NOTICEBORED

Management briefing on

Email security metrics

Summary

How effective are the controls protecting us against email security risks? This briefing outlines techniques to measure the effectiveness of email security in order to relate business results to the investment in email security and optimize the level of security in practice.

Introduction

Email security is a little easier to measure than many other aspects of information security because the threats and incidents are relatively frequent, unfortunately.

Email security requirements (targets and limits)

- **Spam** – even the best anti-spam controls are unlikely to block 100% of spam emails, especially without also blocking some proportion of genuine non-spam emails. A reasonable target may be to block at least 90% of spams and to block no more than 2% of genuine non-spam emails. These figures show a bias towards allowing false negatives since the impact of spams arriving in inboxes is much less significant than the risk of blocking genuine email.
- **Email-borne malware** – likewise, antivirus controls must balance the risk of false negative and false positives but here the former (viruses getting through) is more significant than the latter. Reasonable targets may be to block 98% of malware and to block no more than 5% of malware-free emails. The targets may be broken down into types of malware (*e.g.* virus, Trojan, spyware) at the risk of overcomplicating things.
- **Unauthorized disclosure of sensitive information** – some information disclosure is more-or-less inevitable given the volume of emails but it is reasonable to set limits on the number of disclosures that cause serious incidents *e.g.* no more than one unauthorized information disclosure by email incident in any quarter that is assessed as "serious" or "critical" by the CIO. A target to identify at least 80% of plaintext (unencrypted) emails containing sensitive information may help drive through the technical controls necessary to scan email content.
- **Email service up-time** – this target may already be included in Service Level Agreements for IT. If not, limits may be defined for the frequency and length of email service failures *e.g.* no more than one unplanned email outage per month and no unplanned email outage to last more than 30 minutes. This sidesteps the issue of planned email service outages which may be necessary for backups, configuration changes, security patches *etc.* – if email services are critical to the business, it may be worth setting targets for these too, particularly for outages that are planned for normal working hours.
- **Legal disputes involving inappropriate emails** – it is not unreasonable for management to say that there should be, say, no more than one incident per year involving substantiated allegations of threatening behavior, harassment, sexual discrimination *etc.* by email. Such a target would send a clear message to employees and would reinforce policies in this area.

Measuring and reporting on email security (metrics)

Spam metrics

It is generally straightforward to measure and report the numbers and proportions of incoming (or indeed outbound!) emails that are identified and blocked as spam, using figures obtained from the anti-spam software. These numbers tell a story about the general effectiveness of the technical anti-spam controls. With a bit more work, numbers can also be obtained for false negatives *i.e*. spams that are delivered to email users, either counting IT Help/Service Desk calls or counting spam complaints to an automated internal spam reporting system (*e.g*. the number of spams forwarded by email users to spam@organization.com or whatever).

Email malware metrics

It should be possible to extract the number of virus-infected emails/attachments that are blocked from the antivirus systems, and report it as a proportion of all emails scanned. The number of actual infection incidents resulting from infected emails may be counted from IT Help/Service Desk call records or other sources, depending on the process for reporting/resolving malware incidents.

Unauthorized email disclosure of sensitive information metrics

This is probably the trickiest metric of the set to collect, since (a) the definitions of "unauthorized", "sensitive information" and "disclosure" are all subject to interpretation; and (b) there is no obvious way to automate the collection of data on the proportion of emails containing sensitive information *unless* an email content scanning system is in use. Manual sampling of emails is likely to be tedious, costly and may itself constitute an inappropriate disclosure of information (to the person doing the checks).

Email service uptime metrics

Conventional IT SLA processes should provide this information. Tap in to the existing measurement processes wherever possible.

Email security combined metric

For executive level reporting, it is possible to combine multiple metrics using weighted averages and similar techniques into a single metric. A far simpler version is the classic "traffic light reporting" using red-amber-green to denote the general status of email security. This is subjective and depends on the integrity of the person doing the classification, but has the advantage of ease and low cost. It helps to outline the incidents or issues that contribute to amber or red scores.

Confidence metrics

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

How confident are you that email security meets 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 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

We have probably all seen the voluminous IT service metrics produced by some organizations – pages and pages full of busy tables and colorful graphs. They are often seen cynically as a defensive mechanism to conceal or gloss-over problem areas and justify claims that Service Level Agreements or contractual terms have been met. However some managers genuinely prefer this style of report. They like to check the details.

Others prefer high level summaries, red-amber-green 'traffic light reports' for example. These can either be written summaries with colored blobs identifying the status of each section, or graphical reports using the relevant colors. An effective reporting approach might be a 'heat-map' consisting figuratively of a background outline representation of the entire suite of key business processes, with transparent overlays for various aspects including email security. 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.

Conclusion

The metrics and reporting methods noted in this paper have hopefully stimulated you to derive creative and useful measures for your own situation. Do not neglect the value of having someone present and discuss reports with management. The dialogue that ensues can be very effective at teasing out any underlying issues and concerns on both sides. Why not present and discuss these ideas with your management and seek their opinions, bringing to the table some prototype reports in one or more formats to stimulate discussion and clarify their objectives? Better that than to prepare your reports blindly with no idea whether it is even read, let alone useful for management.

For more information

Please visit the information security intranet website for further information. Additional security awareness materials and advice on this topic are available on request from the Information Security Manager. NIST's Special Publication 800-55, a 99-page "Security Metrics Guide for Information Technology Systems" includes an extraordinarily comprehensive list of possible metrics.