GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Rich Parker
Champlain College, Burlington, VT
Computer and Network Security CIS 378
Gary Kessler, Instructor
GIAC Certification / SANS Security Essentials
Practical Paper Original Submission
11/25/01

When Policies that have 'Always Worked', Don't or "The Mask of the Code Red Death" (with apologies to E.A. Poe)

The challenge

In a small organization the pursuit of a secure and virus free computing environment can be a challenge for those of us who must wear many hats. As Director of Engineering for a statewide public radio network I am responsible not only for our broadcast studios and five transmitter facilities (four on mountain top sites) but also for the oversight of a growing network of office computers, networked audio file servers, and web/email/file servers. To assist me in maintaining this conglomeration of technical equipment I have one broadcast engineer who is primarily responsible for first line transmitter and studio maintenance and an engineering associate whose primary duty is to help maintain approximately 35 desktop computers for office users, including setup of new computers, printers and upgrading software if needed. A critical part of the engineering associate's work involves monitoring the updates of virus signatures on a weekly basis and verifying that users are complying with company policies regarding acceptable software packages for company use.

The scenario I will describe in this paper outlines a failure of our 'human systems' due to a limitation in our thinking about our procedures that could easily have had catastrophic results. What I will describe is a situation regarding one particular software package, but the principle it illustrates I hope will serve as a warning to those of us who may have let our past successes lull us into a sense of complacency regarding the security of our networks.

A practical solution to limited IT resources?

As an important part of our 'defense in depth' for the network behind the firewall, we use standardized software with which we were familiar and had patched against known vulnerabilities, a robust virus scanning software package, and continual education for all of our users regarding the dangers of opening unsolicited email attachments.

The recently published SANS document "The Twenty Most Critical Internet Security Vulnerabilities" points out that one of the dangers of the default installations of most software lies in the fact that they often include installation scripts, sample code and

© SANS Institute 2000 - 2005 Author retains full rights.

unnecessary features that can expose serious vulnerabilities in a system.

> *If you have ever used an installation program to install system or service software (as nearly every company has), and you have not removed unnecessary services and installed all security patches, then your computer system is vulnerable to hacker attack.*
>
> *Even if you did perform additional configuration steps, you could still be vulnerable. You should run a port scanner and a vulnerability scanner against any system that is to be connected to the Internet. When analyzing the results, keep in mind the principle that your systems should run the smallest number of services and*
> *software packages needed to perform the tasks required of your system.*
>
> *Every extra program or service provides a tool for attackers – especially because most system administrators do not patch services or programs that they are not actively using.* [SANS, URL http://www.sans.org/top20.htm, section G1.4 [1]]

Although they are ubiquitous on all Microsoft Windows operating systems installed on machines in our plant, I had as a matter of policy expressly forbidden the use of Outlook for email, or the use of Internet Explorer for web browsing. The default installations of these programs have often been shown to have serious flaws, which in many cases have facilitated and in fact accelerated the spread of various viruses and worms. While there are vendor supplied patches available for these product's vulnerabilities, the labor intensive requirements for verifying that each and every machine is updated promptly when the next 'exploit du jour' is announced made their safe use impractical in a small office environment such as ours.

For document preparation we standardized on Microsoft Office 97, which had more than adequate capabilities for the requirements of our users. When the 'latest and greatest' updates came out and our users began clamoring for new versions of operating systems or Office, I simply asked them to fill out a proposal indicating what functions the new versions had that they required for their daily work which was not currently supported in their version of the software and told them I would handle upgrade requests on a case by case basis. (I received not one single documented request for an upgrade – validating my belief that their desire for the upgrades was merely a response to marketing by software vendors). For virus protection we have a site license for McAffee AntiVirus installed on each user's machine to scan incoming mail and attachments for known viruses.

