Global Information Assurance Certification Paper

Secure Messaging: Communicating securely in an insecure world.

Kyle Weber
December 14, 2003
GIAC Security Essentials, version 1.4b, option 1

Abstract

Just not that long ago many organizations' pure existence relied on the US Mail system and other specialized carriers to ensure their highly sensitive information was delivered securely. This information was delivered to partners in business, other offices within the same organization, as well as, their customers.

In today's world we have that same reliance, if not greater, on email messages and attachments being delivered securely. In the past, however, there was not the same fear of compromise as there is today. If you sealed the envelope you had a feeling of security and you had little worry of data compromise. With email that feeling of security is no longer there.

> "Without specific content protection, e-mail messages over the internet are as secure as postcards. If security is important, precautions must be taken in order to secure the content."
>
> - Gartner

In this paper I will discuss the Secure Messaging space. I will cover how to get started with your Secure Email implementation effort including who the players are in your organization. I will discuss Business and Technical requirements that should be considered when selecting a vendor product and I also will highlight a few vendors to give you an idea of what is available in the market today.

What we all must come to realize

The world is not secure as it once was. The new wave of criminal is upon us and he is finding ways to exploit our data. This is especially true when it comes to the data we share via email. It is such an easy tool to use and ease of use brings ease of compromise. Today we must take that extra precaution to ensure for ourselves that the messages we are sending have the extra security required to protect our sensitive data. Not only must we do this to protect our trade secrets but we must also do this as a result of the many laws coming about as we retain the sensitive data of our customers.

Whatever the tools deployed or the methods followed, vigilance in planning, execution and maintenance is the key, states Julie Lancaster, director of marketing for Visualware, Inc. Email as the killer application for companies will not be going away, after all, so neither will email hazards.

"As it is now a critical component of any IT environment, establishing a strong email security policy will become even more essential, and businesses, will need to continually define procedures, educate employees, and update the policies as needed," she explains. (Armstrong, Illena "Email Security: Juggling the Risks".

May 2002. Retrieved: 15 December 2003. URL: http://www.scmagazine.com/scmagazine/2002_05/cover/cover.html)

Getting Started

Solutions in place today:

One key to getting started is to find out what solutions are currently in place in your organization today. Is this the first attempt to securing email or have there been other implementations that will need to be replaced or integrate with your newly implemented enterprise solution? In many cases larger organizations have implemented their own PKI of which they are using in part the secure messaging capabilities. Many other solutions have also been sold and implemented in this infantile technology. If you find that you have one or more solutions in place don't feel like you are the only one out there, so many others are in the same boat.

Filling the gaps or big bang approach:

Once you have determined what solutions are currently in place you need to figure out if you are just looking for a solution to add to your company's offerings or are you looking to take the bull by the horns and implement a company wide solution that includes decommissioning the currently installed solutions. This can become a significant political battle for some organizations. Those that have spent the money to implement a PKI may be hard fast at getting the most for their money out of this expensive monster. Others may simply be willing to cut their losses and move forward with a simple companywide solution. You must however determine where your organization stands on this issue and what they are looking for in a solution.

Players:

Next step, who are the players? Obviously you have an interest in this technology and more than likely you have a sponsor working on your behalf. Bottom line is unless you and or your sponsor are calling all the shots you must get involvement from many other areas in your organization. Here is a list and a good place to start so you can get that commitment and buy-in early in your project's lifecycle:

- Legal
- Purchasing
- Hardware/Software support areas
- Owning area of this technology once implemented
- Business Areas within your organization
- Key Partners in Business (outside entities your company communicates with)
- Security Policy team
- Testing teams/areas
- Email support team

Gone are the good old days of simply dumping money into IT because everyone has the money and it is the thing to do. Gaining buy-in from your primary business partners from within your company goes a long way when you are trying to sell your ideas and concepts to the group who supplies the dollars and other resources to fund your project. Starting with the list I have provided above will get you off on the right foot. If the business understands it and needs it then you have the battle half won. The next thing is to try and get it higher on the priority list than other important things that must be done within your organization. I can't tell you how to do that in your organization but I can tell you that the more areas within your company that back your idea the better chance you have of receiving funding for your project. Look up grassroots and campaigning in Webster's. If it is good enough and works for the politicians and other political influences then it will work for you too.

