning anyone who uses its services,' says Seth Bromberger, manager of information security at PG&E. IA-CMM calls for a tough exam by an authorized outside firm to evaluate an organization's security as documented and executed.

PG&E, which was evaluated by Security Horizon, late last year, achieved a '3' ranking out of a top score of '5.'

While at first glance that may sound average, only one company has ever achieved a '4,' according to Bromberger, and that's International Network Services. Under the tough IA-CMM ranking system, a '3' means an organization's security as documented and executed is 'well-defined,' and Bromberger is extremely proud his organization could even make it through the IA-CMM evaluation to achieve this ranking.

'This gives us credibility when we discuss the merits of our security program,' Bromberger says. 'It lends additional credibility when we talk to the government or utilities about exchanging information on security. From a practical perspective, it's a tool that gives management confidence.

Related content

- **Operators eye post-paid offers for prepaid**
- **Mobile apps, emerging CE devices top agenda**
- **Systemic approach to end-to-end**
- **Mobile Asia Congress shifts back to Hong Kong**
- **GSMA introduces online community for Mobile Money**

Rating: **5** ★★★★★

Share

Comments

Add a comment