Global Information Assurance Certification Paper

Risky Business – Email usage on the Internet

By Anthony Brooking

Preface

This document is based on a presentation given to a large group in September 2000 on the security risks of Internet email.

Introduction

Organizations are, now more than ever before, reliant on their Internet email system for doing business. However they need to ensure that they are able to protect themselves adequately from the many issues, such as the spectre of virus infection, and it's potential to cause harm to their business.

I'd like to highlight the issues and risks of using Internet email, and what you can do to mitigate the risk of using email to do business on the Internet - for many organizations this business has indeed become "risky business".

Email

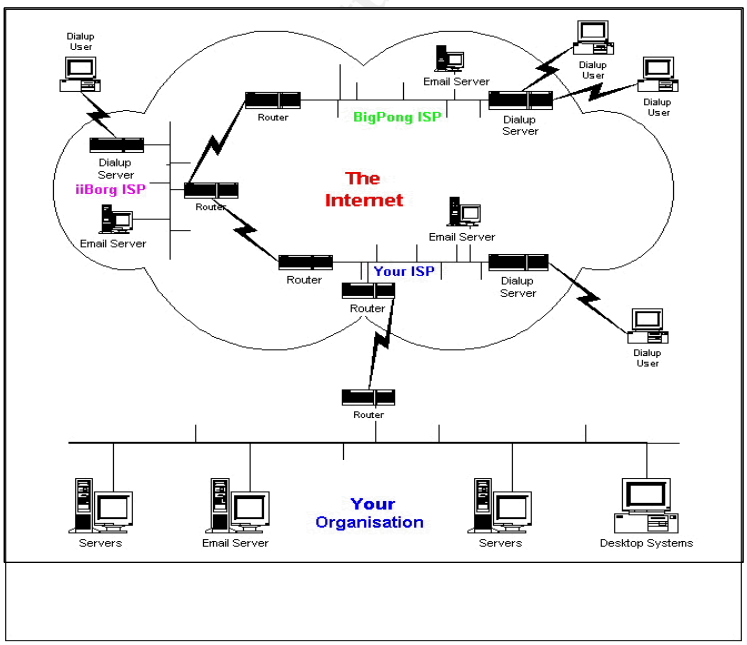
E-mail… Electronic mail … it's been around for quite a few years and is probably the first "E" word coined.

I doubt if there is anyone who that doesn't use it. Everyone uses it. It's an exceptionally useful tool. It's cheap, fast, reliable and efficient. It allows you to bypass most secretaries! It saves you from playing telephone tag! It enables you to attach documents and send them to the other side of the globe in a matter of seconds.

It's now increasingly being used for the procurement of goods, transmitting financial information, lodgments of tenders, job applications, product quotations, …

So let's have a quick and simple look at how it all works…

Shown below is a typical Corporate network connected to the Internet:



You need to send a mail to a client in Zimbabwe… So you type your mail, attach your document, select your clients email address and then press OK.
The mail goes to your email server, it could be a Notes or Exchange server which then converts it to SMTP or Simple Mail Transport Protocol. The SMTP mail does a Domain Name lookup, finds the MX or Mail Exchange record for your client's domain name to determine what SMTP server to deliver it to, and then forwards it to an upstream SMTP server, which is typically your ISP. From that point on it is in the "Internet Cloud" and the route it takes can be quite random. Depending on your ISP and their upstream ISP or the Carrier that they use, and where the eventual destination is located, will determine how many email servers your mail may pass through in the Internet 'public domain' cloud before finally arriving on your client's PC in Zimbabwe.

Notice also that within the Internet cloud there are other people connecting to send and receive their email. When they dialup, they typically use two other mail Protocols, POP and IMAP to retrieve their mail from an email server.

Email Risks
Now that we've seen how Internet email works, lets identify the risks:

Hackers can get access to your network through vulnerabilities in your email system, to get a staging point to attack your network and cause havoc, and/or steal, modify or delete your valuable data.

Viruses – I am sure that you are all more or less aware of the threat that viruses pose to your Organization's. Several of the recent virus outbreaks have made the news and we've all heard the stories of doom and gloom from those affected by the outbreaks.

Trojan horses – so named because like the Trojan horse of Troy, they contain within them something that you aren't expecting. Someone receives an executable file, clicks on it and the rest is history.