What do you need? That is the question.

"To begin, if you aspire to any level of success, you need to make sure you understand 'why' the email security project must exist. Are there specific threats that have occurred in the past that you are trying to prevent? Are there new threats management is concerned with even though you've never experienced them at your organization? Are the threats related to real data loss, customer confidence issues, hacker agents passing through email, or simply bandwidth consumption and abuse concerns?" (Hansmann, Bob "Email Security? Tough, but Do-able" August 2001. Retrieved 15 December 2003. URL: http://www.scmagazine.com/scmagazine/2001_08/cover/cover.html)

Lessons Learned:

A good place to start is take a look at previous implementations, if there are any. This is a resource that many of us do not exploit. If you already have some implementations of secure messaging solutions go take a look at the documentation from the projects that implemented those solutions. You should find some very interesting facts such as; technical requirements for the solution implemented, business area impacts, business area requirements, facts and constraints, potential roadblocks, and most importantly lessons learned. Even if you don't have all this documentation anything you dig up can be of significant assistance to you when planning your project. You should have somewhat of a heads up as to what to expect in your attempt to implement a successful solution. If you do not have the luxury of looking at your own documentation see if any of your business partners are willing to share their lessons learned regarding a similar implementation. There are also many white papers and a subscription to Gartner will offer a plethora of information and things to look out for from an unbiased source.

Business Requirements:

Next step is to determine what your business needs are. Is your company impacted by HIPPA requirements or the California Civil Code? What other legal impacts is your company facing in relation to protecting its data or the data of its customers? This is a great time to begin a strong relationship with your legal department. Not only are they going to be able to assist with requirements around what must be done at a minimum but they may also be able to help you keep from going to an overly extensive solution. More controls usually mean a more expensive solution. As with any security solution you don't want to spend more protecting the data than the data is worth to your company.

" Secure messaging extends far beyond compliance issues. In fact, choices about when to implement secure messaging affect every aspect of banking. Banks that move quickly and aggressively to implement secure messaging – particularly secure e-mail – will have a powerful competitive advantage over those who don't." (Secure Messaging in the Banking Industry: The Business Case, US Banker. August 2, 2003. Retrieved 10 December 2003. URL: http://www.us-banker.com/cgi-bin/readstory.pl?story=20030801USSB598.xml)

At this point you may want to consider an analysis of your email traffic to determine the kind of critical data that is flowing through your email system. You'll want to do this to gain a specific idea of what sensitive data is flowing through your email system. This analysis can look at email flowing in and out of your organization as well as the email flowing internally. This piece is important because you may want to put different controls around the data leaving your companies firewalls than you do the data staying within. Several companies offer this kind of analysis. One of those companies is Zix Corporation™. They offer a service called ZixAuditor®. ZixAuditor® is an assessment service that enables your organization to identify email security vulnerabilities and implement more effective policies and procedures to achieve higher levels of protection. The service also monitors ongoing communications to determine compliance and effectiveness over time. ZixAuditor® helps manage the risks associated with standard of care practices, and provides strategic insight into your organization's email usage and the vulnerabilities associated with its use. This service requires that Zix Corporation™ take a sample of your email data to their lab. You will certainly want to discuss this with your legal and purchasing departments to ensure this is a viable option and if it is viable to ensure the correct contract wording is put in place to ensure the safety of that data.

"Once you have a firm grasp of what the outcome of the email security effort should be, you can truly begin to evaluate solutions. You may wish to consider software-only solutions, or many of the new appliances that are currently available. Regardless, the software and/or hardware components should be evaluated for their ability to address the immediate requirements and their scalability to meet future requirements." (Hansmann, Bob "Email Security? Tough, but Do-able" August 2001. Retrieved 15 December 2003. URL: http://www.scmagazine.com/scmagazine/2001_08/cover/cover.html)

Features:

Now you must determine the features your solution must contain. These can be broken down into: Must have (legal/policy requires), Should have (based on ease of use and required functionality), Future needs (future integration, expandability), etc.

