Ralph W. Coleman

GSEC Practical Version 1.3

"To Be Alerted or Not To Be Alerted-That is the Question"

To Be Alerted or Not To Be Alerted-That is the Question

Executive Summary:
Any one of the jobs as a network, security, or system administrator would be enough to keep a person busy daily in the areas of maintenance or troubleshooting. Unfortunately, most scenarios have a one person trying to fill two or three of these roles simultaneously. Whether you have the luxury of the first scenario or the added pressure of the second, security and bug related alerts should be a top priority. For simplicity's sake, these three positions will be referred to for the rest of this research paper using the single common term, administrator. An administrator must make it a priority to be aware of industry broadcasted alerts concerning system bugs and security vulnerabilities and do so on a daily basis. This issue becomes even more acute in the world Information Technology (IT) contracting because a new trend is beginning to emerge. This trend concerns contracting language, "… that now holds software companies liable for breeches and attacks that exploit their products."[1] Logically, similar contracting language will probably find its way into IT Security Outsourcing contracts soon.

The most interesting aspect of an administrator's job is how to figure out just which alerts are actually needed for a particular IT setup. This research paper will attempt to investigate this subject from several directions. First, the paper will identify what types of alerts are available to an administrator. Second, the paper will discuss what types of alerts does an administrator really needs to glean from those available to do his/her job effectively. Through an overview of how these alert entities function, potential problems associated with the whole process will be highlighted. The research paper will conclude with a summary concerning alerts to the community of administrators.

Types of Alerts Available

Management very naturally views an administrator as the organization's bastion of knowledge for Information Technology (IT) security and bug related issues. Often, whenever a member of an organization's management (or other self-appointed important person in the organization) chances to read an article or see a TV news report hyping the most recent security/bug issue, the same person expects, realistically or not, the administrator to know everything about the issue whether it is relevant or not to the operation of the organization. The administrator is supposed to be able to answer instantaneously whether the organization is vulnerable to that particular security breech. The problem is, this same administrator is usually over tasked and in most cases can barely keep his/her head above the sinking level concerning normal daily tasking and troubleshooting. Thus the administrator has two problems. He/she must recognize bugs and security problems that are truly a threat and deal with these in a timely manner so that the system will not fail. It is just as important to allay the fears of a nervous superior or co-worker about which threats are genuine and which are not and marshal the arguments to back up these opinions.

What types of alerts are available to an administrator so that he/she can be ready? Simply stated, there are commercial (fee based) and there are alerts available free. In both cases, one will often need to subscribe via an online web form in order to receive these alerts. In the next section, both free and fee based alerts will be discussed.

Alert Agency/Vendor Overview
There were two rationales for choosing to review these particular alert services. One was based on this author's own practical, hands on experiences when researching and receiving needed information related to IT security/bug issues he encountered. In this author's case, subscriptions to free alert services and one commercial alert service have been the sources of security/bug information. The other was based on articles and websites accessed in the course of researching this paper.

Free Alert Services:

- **Free, Well Known, Vendor Neutral:**

    - **Computer Emergency Response Team Coordination Center (CERT/CC):**
      CERT may be found on the web at http://www.cert.org. It is a government-funded operation. To paraphrase from a description on the site's homepage, this site and service is a repository of Internet security at the Software Engineering Institute and is currently operated by Carnegie Mellon University. Any person can surf to the site as often as desired for research on recent or old vulnerabilities. The site is vendor neutral although it does have alerts that include vendor specific information. Two types of alerts are CERT Advisories and Incident Notes. CERT Advisories concern vendor related advisories. Incident Notes concern events related to the Internet Community.

      One very important item to note concerning this alert site is how the alerts are released to the public. Alerts are only released after a vendor has had the chance to review the submitted vulnerability about their product and provide guidance or the actual system patch to fix this problem in their product. The CERT web site is also a very useful for security related guidelines on IT products, as well as providing information related to security training.

      An administrator can sign up to receive these alerts via email. This is a tremendous convenience, for it makes news about current vulnerabilities easier to track. And eliminates having to remember to surf to the site looking for new items.[2]

It is very easy for an administrator to receive these alerts via email. The steps are as follows:

- Surf to the site, http://www.cert.org
- Look on the left side of the home page and scroll down until you see the link, 'Advisories & Summaries by Email-The CERT Advisory Mailing List'
- Click on the link
- Once on the next page, find the paragraph entitled, 'Subscribing to the CERT Advisory Mailing List'
- The directions are included below as a convenience as they are short:
    - To subscribe to the CERT advisory mailing list, send email to majordomo@cert.org.
    - In the body of the message, type:
      Subscribe cert-advisory[2]

- **Computer Incident Advisory Capability (CIAC)**
  CIAC may be found on the web at http://www.ciac.org/ciac. This site is funded by the Department of Energy for IT Security Research. The site contains a wealth of information related to IT Security. This site contains both alerts and informational bulletins. Unfortunately, according to the site, CIAC Information Bulletins are released via email only to the Department of Energy community. This is done in order to notify DOE site operators of computer security vulnerabilities and recommended actions.[3]

  Therefore, the drawback in gaining access to this information is that the administrator must manually visit the site. Once there, alert bulletin information related to his/her vendor equipment and software may be found. While not allowed the convenience of email notification, the public user does, however, have the ability to access site sections on virus information, publicly available security related tools, and a section on hoaxes. Using the hoax related section in disproving the many email related hoaxes sent to this author has been very useful.

- **Systems Administration, Networking and Security (SANS) Institute:**
  SANS may be found on the web at http://www.sans.org. This institute was founded as a cooperative research and education organization. The site is publicly assessable and contains volumes of very useful IT Security related information.

The user can search through the Reading Room for a white paper on just about any type of security related need for research or problem solving. A major plus in becoming a part of the SANS community is becoming a beneficiary of security tools created by trusted experts in the security industry. SANS also provides fee-based training that is considered by many in the industry to be the best security training around.

SANS provides several types of alerts email advisories. The administrator and choose from the following:

- SANS Newsbytes (weekly email)
- SANS Windows Security Newsletter (monthly email)
- Security Alert Consensus (weekly email)
- New Alert Emails At the time this research paper was completed, SANS was offering potentially 20 new security related email news letters, voter dependent on most needed. 4

An administrator may easily sign up for these email bulletins by following these steps:

- Surf to http://www.sans.org
- While on the site home page, scroll down to the following section header, 'Security Digest'
- The easiest step to take is to click on the, 'Instant Sign Up for Free Digest Link'
- Once on the new page, read all posted material
- After reading all material, decide upon the needed security related digest by selecting such sections.
- Fill out the personal information section and then click submit
- You will begin receiving the selected digest upon there proper release dates[4]

A helpful tip for the selection of security digest(s) is to also select cross platform digest items. There was a particular incident that occurred with the latest release of the Security Alert Consensus Digest Number 015. There were no Windows related bugs released during the Security Alert Consensus digest creation period for that release. However, there were items in the Cross-Platform section that did affect Windows users. One should not be to focused only on one type of vendor software, operating system, or network device.[5]

- **Free, Well Known, Vendor Specific**

NTBugtraq:
NTBugTraq may be found on the web at http://www.ntbugtraq.com. TruSecure Corporation now funds this site. The site is Microsoft Windows specific and is devoted to the discussion and resolution of vulnerabilities and bugs related to Windows. This author has personally found the site to be invaluable and would recommend it to any administrator working in the world of Microsoft Windows.

The alerts generated by this site are very detailed and will also further explain any Microsoft security and/or bug notices and patches. An added benefit of registering to receive these alerts concerns the access of security related tools created by the site operator and/or members of the list. Best of all, these tools are made specifically for Windows platforms by people in the Windows world. In other words, these tools (usually) do not require a Unix like install and setup to use them.[6]

In order to become a recipient of these alerts, one must perform the following steps:

- Surf to http://www.ntbugtraq.com
- Once on the home page, click on the link at the top of the page labeled, 'List Charter'
- Read the List Charter thoroughly in order to under the specifics related to the site
- Now, click on the link towards the top left of the page labeled, 'Subscribe'
- Your email client will pop up with the 'To' section filled out to listserv@listserv.ntbugtraq.
- NTBugtraq subscribe request will be filled out in the subject line
- The command line needed will be pre-filled out in the email, and is the following: subscribe ntbugtraq firstname lastname
- There may be some follow on confirmation email work, but this is the worst of it. [6]

- **Microsoft:**
Microsoft's security related site may be found on the web at http://www.microsoft.com/technet/security. This part of Microsoft's site is particularly informative for security items related to Window's products. Microsoft has made many security guides and tools available for their products.[7]

As a user of these tools and guides, this author feels they have become less burdensome to use over the last year because they have simply become a better product. Likewise, all of these security related items are free for the moment. Currently, Microsoft's site also has a very informative product alert section. Again, valuable information in the form of product alerts is available for zero cost. In order to become a recipient of these alerts, one must perform the following steps:

- Surf to http://www.microsoft.com/technet/
- Now, on the right side of the page, locate the link labeled, 'E-Mail Notification' and click the link
- Once on the next page, you will be prompted to create a Microsoft Passport in order to continue the registering process in order to receive Microsoft's Security and Bug Bulletins.
- However, I was not prepared to go farther so this author cannot detail the next step is. The next step involved concerned the creation of a Microsoft Passport Identity/Password.[7]
- This author has chosen not create a profile using Passport for two reasons. I do not trust Microsoft to profile me correctly or to maintain my privacy. This may change with time.
- If one feels as this author does on the Passport issue, yet still feels they must still receive emails from the Microsoft Security and Bug Alert Service, then try these two "work around" tactics:
    - Surf to this site several times a day to research any new bulletin releases: http://www.microsoft.com/technet/security
    - Subscribe to the NTBugtraq email alert bulletin notification. Upon receipt from this list there is a new Microsoft Bulletin, surf to Microsoft's site at http://www.microsoft.com/technet/security

- **Commercial Alert Services:**
    - **SecurityFocus:**
      SecurityFocus can be found on the web at http://www.securityfocus.com. The site is very informative but is a little overwhelming with its wealth of offerings to a public end user. For instance, security tools created by many public sources (known, trusted and also unknown, untrustworthy sources) are available. Likewise, this site has many user mailing list/forums to register with in order to gain information about a particular area of computing.[8]

However, it should be noted that there are even more sources from this site are available for a fee. One of the main resources available from this site that is fee based is the alert service. SecurityFocus advertises the ability to deliver alerts based on versions of any particular product. This author could not find online specific cost structures for one user for a year. However, a general cost structure was found in the February issue of *Information Security Magazine*. The article stated that these "…enhanced services can be purchased for $5900.00 per user per year for between 3 to 15 users."[9]

- **IAlertFocus:**
  IAlertFocus can be found on the web at http://www.idefense.com. This is a commercial, fee-based site run by Infrastructure Defense, Inc (IDefense).[10] This author's experience with IDefense concerns the IAlertFocus Alert services. The current customer this author is contracted to provides these alerts to their IT Security Team.

  These alerts are very informative and cover the following areas:
  - Virus, worm and other malicious code warnings
  - Profiles of hacker and other groups
  - Cyber-attack and defense tools
  - Geopolitical threat activity
  - Online cyber activism
  - Vulnerability information[10]

  One help area this service *does not* provide is in security tools. None are created nor provided at this time.

  This author was not able to gain specifics concerning pricing for this service. However, based on the fees charged by other fee-based services for IT Security, it can only be assumed that the fee is not cheap.

Problems Associated with the Current Alert Process

An administrator's job is never finished. The administrator must MAKE time to read the alerts in question no matter how busy he/she may be. Likewise, the same administrator must also understand the alert. This in itself may take several readings of the alert to understand the issue. Simply stated, to not read the alert, or, to read the alert and then not understand it, would be equally detrimental to an organization's IT security.

The next part of an administrator's duty after receiving and understanding said alert is to evaluate his/her network. Finding time to judiciously evaluate is the problem. This becomes more critical because often management has read about the vulnerability at this point and is pressing for an answer. Automated tools created by the same communities mentioned throughout this paper may often help.

In other instances, time has to be allotted for a manual check for these vulnerabilities. Once a compilation of results is in hand, an analysis must be performed to find the most vulnerable system, possibly through exposure or usage.

Finding time again becomes a problem when fixing the vulnerability. Concerns that determine how fast you attempt to fix a vulnerability center around the criticality of the alert, system exposure to the threat vector, and importance of the system to the total business operations. Time to document said actions is also a must in this process to show a best effort via industry security standards, or "due diligence"[11] has been meet.

Along about now, information overload may become a major issue. Perhaps several of your vendor's alert services are reporting the same vulnerability. Perhaps an administrator is subscribed to several vendor neutral alert services that all report basically at the same time on the same issue. Even worse, what about all those helpful friends and bosses that send you news media reports on the same issues?

Sometimes information overload does more than slow a person down in making sound decisions. A common reaction at this point is panic. This is a major problem to overcome and one that takes lots of practice not to succumb to while dealing with any issues related in a security or bug alert. Pick sites that you trust and tune everything else out until you have neutralized the problem. This author, based on his current situation, tends to rely on NTBugTraq and digest alerts form SANS.org.

Finally, but just as bad, is the problem of how to continually evaluate the quality of the alert service. You must continually ask your self, "Did the information from this site alert me in a timely manner, help me assess the threat to my particular system, and help me solve the problem? Did it help me also reassure management in an honest and comprehensive way? It is important to remember that bad security decisions eventually effect an entire organization. This continual re-evaluation is important whether the alert is from a particular vendor or from a vendor neutral source

Summary

Alerts are out there, both fee-based and free. The administrator needs to choose those best suited for his/her situation. Evaluate several sites. Choose one or two vendor neutral alert sites. Choose all vendor sites related to your particular operation. Read alerts religiously and daily. Each site must be continuously evaluated as to its usefulness in a crisis. If it gives information that is too late or untrustworthy, abandon it.

The administrator must continuously evaluate the real threat versus the threat as pictured in media hysteria. Avoid panic and fragmentation of effort by concentrating on information from sites you trust. As a final thought, perhaps the administrator should raise the issue of insurance with his/her company if that company's business is that of IT Security consultancy. Especially so if the IT shop consists of a Windows based environment as this product line currently receives a 15% premium to be insured for IT security.[12]

Citations

1 EWeek, The Enterprise News Weekly, Article Entitled, “Contracts Getting Tough on Security, by Dennis Fisher, Ziff Davis Media, April 15, 2002, Volume 19, Number 15, Page 1

2 http://www.cert.org, Computer Emergency Response Team, Software Research Institute, Carnegie Mellon University, General Site Information

3 http://www.ciac.org/ciac, Computer Incident Advisory Capability, Department of Energy, General Site Information

4 http://www.sans.org, System Administration, Networking and Security (SANS) Institute, General Site Information

5 Security Alert Consensus (SAC), Number 16, Network Computing and the System Administration, Networking and Security (SANS) Institute Thursday, April 25, 2002, Reference to SAC Number 15

6 http://www.ntbugtraq.com, NTBugTraq, RC Consulting, General Site Information

7 http://www.microsoft.com, Microsoft Corporation, General Site Information

8 http://www.securityfocus.com, SecurityFocus, General Site Information

9 Information Security Magazine, Article Entitle, “Feeling Vulnerable?,” by Al Berg, page 42, February 2002

10 http://www.idenfense.com, Infrastructure Defense, Inc, General Site Information

11 **http://www.computerworld.com**, Article entitled, “IT Security Destined for the Courtroom,” Jaikumar Vijayan, May 21, 2001
Direct Link:
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60729,00.html

12 **http://www.zdnet.com/iweek**, Article entitled, “Insurers Consider Microsoft NT High-Risk,” Robert Bryce, May 28, 2001
Direct link:
http://www.zdnet.com/intweek/stories/news/0,4164,2766045,00.html