You can blame Monty Python for the name of the next one – Spam! Lots of Spam. Spam is typically junk email. A bulk mailing company, or 'Spam Merchants' as I like to call them, has obtained your address and sends you mail that you haven't asked to receive…. and keeps sending more… and continues to send you more and more… This can cost your organization quite a lot of bandwidth, and as we know bandwidth and ISP volume charges add up to a lot of money. What if your email system is used by the 'Spam Merchants' to relay this material, so that all the mail appears to be coming from your domain? This can be mildly annoying, or highly offensive depending on the content of the mail. What if the mail contains sexually explicit or racially vilifying content?

Which leads us on to the next risk – inappropriate usage – what are your employees doing. How are they using your email system. What percentage of use is business

related? Are the picture and executable attachments, the jokes that they receive filling your network servers. Are they offensive? Will the content put your organization at risk of litigation from other employees or other organizations?

Let's look now at some trends that are emerging…

Shown below are results from the last available global Internet vulnerability scan which occurred at the end of 1998. A security group used a tool called BASS – the Bulk Auditing Security Scanner which scanned the Internet address space for 18 of the most common computer vulnerabilities, meaning that they could be trivially compromised by a Hacker. This took just 20 days and scanned over 35 million connected hosts. It identified 450,000 hosts and 730,000 vulnerabilities. I've highlighted the email based vulnerabilities in red.
Note: the wu_imapd, qpopper and bind. IMAP & POP are client based mail protocols – typically used when connecting to ISP mail. Bind is DNS – which used for domain name resolution to IP addresses.

BASS Global Internet Scan

BEGIN TIME:	02:00, Dec 01 1998 GMT	
END TIME:	08:00, Dec 21 1998 GMT	
Scanning nodes:	5	
Jobs Per Minute:	250	
Scan time:	20.24 days	
Vulnerabilities tested:	18	
Domain count:	7 three letter domains, 214 national domains	
Host count:	36,431,374	
Vulnerability count:	730,213	
Vulnerable host count:	450,000	
Service	Vulnerability count	Percentage
webdist	5622 hosts	0.77%
wu_imapd	113183 hosts	15.5%
qpopper	90546 hosts	12.4%
innd	3797 hosts	0.52%
tooltalk	190585 hosts	26.1%
rpc_mountd	78863 hosts	10.8%
bind	132168 hosts	18.1%
wwwcount	86165 hosts	11.8%
phf	6790 hosts	0.93%
ews	9346 hosts	1.28%

DNS has become a favorite target, and there are a number of exploits available. If you are running DNS, I would urge you to read up on the CERT advisories at http://www.cert.org/advisories/ and ensure you are running a current patch level. If a hacker gains control of your DNS, they can cause havoc with your incoming & outgoing mail.

Then there are the POP2, POP3 and IMAP vulnerabilities in dialup ISP mail that can allow attackers to gain control of the PC though integrated products such as Microsoft Outlook. What if that PC was inside your network? What damage could that attacker wreak?

Viruses

The recent revival of the computer virus as a threat has come about thanks to the Internet. In the 80's and early 90's viruses were spread predominantly on infected floppy disks. At the time, very few people had access to the Internet, and sharing floppies between computers was the most effective means of propagation. The early anti-virus software packages more or less put a stop to these viruses and for a couple of years all was peaceful and quiet. Recently, the virus methodology has changed. Now, the majority of viruses are propagated in email, either as infected email attachments or as craftily modified email messages that utilize the integrated nature of today's email programs such as Exchange and Outlook.

The Melissa virus last year caused an estimated $1 billion in damages. This year, the "I Love You" strain of viruses caused and estimated 6 to 10 billion $ in damages, and is still causing damage through its variants.

These viruses spread much more quickly that their floppy-borne ancestors. They overload enterprise mail servers, corrupt corporate data, and consume massive amounts of bandwidth as they propagate themselves over the Internet.

As an interesting 'aside' we are now seeing a cross-over between the virus threat and traditional Internet-based hacking. Some of the viruses that are being distributed via email are "Trojan horses" such as the infamous 'Back Orifice' program which compromises the infected PC and allow hackers to remotely control the system resources, and the Trinoo program that enables infected computers to participate in a distributed denial of service (DDOS) attack against a third parties infrastructure which effectively removes them off the Internet map. You may remember the recent DDOS attacks against the Yahoo, Amazon.com and E-Trade sites.