For email and web browsing, we had chosen to use Qualcomm's Eudora (for email) and Netscape Navigator (for web browsing). When we first made this decision, Eudora was not particularly vulnerable to the kinds of exploits that affected Outlook such as the ILOVEYOU virus and other infectors. While we continually educated our users about the dangers of opening unsolicited attachments in email, one of the early CERT advisories concerning the ILOVEYOU virus indicated, *"...advice to avoid clicking on unsolicited*

© SANS Institute 2000 - 2005 Author retains full rights.

email doesn't help in this case, though it does help users of email programs other than Outlook." [2]

Also, at that time, Netscape Navigator did not support automatic execution of Visual Basic scripts by default, as did Internet Explorer 5. In fact, at the height of the ILOVEYOU virus incident, although many of our users received dozens of messages from friends, loved ones and complete strangers which contained the virus, only one of our users was affected – a sales representative who had upgraded to Internet Explorer 5 on her computer without authorization (with Visual Basic Scripting activated) and who then proceeded to click on the ILOVEYOU attachments several times, all the while complaining that 'nothing was happening'. (It deleted dozens of image files on her computer and on the network share to which she was attached. Thankfully our network files were regularly backed up to tape).

As we added machines to our network (all of which had previously been standardized to Windows 95, SP2 and fully 'patched'), we began to receive machines from vendors with newer operating systems such as Windows 98, Windows ME and Windows 2000 preinstalled. While this presented a challenge in terms of 'standardization' (we had fully patched our Windows 95 installation and were fairly certain that we were aware of any known vulnerabilities), we decided that we could maintain a baseline level of security by turning off functions such as Windows Scripting Host (which formerly had only been active by default for users of Internet Explorer 5 and above) and reinforcing our policies about 'approved software'. We were still trying to defend our network through application standardization as one aspect of 'defense in depth' but clearly things were beginning to become a bit more complicated. Our 'smugness' at having avoided the perils of those around us whose networks were down for hours or days because they 'unwisely' chose to use whatever applications were thrown at them by the software industry was beginning to wear a little thin.

Another change crept in when I was asked to provide the ability to send encrypted email between senior managers for discussion of personnel matters and other sensitive matters. I elected to purchase a number of licenses for Eudora Pro and install the PGP plug-in to allow the sending, receiving and signing of email messages. The user interface was very nice, and seemed to be an improvement over the previous 'freeware' versions of Eudora that we had been using (we are a non-profit corporation). As other users saw this new interface, they began asking if they could get the same sort of package. We decided to download and install Eudora Version 5.x in sponsored mode (free) for our other users. As we had always been confident that Eudora was relatively immune to the dangers presented by Outlook regarding automatic execution of various viruses and worms, we did not have any reservations about installing the newer version for our other users.

I couldn't have been more wrong! A new 'feature' of Eudora that we discovered quite by accident was the concept of the *preview pane.* Users could scroll down their list of email messages and see a 'preview' of the message before they opened it. As it turns out, this had been a feature of Microsoft Outlook for some time. This seemed like a relatively

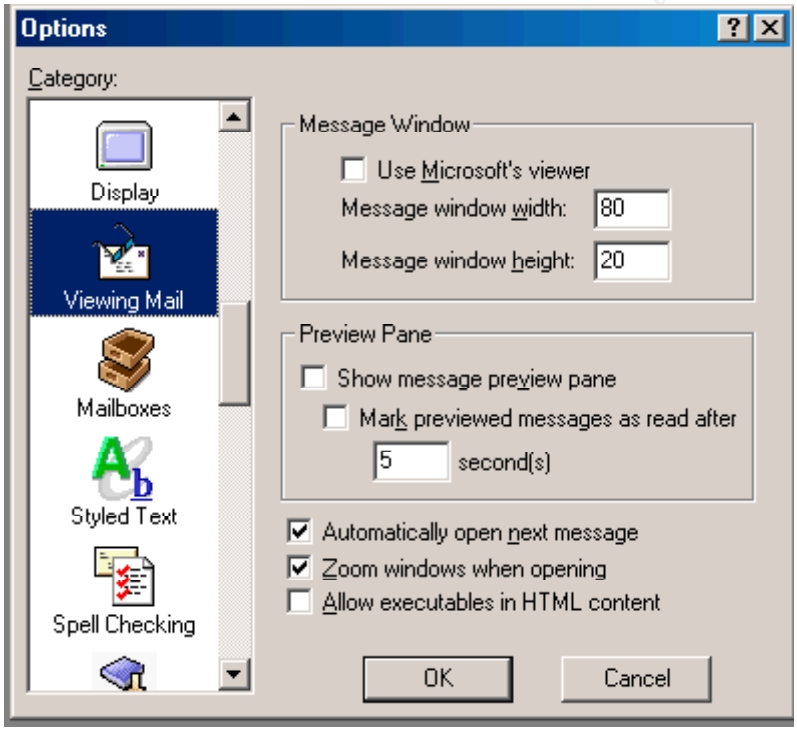
© SANS Institute 2000 - 2005 Author retains full rights.