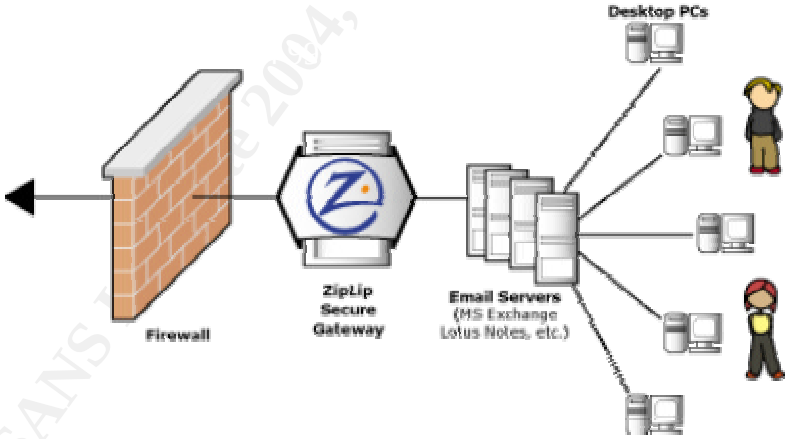
There are many features to choose from. I have provided a sample of those features I feel are important for every organization to consider as they are making a decision on what solution to choose.

- Policy based gateway solution: This solution is great if you want to take the decision making process out of the hands of the users. If you have policy based requirements like HIPPA and the California Civil Code that you need to ensure are adhered to 100% of the time then this is a great solution for you. Several companies offer this kind of solution in different ways. A few companies offer software that you install on your own gateway server and others offer an appliance that you would purchase as a part of a service.

Here is an example from ZipLip® on how a gateway solution is deployed. Keep in mind that this is specifically their solution but the general idea is very similar across the board (Desktop to Email Server to Gateway to Firewall).

Basic Deployment

For the typical enterprise, the ZipLip Platform can act as main boundary control gateway or secure application server.



Graphic: (ZipLip: Technology Deployment Options. Retrieved 15 December 2003. URL: https://www.ziplip.com/technology/deploy_options.html)

- Desktop software: Always a hot topic. Do you want a solution that requires a heavy client or are you looking for a plug-in type solution? The pendulum seems to have swung on this one with many organizations going away from heavy client software to save resources. You may however require desktop software on both ends of the communication channel as this is really the only way to ensure complete protection from end to end.

- API's: Many organizations have a need to programmatically send large numbers of emails. For example you may have secure internet portals that your customers (B2C) and/or business partners (B2B) use. In these scenarios you have a need to send ID's and Passwords through email to the users of that portal. Obviously this needs to be automated and secure.
- Email Portal: Many companies have numerous organizations they do business with. Finding a common solution to use between all these organizations is impossible because each company chooses their solution and vendor to supply that solution. One way to help mitigate that issue is implement a portal for your business partners to come to when they need to communicate with your organization. In most situations all that's required for your partners is an Internet browser with no other technical requirements.
- Branded storage solution: You may not have the resources to host your own portal, so another solution is a hosted and branded storage solution. In this case your organization would use client software integrated with your email solution (i.e. Outlook) to send your secure message. The recipient would receive an email notification that they have a secure message from you. This email would include a link to a secure website branded for your organization yet hosted by the email vendor. The recipient would register and log into the secure site to retrieve their message. Upon reviewing your message they would also have the ability to reply with a secure message back to you.

These are many of the features readily available in solutions currently on the market today. You may choose one that meets your needs or you may incorporate more than one for a fully integrated solution to meet the needs of your organization.

Technical Requirements:

As with any implementation you have to determine your technical requirements as well as your business requirements. The business requirements and technical requirements work hand in hand when your making your decision on which vendor to choose. Following are several examples on the kinds of technical requirements you need to consider.

