CSTL's informative guide to Message Security

=Other Guides available are:

• End Point Security

• Network Best Practices

Electronic communications - email being the most obvious example, but also new technologies like instant messaging - are critical to business operation. The slightest interruption to service access can have a big impact on productivity. Without email, orders could be missed customers let down and colleagues frustrated. But even if you feel that your business could carry on without email access for a day or two, have you considered the damage that email borne viruses, trojans, phishing attacks and other malware could have on your operations? Crashes, data theft and loss are all very realistic possibilities. And as regulations focus increasingly on email security and data retention, losing mail archives becomes not just an operational problem, but compliance issue, too. Fact: Email has become the foremost file transport medium

Email Protection

As email has become the most commonly used file transfer protocol, the inherent risks with electronic files come with it. These typically and unsurprisingly manifest themselves as malicious code such as viruses, spyware, and trojans. We won't dwell on the details of these, but needless to say securing messaging requires adequate malicious code detection. To detail every scenario would be unfeasible, but below are some commonly overlooked issues. An email may have a web link, which when clicked on downloads malicious code. Note the email itself has no attachment or damaging content and as such slips past email gateway AV scanners. An email may have an attachment that cannot be scanned by a simple AV scanner, for instance if the file has embedded file content, is encrypted or has been multiply compressed, rendering it un-scannable.

CSTL Key Recommendation

• Ensure email is scanned at the gateway in both directions and that the scanner has the ability to detect viral, spyware and trojans.

• Ensure the scanner can distinguish between compressed and embedded file types and can block encrypted email.

• Prevention is better than detection and a policy of blocking file types based on the executable nature is better than trying to detect malicious code within them.

• Review other associated communication mediums such as web browsing, Instant

Messenger, Wifi and Potable memory device, as these require the same level of protection as email communication; otherwise the analogy of "Only as strong as the weakest link" comes into play. There is ongoing industry rhetoric that guidance documents such as Acceptable User Guides (AUGs) should be distributed to all

staff explaining what email can and cannot be used for. Our experiences show us that such guides are seldom studied by staff and that without an ongoing education and awareness programme they are next to useless other than as a stick for HR departments to chastise staff after the event.

Productive Email & Communications

Email is a double edged sword in that it may be a useful communication tool but it can also be an intrusive and distracting medium that results in lost time and wasted resources. Spam is an example where email causes lost time and frustration at the work place, as is its use for distributing offensive images or text such as pornography, defamation, racism, and bullying. IM is now also adopting such bad practices and the term SPIM describes unwanted IM messages, which are beginning to be a real issue. However, probably the worst offender after SPAM is web browsing abuse as the internet provides a distraction for most staff.

CSTL Key Recommendation

• Adopt a SPAM blocking solution at the gateway and if possible deploy at the internet level as this ensures your bandwidth is not clogged with emails that nobody wants. The industry is full of solutions that offer statistics to measures their effectiveness in terms of SPAM detection and false alerts. The devil is in the detail and a thorough review of the fine detail, in particular the SLA (Service Level Agreement), is important to confirm what would happen if the solution fails.
• Ensure a cohesive and ongoing awareness programme to educate staff is implemented: a simple tweak of a staff hand book with little other guidance is next to useless.
• Add disclaimers to email to absolve the users' opinions from those of the organisation. It may not stand up in a court of law but the mitigation of blame may reduce the consequences
• Use controls on file types and email body searching to pin point misuse of email such as for profanity and pornography and look to apply such controls to web browsing and IM. Unless you have the resources to deal with every blocked email based on textual or pornographic detection, it may better to 'audit & review' as opposed to 'block & judge' as it is less resource intensive. The key though is to conduct the audits regularly and publicise the results.

Archiving and Control of Email

One of the biggest issues with email that has crept up on most organizations is that staff expect emails to be available no matter how old or large. As such the email systems begin to struggle as storage increases. Even a moderately small user company can quickly outgrow the
suggested MS Exchange server store quota. Removing old emails to backup only leads to issues of wasted time in restoring the files when a user requires them. Other complications are the use of PST (Personal Stores) files where email archives are distributed around the network on workstations. The associated problems of backing up such distributed stores and managing their integrity and availability becomes next to unworkable. Compliance is a term that is often misused, but in this context refers to the ability to demonstrate adherence to either specific regulatory requirements or accepted industry good practices in relation to message retention and availability.

CSTL Key Recommendation

• An archive solution should complement the email system and not replace it. Both have distinct tasks that should not be compromised. A solution should ensure that the storage load on the email server is removed and ideally compressed in the process.

• If compliance requirements dictate the ability of users to delete emails or retrospectively edit sent emails then a solution that supports journaling is necessary.
• The end user experience of archiving and retrieving emails from the archive should betransparent with no obvious difference to they way they work.
• Review other communication mediums such as IM and where compliance pressures apply, either denying or apply archiving to such messages.

Our approach is one of consultative and education and welcome the opportunity to have informative and informal discussion with you, being independent from any single vendor allows us contrast the many options and provide real world insight.

You can request a meeting at our city demo suite or at your offices now on: security-info@cstl.com
Alternatively for further information on Message Security please contact CST on:020 7621 7832