innocuous addition to Eudora, but it held a hidden danger. One of the default options for the behavior of the preview panes was the ability to 'Use Microsoft's Viewer'. What was this Microsoft Viewer? It was Internet Explorer!

Quoting from the Eudora Help File topic on *Viewing Mail Options Window*:

Use Microsoft's viewer - *If this is off, Eudora displays advanced formatting, graphics, and multimedia in incoming and outgoing messages, using its own built-in viewer. If this is on, Eudora takes full advantage of the Web browser capabilities of Microsoft's Internet Explorer 4.0 or later by showing Web content right in incoming and outgoing messages or linking to the Internet, without your having to open the Web browser. This option is only available if you have Microsoft's Internet Explorer version 4.0 or higher installed and available on your system.* [Qualcomm "Eudora v. 4.3 – Help][3]

The applicable section from Options portion of Eudora is shown below - note the checkbox for "Use Microsoft's viewer. This was (to us) a new addition to the Options for Eudora, and was not a familiar feature or one that at the time we thought needed to be investigated:



[3]

So, now that we had discovered this 'feature, we knew we had a potentially serious problem – the newer computers we were receiving had IE installed at the 'factory' as part of the default installation of Windows operating systems, and by this time (early 2001) they were all using IE at version 4 or higher – many of them were IE 5, with all the bells and whistles turned on. So, even though our users were instructed not to use IE, one of

© SANS Institute 2000 - 2005 Author retains full rights.

our ‘trusted programs’ Eudora was set to use it without our knowledge as an *improved feature*.

What this would mean in practice was that if the checkbox for Use Microsoft Viewer remained checked and an unpatched version of Internet Explorer was installed on that computer, all of the IE vulnerabilities relating to automatic execution of embedded MIME types, html and scripts could affect our users. Even if they received a maliciously encoded email or attachment and never opened it as long as the preview pane was active on their version of Eudora they could be at risk.

And how exactly does this IE vulnerability affect users who might receive malicious email? The following excerpt is from Microsoft’s own web site that explains the problem as it relates to the interaction between Internet Explorer and Outlook – but in this case Eudora is vulnerable as well:

From Microsoft Security Bulletin (MS01-020)

> ***Why is IE used to process HTML mails? I thought mail programs like Outlook and Outlook Express were in charge of displaying mails***.
>
> *In general, they are. Mail clients handle creating, sending, receiving and displaying e-mail. There is one exception, however – they rely on IE to perform a process called “rendering” if the mail is an HTML mail. Rendering is the process of processing and displaying a web page. HTML mails are rendered by IE because they are essentially web pages sent as mails. The flaw in this case involves how IE renders HTML mails.*
>
> ***What’s the problem with how IE renders HTML mails?***
>
> *If a mail contains an attachment, IE should provide the ability to open the attachment when it renders the message. The precise meaning of “open” depends on the type of file. If the attachment is a text file, IE should provide the ability to read it; if it’s a video clip, IE should provide the ability to view it; if it’s a graphics file, IE should provide the ability to display it; and so on.*
>
> *Some types of attachments, such as executable files, are inherently dangerous. In these cases, IE should only open the attachment if the user expressly asks to do so, and confirms that he wants to open it. The flaw, however, enables this safeguard to be circumvented by specifying an incorrect MIME type in the e-mail.* [Microsoft Corporation: 1.7 MS01-020] [4]

© SANS Institute 2000 - 2005 Author retains full rights.

