NOTICEBORED

Management briefing on

Malware metrics

"A few well-chosen metrics can be a huge help in monitoring controls and measuring their effectiveness"

Clint Kreitner, SANS

Summary

This paper outlines metrics that may be used to measure and set targets for controls against viruses, worms, Trojans and other forms of malware, using the international standard code of practice for information security (ISO/IEC 27002) as a guide to the controls.

Introduction

Malware may be *the* most significant information security risk overall since malware is prevalent, vulnerabilities are common (with controls being imperfect) and the impacts of incidents can be serious. Malware attacks number in the millions every day and the effects can be readily seen in aspects such as the avalanche of spam generated from myriad "botnets" each comprising hundreds or thousands of compromised machines, and the fraud losses from identity theft resulting from keyloggers and Trojans. New types of malware emerge every few months and increasing interest from organized crime is a sign of the potential to make money from malware.

Measuring and improving the organization's response to malware is therefore an important management function. The maturity of an organization's malware controls, and hence their success in minimizing the costs of malware incidents, might even be taken to indicate the effectiveness of the organization's overall information security management system.

Malware control requirements (targets and limits)

Section 10.4 of ISO/IEC 27002:2005 "Protection against malicious and mobile code" states the control objective: "To protect the integrity of software and information." It goes on to note that software and IT facilities are vulnerable to malware (called "malicious code" in the standard) such as viruses, worms, Trojans and logic bombs, and recommends precautions (controls) to prevent, detect and correct malware.

Several malware controls are 'suggested' although none are actually mandated by the standard:

- Policies prohibiting unauthorized software and managing the malware risks associated with using external networks and storage media, indicating the controls;
- Reviewing the content of systems supporting critical business processes and investigating unapproved files or unauthorized amendments;
- Installing and regularly updating antivirus software (ideally from more than one vendor) on all relevant systems to check files on electronic or optical media, received over networks, email attachments, downloads and web pages;
- Procedures, responsibilities and awareness to deal with malware protection, training users, and reporting and recovering from incidents;

- Preparing business continuity plans to handle malware incidents, including data and software back-up and recovery arrangements;
- Procedures to stay up to date with evolving malware risks;
- Procedures to verify malware warnings and avoid circulating hoaxes;
- Avoiding the introduction of malware during IT maintenance and emergency procedures.

The controls fall loosely into two categories:

1. Manual controls such as policies, procedures, responsibilities, awareness *etc*.
2. Technical controls, primarily antivirus software.

Metrics corresponding to these two categories will enable us to measure the controls. These and further metrics are described below.

In relation to malware targets and limits, stopping *all* malware incidents may seem like a laudable goal but it is practically impossible to achieve in practice due to severe disruption to business processes and the associated high cost of control. At the other end of the scale, insufficient investment in malware controls will lead to a significant number of avoidable incidents and costs. Management may therefore define targets for the maximum acceptable rate of malware incidents (such as "No more than 1 major and 5 minor malware incidents per calendar year") which will naturally suggest the associated metrics, provided 'major' and 'minor' and 'malware incidents' are reasonably well defined.

An economic target might state that "Malware control costs must be less than the costs of malware incidents", implying that both types of cost must be tracked, accumulated and reported. It is not easy in practice to determine all the costs associated with incidents although they may be estimated – the more accuracy that is demanded, the higher the costs incurred in measuring.

One issue affecting all malware targets and metrics is the variability of the rate and extent of malware incidents.

Measuring and reporting on malware (metrics)

Manual control metrics

The presence or absence of policies, procedures, guidelines, awareness materials, training notes *etc*. is easy enough to measure but is a poor guide to the quality and suitability of the documentation, and an even worse guide to the level of compliance by employees. Awareness metrics may be worthwhile, measuring familiarity with and understanding of the malware risks and controls, while compliance may be assessed using self-assessment checklists and independent audits. 'Relative' metrics should also be considered *e.g*. "Are the malware policies, procedures *etc*. and the level of compliance better or worse this period than last?", with some explanation of the differences.

Technical control metrics

The 'coverage' of antivirus software (*i.e*. the proportion of relevant systems that are protected) may be interesting and not too difficult to measure. The currency of virus signature files *etc*. is probably worth tracking too: we would suggest measuring the 'update half-life' being the time from release of each new signature file to update half the population of systems, to de-emphasize the tail of systems which are not often on the network and hence are limited risks.

Malware incident metrics

These are what most people tend to think of when asked about virus metrics, namely the number or rate of virus infections. Slightly more insight comes from comparing the number of infections against the number of viruses (and other forms of malware) detected and blocked, making the point that effective antivirus controls are preventing almost all malware attacks.

As noted above, the costs of malware controls and incidents may be measured and reported, provided suitable processes are implemented. Here are some of the cost elements to consider:

Control costs	Incident costs
• Man-days spent evaluating, implementing, maintaining and operating antivirus software, procedures *etc*., plus the associated training and awareness activities • Antivirus software license charges • Cost of the processing and storage overhead caused by antivirus software • Cost of measuring, reporting and discussing malware metrics	• Man-days spent investigating and resolving incidents • Lost productivity and consequential losses while infected networks and systems are disinfected and restored • Other costs such as loss of/damage to data • Cost of reporting and discussing malware incidents (possibly including external reporting) • Intangible costs relating to loss of trust in the IT systems

'Confidence' metrics

A rather different style of metric involves surveying people regarding their confidence in malware controls, for example:

How confident are you that our malware controls meet the business needs? Please mark the following percentage scale at the appropriate point, in your opinion.

0% 50% 100%

|----------+----------|

Not at all. Not quite enough | Just about enough Absolutely!

Comments *e.g.* what led you to this score? Have there been particular situations or malware incidents that influenced your decision?

It is a simple matter to measure percentage values from each response and calculate the mean score. Provided enough survey forms are completed (ideally more than 30), the results should be statistically valid. The comments can provide useful feedback and quotations for use in management reports and other awareness materials.

Reporting malware metrics

An effective reporting approach might be a 'heat-map' consisting figuratively of a background outline representation of the entire suite of key business processes and/or major IT systems and locations, with transparent overlays for various aspects including one for malware. Various elements would be picked out on each layer in color, with annotations to explain the specific ratings and highlight particular improvements or outstanding issues. These might be presented on a web page with tabs for each overlay.

Executive dashboards are also in vogue, using more or less sophisticated database and presentation applications to analyze and report on underlying metrics. No matter how flash the output, however, their value absolutely depends on the quality of the information feeds and the analysis performed, while management's response to the information determines whether the pretty graphs and dials are anything more than a distraction.

Conclusion

The suggested metrics are intended to help you derive creative and useful measures for your own situation. Do not underestimate the value of presenting and discussing metrics with management. The dialogue can be very effective at teasing out any underlying issues and concerns on both sides, and it promotes adequate investment in information security.

For more information

Please visit Information Security's intranet Security Zone for further information on malware. Additional security awareness materials and advice on this topic are available from the Information Security Manager. NIST's Special Publication 800-55 "Security Metrics Guide for Information Technology Systems" includes an extraordinarily comprehensive list of possible metrics, while Andrew Jaquith's book "Security Metrics" is a more pragmatic and useful guide.