So what can a virus infection mean to your organization?

If an organization receives a virus infection, the effects could be wide reaching and potentially disastrous. The immediate reaction would be to shut the email gateway. But what if the Organization relies on email for business critical functions? Do you have a standby plan?

Depending on the damage caused by the infection, the associated cleanup may range from the simple removal of the virus from desktops, possibly removing the virus from every email residing on the email servers, through to cleaning corporate file servers or maybe recovering data from the last backup. While this is happening the business could be at a standstill and employees sitting idle.

Again, depending on the type of virus, the virus may have propagated out to partner organizations or clients. This may potentially cause embarrassment or reduce corporate reputation – imagine the results of the Managing Director sending a virus to an executive of another company who are currently involved together in delicate corporate negotiations.

These incidents may also prove to be an opportunity for competitors or the media to highlight your situation.

All of the above scenarios can cause a potential loss of business.
So what about the employees, how are they using the email systems? Do you know what information passes through your email system? Much of the traffic passing through email systems is not work related. Some of this traffic is inappropriate. It may contain pornographic, drug related, anarchistic, racist, sexist, discriminatory, morally objectionable or illegal content. Many Organizations have never let their employees know what is acceptable in email.

Recently there was an incident within the Australian communications carrier Telstra where a number of employees were dismissed for passing pornographic material through email.
There have also been incidents where confidential data has been passed out of organizations using email.

Finally we have the risk of litigation. Libel, defamation and sexual harassment are risks that need to be considered by an organization. There have been several cases in recent years, of organizations being held legally responsible for email that their users have sent. Litigation can have a very high dollar cost, as well as the associated negative publicity that your organization could receive.

So what can you do to mitigate these risks?

Reducing the risk
Each organization has different needs. Identify the areas of risk to your organization. Try and quantify each risk with a dollar figure. This will make it easier to determine the how much to spend on mitigating the risk.

Publish and widely distribute the Corporate security policy. This must have executive buy-in. It should include all levels of the organization. Everyone has their part to play – from the CEO, the CIO, the IT management, the system administrators, the application stakeholders and the end users. Incorporate a virus policy, an incident response policy and an acceptable use policy in the security policy framework. User

education is a very important step in risk reduction. An acceptable usage policy, and adequate training for users is a very good step in reducing the impact of these issues.

Ensure that your network has secure design. Install a firewall at the network perimeter.

Ensure that no POP or IMAP services are allowed to pass through the firewall. Configure the firewall so that all Internet SMTP email passes through an email relay server. This will reduce the ability for viruses to enter your organization.

Apply all vendor security patches to your firewalls, email servers, email relay servers, and Anti-virus (AV) solution. This will reduce the possibility of hackers gaining access by utilizing known program vulnerabilities.

Avoiding the virus threat is a relatively simple matter. There is a large range of commercial anti-virus software available. Anti-viral software suites should cover all entry points to your network server and desktop PC's. AV products provide a second level defense against viruses that may be brought into an organization through other means, such as on floppy disks and CDs. Email gateway and email server AV products scan incoming and outgoing email for virus-ridden attachments and maliciously formed messages. Content control on the email server and email relay needs to be part of the AV solution.

It is vitally important that anti-virus pattern files for all AV products be updated on a very regular basis. New viruses are appearing all the time and the AV products can only defend against the viruses that they know about. Pattern files are published by the AV software vendors every time a new virus is discovered, and these pattern files should be downloaded and incorporated into your anti-virus software on a daily basis at the very least.

Covering all the data entry points to your network will ensure that virus outbreaks are avoided and that individual viruses are contained and reported to your administrators.

Email content control is another means of reducing inappropriate content. Content control packages can filter certain types of email attachments, while allowing others. They can also be configured to filter email messages based on keyword searches – for example you could filter out messages with bad language or abusive or discriminatory content.

Content control can be used to block attachments of certain types. For example if might be possible to block any MP3 attachments to email messages. Content control can be used to filter chain letters and Spam from your email traffic.

The threat of harassment and resulting legal liability can be reduced by implementing email content control. This software can be configured to attach legal disclaimers to outbound email. It can also be used to filter for potentially abusive or inappropriate words in inbound & outbound email.