So, our old friend Eudora let us down, and had we not 'accidentally' discovered the problem we might have been unwitting accomplices to the spread of viruses and worms such as Nimda which could be spread through just such a vector, even while we mistakenly thought we were 'safe'.[5]

I should point out that had I done my homework, I might have noticed that this vulnerability in the preview pane and Microsoft viewer had been discussed in the 'help section' of a number of university computing sites, but since we believed that Eudora was a 'safe' program I did not do an adequate research for any vulnerabilities in the newly installed versions. (for example see http://chdccs.ucsc.edu/ResNet/Eudora-win/Eudora5win.htm for a warning to uncheck the 'Use Microsoft Viewer')
In fact, (and particularly for organizations with limited IT resources) I would recommend a regular perusal of the user help areas of various university computing centers as they are often a wealth of thorough and well written information about the proper installation, configuration and disabling of 'dangerous features' for common and widely deployed software packages.

What have we learned?

Defense in depth and complacency are mutually exclusive in any environment. We let ourselves fall into a dangerous pattern of thought regarding the security of our network. Past experience had taught us that many of the outbreaks of viruses and worms were caused by unpatched or default configurations of products like Microsoft Outlook or Internet Explorer. Since we had a company policy that proscribed the use of those products we felt reasonably certain that we had very little risk. What little exposure we thought we had came from users who needed to be constantly educated about the dangers of opening unsolicited attachments. Since we had a very high level of compliance and understanding among our users and a very aggressive program of updating and monitoring our virus scanning software we felt reasonably confident that we were protected. Given the decisions we had to make about allocating resources to IT related issues with no full time staff devoted to that tasks, we felt assured that our current prophylactic efforts were adequate to protect us from any known problems, and our virus scanning software would serve as a next line of defense against new exploits which might occur. In fact, much of our current 'patching' efforts were related to advisories we received from anti-virus vendors and some times CERT or SANS. Due to limitations of time and resources, we simply weeded out those advisories that didn't appear to affect us directly.

When other organizations around us announced that their mail or web services would be down for indeterminate amounts of time due to some infection or another, we smugly congratulated ourselves on our 'wise decisions' and wondered why no one else 'saw the light'… after all, *we* had never had an interruption of our essential network services due to a virus or worm, and we were very proud of our record in that regard.

The introduction of new elements into our network in the form of newly purchased

© SANS Institute 2000 - 2005 Author retains full rights.

computers with vendor supplied operating system software with which we were not totally familiar, and the upgrading of our 'trusted' Eudora to a version with new 'features' added a new layer of complexity and vulnerability that we did not adequately assess. Eudora had never let us down, and a quick check of their website listed no new known vulnerabilities or problems that might affect us. In fact, the latest advisory on their site that might have affected us listed a fix dated April of 2000 regarding adding file extensions for vbs to the facility that warned users before attachments were opened or executed and we had already done that fix. There was (and still is at this writing) no mention at www.eudora.com/security.html of the Preview Pane/Microsoft Viewer issue. [6]

As humbling as this experience was, we were fortunate in that we found the problem before any damage could be done, but I believe we were extraordinarily fortunate. We even failed to see (or look for) a very clear announcement of this vulnerability on the SANS web site which was posted more than a year ago. [7]

Because we didn't use Outlook or IE we simply weren't looking very diligently for MS product vulnerabilities and so missed an important fact. All of our systems use Microsoft operating systems of some kind. We had known for many years that as delivered these systems included Internet Explorer and Outlook, as well as Windows Scripting Host, and other means for the execution of Visual Basic programs and scripts. Our greatest error lay in assuming that because we did not use these products that we could safely ignore them.

