nCircle

Proactive Network Security:

Making Your Network Unassailable

Table of Contents

> “The art of war teaches us to rely not on the likelihood of the ememy’s not coming, but ***on our own readiness to receive him;*** not on the chance of his not attacking, but rather on ***the fact that we have made our position unassailable.***” - SunTzu

1. Executive Summary

The "market" for digital attacks is growing rapidly as the number of networked devices and software vulnerabilities continues to increase. Organizations are already so deluged with attacks that the current strategy of responding to intrusions no longer works because the alarms are turning into a new source of organizational white noise. *Proactive Network Security* offers a new strategy by combining five key elements: Detailed assessment of all the devices on the network; continuous monitoring of those devices; maintenance of a database of known vulnerabilities; evaluation and prioritization of threats based on the business value of each of the networked devices; and management of corrective actions through ownership and workflow. Used in combination with reactive technology such as Intrusion Detection systems, Proactive Network Security offers realistic protection by treating threats and vulnerabilities not as isolated events but as permanent "features" of the new networked environment.

2. Introduction

Security has of course become one of the highest priorities of every company. Despite all the hype, the extent of the problem isn’t always understood.

For example, a typical global 2000 enterprise security system generates over 2,000,000 alerts every day. In 2002, digital attacks did $42 billion dollars worth of damage.[1] And, according to the CERT® Coordination Center (CERT®/CC)[2] at Carnegie Mellon University, the number of attacks is doubling every year. Even if you don’t believe the numbers, the reality is that you or someone you know has been affected by an information security incident within the past 24 hours.

Security is no longer a matter of guarding against occasional attacks. Organizations are under perpetual and continual attack. Digital attacks are now more frequent than spam. And, just as it is no longer possible to deal with spam by opening each message for visual inspection, digital attacks need to be dealt with *proactively*.

The constant flood of attacks is a new fact of life for organizations. It requires a new approach to security.

3. Network Security: A brief history

There are only two reasons why TCP/IP networks are vulnerable to attack: the network itself and the software applications that run on it

[1] mi2g

[2] http://www.cert.org/

3.1 The Network

TCP/IP's vulnerability is a consequence of a fundamental design decision: TCP/IP is a "stupid" network, in the words of David Isenberg[3] in a paper he wrote while working at AT&T. A stupid network doesn't have many services built into it. In contrast, a smart network, like the telephone system, puts in lots of features and services: call waiting, caller ID, and the like. This works well for the phone companies because it is a private network that they completely own and can control. For example, they have the power to decide which services are put in; they can charge several dollars a month for caller ID even though it does nothing but transmit a handful of information at the beginning of a call.

But the designers of the Internet had different aims. They wanted a public system that would easily integrate existing networks, would be easy to join, and would encourage innovation. So, they built a "stupid" network – also called an end-to-end network by Clark, Reed and Salzburg[4] in their seminal paper in 1984 – that does little more than move bits from any A to any B. That way, the network can accommodate any project that needs to move bits around without deciding ahead of time which sorts of projects it will favor.

The Internet has worked out better than its designers could have ever imagined, in large part because of its end-to-end architecture. But this success comes at a price - especially when it comes to security.

With the "end-to-end network" there are solid network architectural and economic reasons for building services at the "ends" of the network rather than into the middle. However, security is not of the underlying reasons for this structure. As the Internet is by its very nature decentralized and open, there is no control over who gets onto the network. The result is that it is so easy to hook devices into the network, most companies of any size literally do not even know what they have on their network. And because the end-to-end Internet leaves security to the ends of the network, applying uniform and effective security controls on every single TCP/IP device is pretty much impossible.

3.2 Complex Applications

The other reason TCP/IP networks are vulnerable to attack: complex applications. Software applications are not getting any simpler. They have more features, they interact with more applications, and they work over increasingly complex networks. Inevitably, this complexity breeds error.

Currently, there are three categories or errors that create network vulnerabilities and exposures:

- **Design error:** There is little that a customer can do about *design* errors in the software his or her company uses.
- **Implementation Error:** Errors the vendor has made in *implementing* its software leave the customer with no recourse except to apply the patches as soon as they become available.

[3] http://isen.com/stupid.html

[4] http://www.reed.com/Papers/EndtoEnd.html

- **Configuration error:** The customer can continuously work on fixing *configuration* errors, but in a complex software environment – i.e., every organization's software environment – perfection is not an option. Continuous improvement is the best that can be expected. To sit and do nothing offers your attacker a target-rich environment.

3.3 Changing Threat: Unstructured vs. Structured[5]

The current realities faced by organizations when dealing with network security are largely the result of the original design goals of TCP/IP that fall short in providing an effective platform for security controls. Also contributing to the challenges of network security is the growing complexity of applications that make them inherently insecure. This means that for most organizations the need to find and fix errors before your opponent can exploit them has become like a game that you have to play every single day. And as with any good game, you must get inside the mind of your opponent to understand your own position.