General Requirements:

- What Email solution must the product integrate with (Outlook, Outlook Express, Netscape Communicator, Lotus Notes)
- Vendor Support (24x7 or otherwise)
- Revocation of users (do you need to be able to handle this internally)
- Secure Communications traveling on an un-trusted Network (require 128-symmetric or higher or lower)
- Must be able to send attachments within the email message
- Must be able to meet performance and availability requirements
- Compression capabilities (need to determine how much overhead your willing to accept)

- Integration with other solutions (If you choose to implement more than one offering from one or multiple vendors then you probably want seamless integration)

Policy Based Gateway Requirements:

- What fields of the email are the policies based on (content, sender, receiver, subject line, etc.)
- Does the company offer reusable packaged policies (i.e. HIPPA, GLB, California Civil Code)
- Hardening requirements
- Performance impact kept to a minimum
- How is technical handled (must your organization administer all hands-on support or do you allow remote support by the vendor)
- What monitory products must integrate with the solution
- Failover and redundancy requirements

Portal Requirements:

- Must support standard web browsers
- Email stored at portal must remain encrypted
- If you are adding this functionality to an existing portal you will also want to integrate the authentication so as to not create a need to re-authenticate when using the email capabilities.
- Support staff's ability to administer mail boxes (create, delete, etc.)
- Do you want the users to only have the ability to read, read and reply, or read/reply and create new messages from this portal?
- Do you limit who a user of the portal can send messages to?

Client Software Requirements:

- Key exchange (does it matter if key exchanges are required?).
- Support of standard attachments.
- Your partners must be able to register and obtain software easily and quickly.
- Support industry email clients.

The skinny on the vendors

A short List:

There are several secure email vendors that offer one or more of the solutions I have mentioned above. Here is a short list of vendors that meet the following requirements: 1. Client software is available but not required, 2. Policy based Gateway solution is available, 3. Portal solution is available.

Note: This list is not intended to be all inclusive.

- Sigaba
- CertifiedMail
- PostX
- Athentica
- ZipLip
- ZixCorp

The details:

Let's take this list one step further and show what each has made available to the market place for us to choose from.

Vendor	Gateway Solution	Portal	Software Solution
Sigaba® http://www.sigaba.com	Solution: Affiliate Gateway Features: • Policy Based • Uses your Key Management and Authentication Services • Transparent to end user • Setup at affiliate site	Solution: Send Anywhere Features: • Configured within Sigaba Affiliate Gateway • Web based user interface • Configurable templates • Integrated content filtering and Virus scanning	Solution: Plug-In • No software required. • Plug-in technology available for desktop-desktop encryption.
PostX® http://www.postx.com	Solution: PostX Enterprise Features: • Provides recipients a choice of email "Push" or web "Pull" for delivery of secure electronic communication. • Supports Outlook, Netscape, Lotus, AOL, Yahoo! mail, Hotmail.	Solution: Websafe Features: • Optional component of PostX Enterprise Platform. • Recipients are sent an email with a link to their online mailbox. • Can be used as a standalone "pull" solution.	Solution: PostX Desktop Email Features: • Integrates with Outlook and Lotus Notes. • Desktop to Desktop encryption
ZipLip® **http://www.ziplip.com**	Solution: ZipLip Integrated Gateway v4.0	Solution: ZipLip ecure – Web Server Component • Non-client recipient can receive secure messages through ZipLip's staged delivery, secure large file delivery, or JS payload methods. Zip Lip Hosting Services ZipLip manages all storage, configuration, network, servers, and database for the service and customers can access through ZipLip's webclient or through standard email clients.	Solution: Plug-In • No software required. • Plug-in technology available for desktop-desktop encryption.
CertifiedMail™ http://www.certifiedmail.com	Solution: CertifiedMail Director™ Features: • Route sensitive messages securely and transparently at the server level with central policies • Integrates with Microsoft Exchange and	Solution: CertifiedMail ASP™ Features: • Send, retrieve, and track emails from any web browser • Oops button retracts emails that have already been sent • Send to individuals or groups of users and know who has	Solution: Send Certified™ Features: • Secure plug-in available for MS-Outlook and Lotus Notes. • Comes bundled with other CertifiedMail™