We know now that we must also remain vigilant regarding any software that is installed on our machines, whether we use it or not. If it is on the machine, it may get used, either by a user who violates policy or by a software program that interacts with other software in ways that we may not be aware of. Part of our network defense must include making sure that all of the installed programs and operating systems are at their latest patch level and that we monitor vendors' web sites, mailing lists, SANS, CERT and others for announcements concerning vulnerabilities and recommended patches and immediately take corrective action.

To the extent we are able, we must continue to follow the guidelines listed in "The Top 20 Most Critical Internet Security Vulnerabilities" and disable all unneeded functions, scripting and components that are not essential to our users. We must remain vigilant about any new versions of previously 'trusted' software and keep up with not only the vendor announcements, but with postings to security newsgroups. Most of all we must never allow ourselves to be lulled into a false sense of complacency or what may be even worse, snobbery and hubris regarding our policies and procedures. Security is a 'moving target' and what was safe today may not be safe tomorrow. New versions of software are being foisted upon us at an alarming rate, all with new 'features' which may have unexpected consequences. Even in a small company, the damage to time and resources that could have been done by the unchecked release of a destructive virus or worm would far exceed the time for front-end work to prevent the occurrence in the first place.

© SANS Institute 2000 - 2005 Author retains full rights.

Bibliography (URL access times indicate last access to check for availability)

[1] "The Twenty Most Critical Internet Security Vulnerabilities" Version 2.501 November 15, 2001 URL: http://www.sans.org/top20.htm (November 25, 2001)

[2] CERT: "CERT® Coordination Center Fights Love Letter Virus" May 4, 2000 URL: http://www.cert.org/about/loveletter5-2000.html (November 25, 2001)

[3] Qualcomm "Eudora v. 4.3 – Help" program help file topic - "Viewing Mail Options Window"

[4] Microsoft Corporation: 1.7 MS01-020 – "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" March 29, 2001 URL: http://www.sans.org/newlook/digests/ntarchives/033101.htm#1.7 (November 25, 2001)

[5] McAffee: "Virus Profile for Nimda Virus" (evidently) September 18, 2001 URL: http://vil.mcafee.com/dispVirus.asp?virus_k=99209& (November 25, 2001)

[6] Qualcomm: "Eudora Security Advisory" (evidently) November 25, 2000 URL: http://www.eudora.com/security.html (November 25, 2001)

[7] SANS Flash Advisory 'Dangerous Windows Flaw' July 17, 2000 URL: http://www.sans.org/newlook/resources/win_flaw.htm (November 25, 2001)

10 Questions to accompany Practical (5 T/F and 5 multiple choice)

True/False

1) The best security can be maintained by using the latest version of all software.

   False: Often new software is released in response to market pressures and is not always fully tested in a hostile environment.

2) Once you have determined that a particular brand or type of software can be secured to meet your needs, you can be sure that subsequent releases will be safe.

   False: Again, market pressures often may cause vendors to add features that were not present in earlier versions of their software to mimic other vendor's releases and this may introduce unexpected behaviors or interactions.

3) Everytime you install new software it should be tested and examined to ensure that it does not contain any new vulnerabilities.

© SANS Institute 2000 - 2005 Author retains full rights.

True: Even new software from trusted vendors may incorporate features or bugs that were not present in earlier versions.

4) Once you have settled on a set of best practices for your computing environment you can relax and congratulate yourself on a job well done.

   False: Security is a moving target and an ongoing struggle to keep up to date on risk assessment, vulnerabilities and newly discovered exploits.

5) Once you have chosen a set of software tools for your users and they have been instructed in it's proper use, you do not have to bother them anymore with information about it's use.