Post 9/11, the awareness and categorization of threats have changed. Most of what the connected world has experienced are *unstructured threats*, i.e., attacks directed not at a specific organization but at a technical or social flaw present in many organizations, often at the infrastructure level. Your Aunt Alice and Uncle Bob have the same chance of getting hit by an unstructured attack as a large financial institutions or government agencies. The perpetrator of an unstructured threat presumably "succeeds" if some indefinite percentages of machines are vulnerable.

Over the past few years, the number of *structured threats* has been steadily rising. These sorts of threat are far more dangerous to organizations, for they are targeted specifically and will be repeated until they succeed. The opponent is patient, well funded (sometimes by states), and will enter your network in ways creative enough to entertain a Hollywood audience.

If an organization does not have an effective security program that can handle unstructured threats, they probably don't have a fighting chance to fend off a structured attack.

4. The Customer Problem

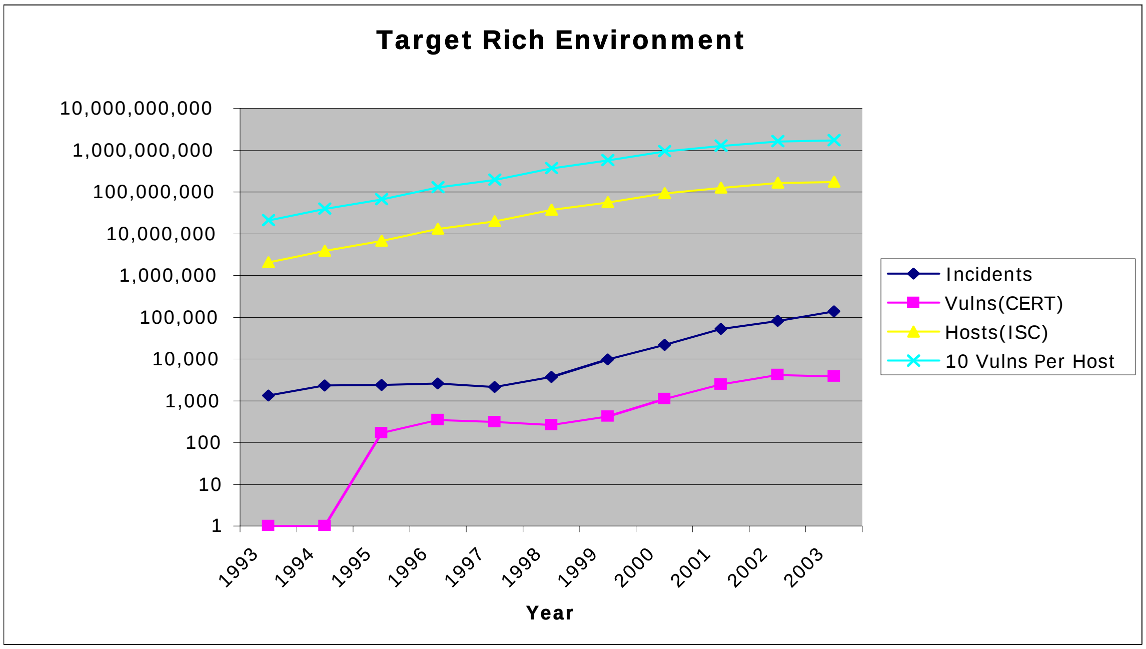
Companies face an unprecedented problem securing themselves against intruders and attacks. Every single day, their infrastructure is changing, the threat environment is evolving and more and more business functions make their way on to the TCP/IP network.

To get a sense of the magnitude of the problem, it is not sufficient to just look at the growing number of known vulnerabilities or the reported incidents. The other important parameter to the dimensions of this problem is the number of IP devices connecting to the network. What is important to your opponent is how much of a 'target surface' they will have to attack. Using publicly available statistics from CERT®/CC[6] and Internet Software Consortium (ISC)[7], we can estimate how target-rich the Internet is today.

[5] http://www.whitehouse.gov/homeland/

[6] http://www.cert.org/

[7] http://www.isc.org/



The chart above shows that there are statistically more untapped targets for your opponent to exploit.

CERT®/CC publishes information on known security incidents, reporting that there were 137,529 incidents in 2003. CERT®/CC uses the word incident as an administrative term that groups together any related set of activities; for example, an intruder uses the same tool or exploit technique in their activity. A single "incident" can involve anything from a single host computer to a very large number of host computers, at a single site or at hundreds of thousands of sites.

For example, the CERT®/CC counts all reports related to the Melissa virus, or all reports related to the LoveLetter worm, as a single "incident" for administrative purposes. Therefore, the number of incidents reported in the CERT®/CC statistics may appear to be smaller than the scope of the problem really is. ISC estimates there were more than 171 million connected hosts on the Internet in that same year. (Note: This number does not include the private networks sitting behind firewalls on private addressing schemes.)