	Lotus Domino • Central creation of policies • Apply rules based on particular users or group membership	opened your message	products
Authentica® http://www.authentica.com	Solution: Authentica Secure Gateway Features: • Automatic protection and delivery of messages, documents, and files • Integrates with any third party content scanning engine • Securely delivers any file format	Solution: Authentica Content Security Server Features: • No client software required • Support for multiple authentication methods • Secure reply to messages	Solution: MailRecall Features: • Integrates with MS-Outlook, Lotus Notes provide desktop to desktop e-mail protection • No client software is needed • Dynamic control over message forwarding, printing, and copy/paste.
ZixCorp® http://www.zixcorp.com	Solution: ZixVPM® Features: • Policy Based server • Transparent to users (no desktop software required) • Message and attachment compression • Preconfigured policies available (e.g. HIPPA)	Solution: ZixPort™ Features: • Branding available • Recipients can reply securely to messages they receive • Can integrate with your companies Internet portal or work as a stand alone • Integrates fully with other ZixCorp® offerings	Solution: ZixSelect Features: • Integrates with ZixVPM • Allows user to flag an email to be encrypted regardless of the rules of the VPM ZixMail™ Features: • Offers desktop to desktop encryption • Message attachment compression • Messages stored securely

Now you have some basic knowledge on what is available in the marketplace today. The information listed above is only a small portion of the technologies and vendors ready and available to provide you with the solution(s) you need.

The Balance

Balancing the business requirements, technical requirements (constraints), ease of use, ease/speed of deployment, ease of support, cost to purchase, and cost of ongoing support is a tricky thing to do. All these things must be taken into consideration. For your organization you will have to determine which items carry the most weight and give them the highest priority.

The Policy

As with any good security implementation you must include policy updates around this implementation. Depending on the solution you choose you may have to specifically state the shall's and shall not's related your solution. Encrypted Email means more than simply protecting the data of your organization. It can also mean the hiding of inappropriate content within encrypted emails. Depending on the solution you choose you may not be able to easily scan those messages to stop the culprits. Although policy can not keep someone from doing something wrong hopefully it can deter those potential wrong doers.

HIPAA's impact on messaging (including e-mail and instant messaging, or IM) is simple: government-mandated privacy standards mean that messages have to be kept secure and logged. (HIPAA-Compliant Messaging Siemens, Line56.com. July 3, 2003. Retrieved 1 December 2003. URL: http://www.line56.com/articles/default.asp?ArticleID=4790)

The Implementation

The implantation of a secure messaging solution is no small feat. As with most technologies the vendors will tell you that the implementation is seamless, the users won't even know it is there. Well we have all been down that road before. Make sure you take all the precautions that you would normally take with an enterprise solution. An enterprise solution always has its special bumps along the way. Take your time, don't let the vendors rush you and you'll be much happier in the end.

Communication

This is probably the most critical piece to your effort. Keep the communication lines open with the key business departments/areas within your organization, the partners you will be doing business with securely, the support areas in your IT department, and the end users of this technology. Tell them what is coming, tell them the importance of this new technology, tell them the benefits they will see and you'll have a widely supported implementation.

Conclusion

No doubt about it, this is going to be one of the biggest implementations you have been involved with. This implementation may also bring the most benefits of any single implementation that you have seen. Understanding the importance and benefits of secure messaging and being able to talk about it with anyone who will listen is your ticket to selling this implementation and getting the organizational buy-in to get the funding you need. Good Luck……..

List of References

1. Hansmann, Bob “Email Security? Tough, but Do-able” August 2001. Retrieved 15 December 2003. URL: http://www.scmagazine.com/scmagazine/2001_08/cover/cover.html

2. Armstrong, Illena “Email Security: Juggling the Risks”. May 2002. Retrieved 15 December 2003. URL: http://www.scmagazine.com/scmagazine/2002_05/cover/cover.html

3. Secure Messaging in the Banking Industry: The Business Case, US Banker. August 2, 2003. Retrieved 10 December 2003. URL: http://www.us-banker.com/cgi-bin/readstory.pl?story=20030801USSB598.xml)

4. HIPAA-Compliant Messaging Siemens, Line56.com. July 3, 2003. Retrieved 1 December 2003. URL: http://www.line56.com/articles/default.asp?ArticleID=4790

5. Unleashing the Value of Collaborative Portals, IBM Corporation. April 01, 2003.

6. Fong, Kevin “Messaging Goes Mission Critical”, Network World. November 24, 2003 URL: http://www.nwfusion.com/columnists/2003/1124fong.html

7. http://www.sigaba.com

8. http://www.postx.com

9. http://www.ziplip.com

10. http://www.certifiedmail.com

11. http://www.authentica.com

12. http://www.zixcorp.com