   False: User education is an ongoing process. They need to be reminded of company policies regarding email, adding programs without authorization, and social engineering ploys (such as giving a password to a stranger on the phone)

Multiple Choice:

1) A user insists on installing the latest Framus Boogie package on their desktop computer. What is the proper way to handle this request?

   a) Tell them to go ahead but to not expect you to support it if there are problems.

   b) Tell them it's not allowed unless the boss says it is ok

   c) Send an angry email to personnel and their supervisor informing them that the user is violating company policy.

   d) Remind them of your company's policy on acceptable software installations for corporate resources and ask them to submit a formal proposal outlining why they need this installation to perform their work.

d: You do have a policy don't you? Although it may take time, it's important to cultivate compliance among you users by having them help you understand what their legitimate needs are and in turn helping them understand what the risks may be to everyone on the network. A heavy handed attitude will often just get them to install software secretly and hope you don't catch them.

2) You discover that a user has been using the latest version of a software package

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

that your company uses because they have it and home an 'it works better'. You should:

a) Angrily berate them via email for violating company policy

b) Send a strongly worded email to them and their supervisor reminding them of corporate software policy.

c) Set up a meeting with them (and their supervisor if appropriate) to go over the existing policy and help them understand why unilateral action is dangerous to the network.

d) Let them use it and then tell them "It's your own fault for not using approved software" if something goes wrong.

c: Similar to the first question, keeping open communication is the key to compliance. In this case it may require more firm measures, backed up by the appropriate corporate authority, to have the software removed until it can be evaluated under the conditions of the previous question. These cases are a bit more difficult and require management buy in and support to enforce. Try to make an ally of the person in your goal to provide a safe and effective computing environment for all users.

3) Your boss wants to use a different software suite from the rest of the company.

a) You let her use whatever she wants (she's the boss)

b) You work with her to determine what her specific computing needs are and if they can be adequately met by the supported software. If not, you carefully explain the additional risks and costs associated with her request and provide the best information about what the tradeoffs are relating to her request in terms of security and network health.

c) You tell her boss that she wants you to violate company policy

d) You quit because you can't take the stress of the confrontation

b: Possibly the most difficult scenario of all – if existing policy does not support you you must make sure that you can explain your reservations while at the same time determining what her legitimate needs may be. If you can show a cost/benefit type of analysis to the change (ie the costs of repairing the network) she may be persuaded that she does not want to be responsible for a budget busting incident that requires you to clean up the network. On the other hand, you need to be flexible and recognize different work styles and offer realistic solutions.

© SANS Institute 2000 - 2005 Author retains full rights.

4) A number of people in the company are convinced (after watching the Super Bowl) that the company simply must have the latest software suite from MegaSoft:

    a) You install it on their machines because, hey, it's their budget

    b) You tell them you won't do it because it's too much trouble

    c) You complain to the boss that they are making your life difficult

    d) You ask them to submit detailed requests for the new package which explains what features it has that your current software does not have that is essential to the continuance of their normal work and evaluate their requests in conjunction with upper management to provide the best work environment.

d: Often this is the easiest way to head off a full scale vendor brainwashing. If the need is legitimate then a testing period needs to occur so you can evaluate the effect the new software will have on your total network environment. On the other hand, if it's just a 'gee whiz' response to clever marketing, it probably won't last.

5) You have always used Glaxxon software because it provides the security and manageability that you need to keep things running smoothly. A new version is released:

    a) You have your assistant install it on all company machines right away

    b) You carefully evaluate a sample copy, check the vendor's website for information about any new features, and check security or bug tracking type web sites to see if there are any problems with this version.

    c) You ignore the release notice because your current version works fine.

    d) You complain about how the companies are always out to gouge you by making you upgrade and talk about how you won't be bullied.

b: No matter how familiar you are with a company's software, things always change. What worked well yesterday may not work adequately today. New vulnerabilities are found every day (how many of you turned off telnet to your Unix machines only to find

© SANS Institute 2000 - 2005 Author retains full rights.

that there was a new exploit for your current version of SSH?) Testing is the key, education and keeping informed by your peers is essential.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.