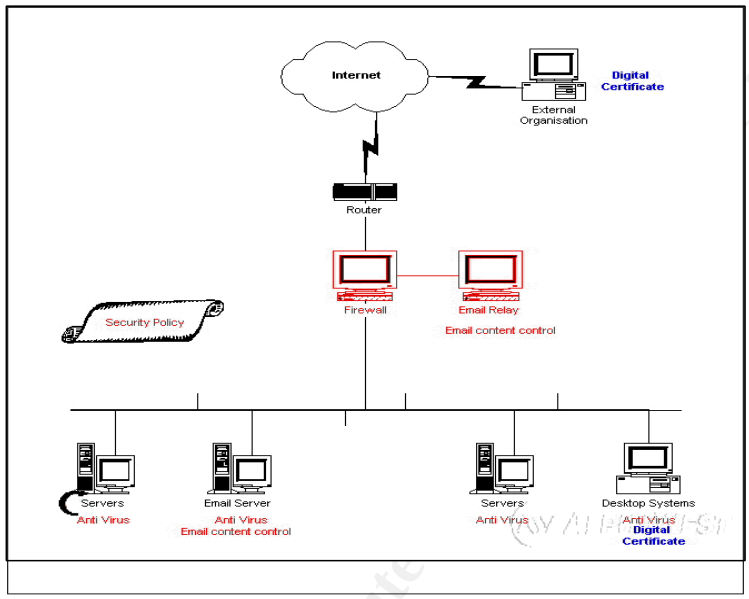
Encrypt your sensitive email. Most email systems can support digital certificates . It is worth noting that you need to ensure that the email recipient is also using digital certificates to allow the mail to be decrypted.

Finally, monitor the compliancy of your Corporate security policies. Following up on policy breaches will allow you to determine how successful the application and acceptance of the policies are, and allow you to fine tune them if required.

Remember: A security policy not actively applied isn't worth the paper it's printed on.

Conclusion

By applying these risk minimization techniques, our typical corporate network now looks a little different…



We identified the risks to the organization… We've installed a firewall.

We've installed antiviral software on all of the internal machines:
Server and desktop edition virus scanners are installed on the servers and desktop PCs. An email virus scanning package is used on the email server.

We've deployed an email relay machine. In this network, SMTP is the only email traffic allowed to enter the internal LAN from the Internet. Everything else originates as connections from within the internal LAN out to the Internet. It is an important security design technique to isolate machines that receive connections from the Internet. The publicly visible machines are the most often compromised by Internet hackers. By placing the email relay on its own network segment, we have reduced the risk to the internal LAN. If the email relay were compromised, the attacker would still need to hack through the firewall to reach the internal LAN.

We've added content control to the email relay. These software packages can be used to enforce policy decisions on all email that enters and leaves the organization.

We've added digital certificates to enable sensitive mail to be encrypted.

Finally, and possibly most importantly, we have defined a security policy. The policy provides and dictates the procedures and principles relating to the organization's computer security.

So now what was originally a "risky business" is now not so risky.

Sources:

Raven, "Computer Trojan horses". URL: http://www.securitywriters.org/texts/internet%20security/trojans.html

Siri, Liraz. "The Internet Auditing Project." 11 August 1998. URL: http://www.securityfocus.com/templates/forum_message.html?forum=2&head=32&id=32

CERT Incident Note IN-99-01. " 'sscan' Scanning Tool". 28 January 1999. URL: http://www.cert.org/incident_notes/IN-99-01.html

CERT Summary CS-99-04. 23 November 1999. URL: http://www.cert.org/summaries/CS-99-04.html

CERT Advisory CA-2000-03"Continuing Compromises of DNS servers". 26 April 2000. URL: http://www.cert.org/advisories/CA-2000-03.html

Dittrich, David. "The DOS Project's 'trinoo' distributed denial of service attack tool". 21 October 1999. URL: http://packetstorm.securify.com/distributed/trinoo.analysis.txt

CERT Advisory CA-2000-04. "Love Letter Worm". 9 May 2000. URL: http://www.cert.org/advisories/CA-2000-04.html

McMillan, Rob. “Lessons Learned from Loving Melissa”. 5 July 2000. URL: http://www.auscert.org.au/Information/Auscert_info/Papers/loving-melissa.html

Last Updated: September 24th, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive