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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Charles F. Romanus
Assignment Version: 1.2e

NETWORK SECURITY Is Like Eating Crab's Legs – Is the taste Worth the Effort?

When I started on this assignment I wanted to attack the SANS GIAC crowd as a bunch of whiners who would yell fire in a movie theater crowded with overworked and underpaid network managers. I saw the whole network security issue as a place where people interested in a fast buck using scare tactics had gathered to create a new industry built on the fears of non-technical managers propagated by an unknowing media. Security was just one more thing to add to the already overburdened network manager's plate. Let me tell you a quick story so you'll have a better idea where my distain for network security was born. I'll establish my bona fides later in this paper, but for now let it suffice that I have been managing networks in one form or another since 1982. During the time of the famous MELISSA virus I was working as a network manager at a medium-sized civil engineering firm operating in a large metropolitan area in the Pacific Northwest. When rumors of the impending attack by the MELISSA virus began to spread, my supervisor (an accountant – naturally) called me in and asked a thousand questions about our preparedness, how were we going to defend ourselves and what would the MELISSA virus do if it were to breech our then meager security fortress? His questions sent me off on an odyssey of research, taking me away from what I considered my primary task of keeping the network functioning in order to make a profit in order for me to receive a pay check. After about 80 hours of research and compiling many educated and uneducated guesses, I reported back that the MELISSA virus could, theoretically, bring us to our proverbial electronic knees. Well, my report started the expected chain reaction. My boss went to his boss and so on up the chain with fear and hand wringing added at each level. Finally, I was asked to brief the principals on the MELISSA virus and what we were going to do about it. I must have done a good job because the resource floodgates opened and I had carte blanc, much to the chagrin of the engineers who would have to suffer with used graph paper while I was on my spending spree. I knew that I wasn't up to speed on security so we called in a purported security expert. That guy, like a skilled surgeon he wasn't, poked and prodded my little network. He applied patches, fixes and all sorts of software voodoo. He also presented a very large bill which the owners gladly paid recalling my dire forecast. Well as I'm sure you remember, the MELISSA virus for the most part didn't amount to Tinker's damn and with all of the added mumbo-jumbo my little network had become extremely unstable to the point that it was crashing daily – reeking more havoc than MELISSA ever could have caused. Thus I became a victim of MELISSA. She grabbed me and effectively destroyed a fine, functioning network, yet, not one byte of her code had crossed my electronic threshold. Needless to say, I was the brunt of water cooler jokes and I couldn't show my face at the company softball games for the whole season. MELISSA had burned me because I overreacted. The cure was worse than the disease – I vowed death to all supposed network security experts.

© SANS Institute 2000 - 2005 Author retains full rights.

Time has passed and I have mellowed but my little story does present the dilemma that every network manager faces today: How much energy, how many resources and what level of concern should a network manager put into security? At one end of the security spectrum is Stephen Northcutt who, as quoted in a recent article, states that network managers "are making the attacker's job easier and making the problem worse."[1] At the other end of the security spectrum was me who, after being burned by MELISSA, chose to concentrate on network functionality at the expense of network security, kind of a Damn the hackers, full speed ahead approach.

When I sat down at the keyboard to write this paper, I was going to spend my energies trying to show that providing network security was a myth, something dreamed up by the Northcutt's of the world to generate fast cash. However, as I progressed in researching this paper I now feel that there is a valid security concern and I changed the thrust of this document. Now it is the intent of this paper to determine where security should fall in Network Manager's list of concerns. I want to explore what is the right balance between network security, network functionality and ease of operation? Obviously in this time of constrained resources not every dollar can go into security, as Northcutt would suggest. On the other hand, the rightful place of security in Maslow's Hierarchy of Need for computer networks must be determined.

Before tackling that daunting task, let me tell you something about myself. I have been involved in managing, either in a hands – on role or as a supervisor, computer networks since 1982. In that period I have worked for the National Security Agency, folks who know something about computer and communications security; the civil engineering firm mentioned above and a federal agency involved in disaster management. My network experience is primarily Novell using SPX//IPX and, more recently, NT using TCP/IP as a transport protocol. The networks have ranged from dedicated, closed looped systems with a specific mission where security was paramount to wide open, 'MODEM on every desk' operations with little thought given to security. All the networks functioned and continue to operate today. The current network within which I operate is a mixture of Novell and NT with Novell providing the LANs and NT providing the WAN backbone. There is a centrally controlled firewall. No MODEMs are allowed on computers operating behind the firewall. Norton Antivirus Corporate edition is the standard anti-virus software and, of course, passwords are required. I'll have more to say about passwords momentarily. Full backups are run on the LANs daily and there is one centrally managed database that is also fully backed up every night. The network has suffered two security beeches that have been identified: the ILOVEYOU virus and the Anna Kournikova worm. Both were caught very early and did not do any damage to any computer, data or packet transmission media. It is from this baseline that I will attempt to answer the question posed earlier: How much energy, how many resources and what level of concern should a network manager put into security?

When I worked for the civil engineering company I was also the corporate risk manager – I was given that task because I was not an engineer (didn't want to take up

© SANS Institute 2000 - 2005 Author retains full rights.

their time) and I could spell INSURANCE. When calculating what level of insurance coverage the firm needed, we would assess the risk, determine our exposure and then determine how much insurance it would take to cover the exposure. As an aside, we figured (in a non professional mode) our greatest risk was one of the survey trucks being in an accident and killing someone. Our lawyer told us that (and he had lots of qualifiers) should one of our survey trucks be in an accident and found at fault – he used the example of the surveyors having a few surruptious brewskis and plowing into a school bus. He estimated our exposure to be anywhere from $1Million to $8Million. We weighed the probability of our surveyors getting tipsy (low), the probability of them smashing a school bus (medium – lots of school buses in Redmond, WA) and we determined that we were toward the low end of the exposure range. We then cranked in a fudge factor and insured ourselves for $4Million. We also tried to put in place procedures to preempt or mitigate the risk. We could have insured for $8Million, the estimated maximum exposure with maximum insurance cost or we could have self-insured at no insurance cost. We chose a middle of the road approach. That seemed like a logical way for a medium sized firm without a risk management department to determine the right amount of insurance coverage for the firm. I think the same formula: assess the risk, determine the exposure, add a fudge factor and purchase the right amount of insurance, can be applied to computer security as well. To support my theory that you can be over or under zealous in protecting a network from risk, I refer to an article by Fred Langa. Fred proposes that you can over insure by having multiple layers of conflicting and contentious security software which brings an otherwise operational network to its knees or you can under insure by only having a single layer of network security that is easily circumvented.[2]

So what is the risk to today's network? Where should the network manager put his security resources and how much of his total resources should the network manager put into security.

I think we'll attack the questions and see if the answers also fit in determining securities rightful place in the Network's hierarchy of needs.

What is the threat, what am I developing a balanced security approach against? The threat, as I see it, is loss of ability to access the data and/or applications on my network by the network users. That's the threat I face. Other network managers may perceive their threat to be loss of ability to communicate while other network managers may perceive their threat to be damage to equipment. I have multiple communications paths and abundant computer resources so I'm not concerned in those areas but I only have one database. So, I know my primary risk is loss of data not loss of communications and not equipment damage. How do I insure my database against the threat and what level of insurance do I apply? To determine how to protect my database, I need to know what shape the threats may take. Am I most likely to be attacked by a horde of Chinese hackers intent on denying Wet Grass, Wyoming it fair share of disaster dollars? Not likely. According to text, Managing Information Technology, "…employees are the most knowledgeable about the technology and even about the

© SANS Institute 2000 - 2005 Author retains full rights.

company's security system."[3] The text concludes that the greatest threat to computer systems is from the employees. The internal threat is further substantiated in an article by Howard Millman in CNET.[4] But there is also another threat referred to in Mr. Langa's article: The threat of interference from contentious security programs.[5] Thus, I face two threats to my data one from employees and one from contentious security and other programs that are put in place to counter the attack from employees. I think I detect a loop. But what about the ubiquitous hackers, the hordes of Chinese salivating over the thought of denying Wet Grass, WY a piece of the federal pie? I don't know the level of external attack my network is under. I have a firewall but it has not shown any external activity directed against my location. I have had two security breeches but those were ".vbs" and they didn't do any damage

Ok, so here's where we stand: 1. employees, either intentionally or unintentionally, seem to present the greatest threat to my database, 2. Contentious security software can perform an unintended denial of service attack and 3. My firewall indicates that the hordes of Chinese are ignoring my little network. Now, what can I do about employees and what price should I pay to implement my employee strategy? Without a doubt, employees can devastate my database whether they are operating intentionally or unintentionally. How do I stop them? How do I know they have damaged the data and how can I restore the data to its pre-attack condition? These are damn good questions. I have no way of knowing if false data has been entered into the database, only another employee can tell me that. I have a good back up system where I have a year's worth of data at any time, so presumably I can go back and recapture the last known good data. If the data has been destroyed, I can easily recover. If the data has been maliciously manipulated – I may never know. So what do I do to reduce the risk of an attack on the database by an employee? Most of the actions that can be taken to eliminate employee sabotage are non-electronic. Every employee goes through an interview process and a background check. Employees receive initial training on the functions of the database and periodic refresher training. Finally few employees have access to the entire database. Most folks only have access to one or two modules. Determining the access to these modules is administered by other departments and doesn't take any of my time. I do, however, administer the password program that does take a great deal of my time. The passwords grant or restrict access to the various database modules.

I can set the level of passwords from none to complex (strong) and I can set the expiration date from never to everyday. I have it set for 90 days. On the surface it would seem that this is an easy area to manage and over the years employees would grow use to changing passwords. Unfortunately that is not the case. For this paper I reviewed 2 months worth of my helpdesk calls and fully 53% were password related – amazing!

