The Center for Internet Security

The CIS Security Metrics Service

July 1

2008

Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS has established a consensus team of industry experts to address this need. The result will be an independent, metric framework and service to define, collect and analyze data on security process benefits and outcomes.

Service Overview

Contents

Introduction

Cyber threats and attacks are on the rise and becoming ever more sophisticated. The TJ Maxx security breach and DNS cache poisoning of recent memory illustrate the need for tighter cyber security to not only keep up with such attacks but to proactively prevent them. The results of attacks can be devastating for all parties involved: customers' private data is at risk or tampered with, business' reputations are often damaged, trust amongst customers is destroyed sending them to competitors, and millions of dollars must be spent to fix the breach and its many consequences.

To remedy this growing problem, our goal is to develop practical, security outcome metrics to enable businesses and organizations to make cost-effective security investment decisions. Furthermore, since there are no standardized security outcome metrics currently in place, it is our aim to become the definitive source for standardized metrics for use amongst all industries and sectors.

Background

Whether it is for personal or organizational purposes, it is clear that global cyber infrastructure serves as an indispensible tool to conduct human affairs; individuals and organizations now depend almost wholly on consistent access to information.

Therefore, information must be consistently available and the cyber infrastructure that supports its access must be fully functional on demand.

The concept of electricity and the power grid can be applied here: success is measured by available electricity and the grid functioning as designed when needed.

After expending considerable resources in recent years to improve cyber security, legislators and senior executives in both the public and private sectors responsible for allocation of said resources have begun to raise questions regarding the effectiveness of these expenditures:

> ***What are the business benefits for current and alternative efforts?***
>
> ***Which measure(s) should we pursue to achieve a desired business benefit?***
>
> ***How do we spend a given budget to obtain the greatest benefit from available resources?***
>
> ***Which effort should be implemented first to maximize business benefit?***

These appropriate and timely questions motivate us to define and measure the results (outcomes) of our cyber security efforts. The primary focus of efforts to date has been on the use of so-called "best practices" and compliance with them.

Consequently, there is scant information on the correlation between the benefit(s) of various best practices and actual security outcomes.

Until greater knowledge is available, making cost-effective security investment decisions will continue to be an intuitive process rather than one based on hard data.

The primary desired outcomes of cyber security are: (1) a sustained reduction over time of the frequency and severity of security incidents, defined as operational interruptions (Availability) or unauthorized access to/disclosure of/tampering with information (Confidentiality and Integrity); and (2) a basis for correlating specific security practices with incident reduction to make better security investment decisions.

Generally, an unacceptable outcome indicates that one or more of the processes that produced that outcome needs improvement. Monitoring the outcomes of enterprise security practices via outcome metrics constitutes a critical feedback loop required for improving those outcomes over time. This feedback mechanism is a fundamental and indispensible characteristic of the competitive free enterprise system.

The CIS Security Metrics Service

Goals

CIS's successful use of the consensus process in producing widely used security configuration benchmarks is being employed to:

(1) Achieve community consensus on a small number (fewer than 10) of unambiguous business outcome and process security metrics, and

(2) Provide an operational security metrics service that enables: communication of internal security performance over time, anonymous inter-organization comparison of security status, mechanisms for organizations to determine security practice and outcome benefits to capacitate more informed security investment decisions in the future.

Initial Scope

Key criteria were established for the initial set of consensus metrics. They are a balanced combination of outcome and practice metrics measuring:

(1) The frequency and severity of security incidents,

(2) Incident recovery performance, and

(3) Use of security practices generally regarded as effective. Developing metrics that utilize data commonly available in most enterprises was recognized as a practical consideration.

Requirements

Critical requirements for participant submission of their metric values were also recognized as key factors. They include:

(1) Privacy and assurance that individual data values cannot be traced back to their identity,

(2) Protection against the submission of non-legitimate data by non-legitimate submitters, and

(3) Provision of a robust set of analysis and reporting features.

Solution

To fulfill these requirements, the CIS Security Metrics Service is designed with the following core features:

(1) Anonymity of data submitter,

(2) Strong authentication and validation for syntactical as well as semantic validity, and

(3) The first integration for security metrics of several specialized open source technologies for business intelligence, statistical processing, spreadsheet-based data analysis, visualization, and the semantic web.

Security Metrics Consensus Team Progress

Accomplishments

A team of over 60 government, private, and academic experts have been working to reach consensus on a small initial set, fewer than ten (10), of security outcome and practice metrics.

At present these are not fully and unambiguously defined metrics, only concepts. They represent outcome and practice areas of security regarded by the consensus team as important yet subject to further refinement by the team.

Currently, the team has achieved agreement on developing metrics in the following conceptual areas:

Outcomes

Mean time between security incidents

Mean time to recover from security incidents

Processes and Practices

% of systems configured to approved standards

% of systems patched to policy

% of systems with anti-virus protection

% of business applications that underwent risk assessment

% of business applications that underwent penetration or vulnerability assessment

% of application code that underwent security assessment, threat model analysis, or code review prior to production deployment

Metric Schema

A security metric schema has been developed that will serve as a structure for the final definition of each metric so that terms, definitions, and computational aspects are unambiguous.

Future Benefits

Once a significant volume of outcome metrics data is available, a number of important purposes will be served:

(1) The ability of organizations to compare their outcomes against the distribution curves derived from data populated by other entities, thus creating an intrinsic improvement mechanism by invoking the desire to remain competitive and innovative.

(2) The understanding of practical benefits and effectiveness of "best practices" such as monitoring information flows, risk assessment models, patching, configuration, and maturity models, as they affect the reduction of the frequency and impact of security incidents. In that respect, business outcome metrics will serve as the learning and feedback loop that is currently missing from these practices.

(3) The provision of a rational basis for making cost-effective security investments.

(4) The sustained downward trend over time of security incidents impacting the availability, confidentiality, and integrity of information needed by users of the cyber infrastructure through wiser security investment decisions.

Contact

If you are interested in actively participating as a member of the virtual, CIS Security Consensus Metrics Team or have questions, please contact Steven Piliero at spiliero@cisecurity.org .