According to the text, Managerial Economics, one technique for determining the cost of a project is by using its overall expected cost[6]. If I apply that analysis to my password situation perhaps we can shed some light on where security falls in the grand scheme of things. Now, some calculations to determine the cost of the risk of loss of

© SANS Institute 2000 - 2005 Author retains full rights.

data: Let's worst case this situation and say that there is complete loss of the database. I can run a recovery in about 5 hours. I make $25 per hour so my cost to recover the database is $125 plus some opportunity cost of not doing other things. The employees would not have access to the data during the recovery period that would hinder their productivity. I estimate that the cost to my office is about $8,000 for a total loss of $8,125 plus some nebulous opportunity costs. So, if I lose the entire database by not having a strong password program I could lose $8,125 on the first occurrence and probably my job on the second.

The next question is, how much does it cost me to manage a strong password program? Records show that 53% of my trouble tickets relate to passwords. There were a total of 120 password related trouble tickets and it took approximately 15 minutes to fix each trouble ticket. 15 minutes time's 120 equals 30 hours of my time spent resolving password related troubles. The individual employee was also denied access to the database but they could, for a while, perform other tasks. This means that it costs 30 time 25 or $750 to administer a strong password program for 2 months. Well less than the $8,125 it would cost me to recover the database. Therefore from a dollars and cents standpoint it makes sense to have strong password program. But if you look at just my cost, administering a strong password program costs about $750 for every 2 months versus $125 to restore a database. The economics of the situation would indicate that, if it were just my time, I would be better utilized by having a weak or non-existent password program provided that I had no more than 6 database restorations in a 2 month period.

Unfortunately the intangibles start to come into play. If my database experienced any unnecessary downtime, the confidence of the users in the database would begin to crumble. That would bring senior management into play and I doubt they would buy off on my economic approach to database management. The introduction of the intangibles puts me back at square 1 in an attempt to quantify the cost of a strong password program as part of an overall security scheme. I just can't quantify a good butt chewing. Where does this leave me? Perhaps a more general approach is necessary to determine securities rightful place in the Hierarchy of Network Need. Perhaps a logical approach will work better than an economic approach. Let's take a look.

Logic tells me that without the network, there is no need for network security because there is nothing to secure. Further, logic dictates the purpose of my network is to provide effective access to the data contained in the database. In other words without the data, there is nothing to secure. So, having access to the data would seem to be the highest priority and to achieve that there must be a functional, effective network. Therefore the highest priority is to have an operational network that provides access to the data contained in the network database.

Next, logic dictates to me that the accuracy of the data must be assured. The accuracy can be affected by improper input or malicious manipulation. Training and periodic audits are the way to protect the accuracy of the data. I do not see a software fix for the auditing, this looks like a blood, sweat and tears operation. If the audit shows that

© SANS Institute 2000 - 2005 Author retains full rights.

I have accurate data then my training is paying off and I need go no further other than continuing the training program. If, on the other hand, the audits show corrupted data, I have a problem and I need to determine if the corruption is caused by internal or external activities. At this point I run into another dilemma: I can correct the data and just go on or I can attempt to identify the culprit. If the problem is recurring then I need to do something about it. If I can, via the audit, track the problem to an employee – fine, I can deal with that. If the problem is external to my network, then I need to take further action in terms of tightening the firewall or applying any of the numerous fixes referred to in the class. But my bottom line is that I will not take multiple software fixes unless I have evidence from an audit that I am facing a recurring external attack. I want my network to be as clean as possible and not have many layers of potentially conflicting security software.

Time to summarize this tome. The point I have made is that there must be a place for network security but where is that place in the grand scheme of network management? I've shown, through an small economic analysis, that when considering just the network manager's time it is possible to make a case that it is not worth having a strong password program and by implication a strong network security program. I've also shown that by using a logical approach to network security management, it falls after management of the network and the data thereon – kind of a chicken or the egg approach. It is obvious when you consider all of the factors a network manager must comprehend and apply, the integrity of his network and the data thereon is his reason for existence and the security of that data must be a consideration but not necessarily the prime consideration. So, if you like crabmeat then expend the energy but in the end only you can determine the right amount of energy to use to extract the meat from the claw.

© SANS Institute 2000 - 2005 Author retains full rights.

Notes

[1]Jason Levitt, "Security – The Enemy Within," INFORMATIONWEEK.COM, 23 April 2001. From www.informationweek.com/834/prsecure.htm, 1.

[2]Fred Langa, "How Much Protection is Enough?" INFORMATIONWEEK.COM, 4 June 2001. From www.informationweek.com/840/langa.htm., 1.

[3]Martin, E. W., Hoffer, J., DeHayes, D., Perkins, W., Managing Information Technology, ed. Charles E. Stewart (Prentice-Hall, Inc., 1994), 412.

[4]Howard Millman, "The Invisible Threat," Enterprise Business, 18 July 2001. From www.cnet.com.

[5]Langa, 3.

[6]Maurice, C., Thomas, C., Smithson, C., Managerial Economics, ed. Jean L. Hess (Richard D. Irwin, Inc., 1992), 710.

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

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

© SANS Institute 2000 - 2005 Author retains full rights.