In 2003 alone, CERT®/CC reports about 3784 vulnerabilities were known. These vulnerabilities are in addition to those from previous years since legacy systems or poor application hygiene could make these counts cumulative over the years. You may have a vulnerability on your network right now that was first published back in 2002.

Be careful what you count: Why not just track the number of attacks or security incidents per year? Historically, this was the case but it is dangerous because for one, not all incidents are reported and two, any smart biological agent knows that it is far more important to compromise its host but keep it alive. It is much more valuable for your opponent to take control of a computer and use it for secondary activities (stealing credentials, exploiting the trust this machine might have with other machines, etc.) than to affect the machine in a way that is easily detected or kill the resource they just compromised. For that matter, basing your strategy on the attack and security incident statistical data is like driving your car while looking only at your rear-view mirror when someone is trying to run you off the road.

In determining the number of vulnerabilities, a conservative approach is to assume an average of 10 vulnerabilities per connected host. As you can see, having the potential target number up in the billions is not a good thing. There are a number of questions to be considered in estimating such numbers. Is the attack surface available to attackers really that large? Do the attackers have even more untapped targets to comprise? You could sit and argue the numbers, but not knowing the target surface of networks with your organization is not acceptable. Not only should you know what the target surface looks like today, but last week and last month as well. Are your resources operationally fit and battle ready? In the spirit of Sun Tzu, have you made your position unassailable?

One thing is for certain; there are more targets for the bad guys, more bad guys, and more creative attack methods. Enterprises have to assume that their IP networks will continue to be assailed. In fact, the numbers published above from CERT®/CC are conservative since they only take into account known vulnerabilities and reported incidents; a Price-Waterhouse study showed that 41% of senior technology executives at companies with a serious security breach didn’t report them to the authorities.

With so many risks, organizations cannot wait for attacks to damage them and then respond. Organizations need to *proactively* guard against the attacks that are a new part of the network infrastructure, not merely react to them.

5. Proactive and Reactive

Reactive systems, such as intrusion detection or intrusion prevention systems depend on an attack, incident, or loss of some degree to occur before they start the information gathering and analysis that ultimately drives some form of automation or reporting. They complement proactive security measures the same way fire-fighting complements fire prevention.

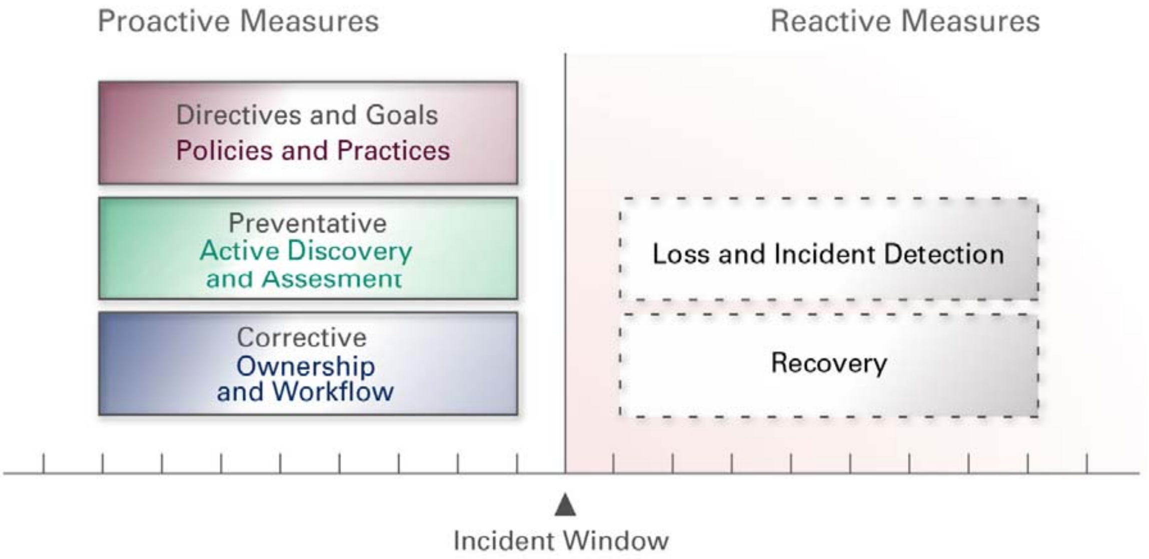
A proactive system constantly *tests* the organization’s network for vulnerabilities and exposures. It then *assesses and prioritizes* those vulnerabilities and exposures and *manages* the process by which those vulnerabilities and exposures are addressed. All IP devices attached to the network are periodically or continuously scanned and profiled for changes, violations to policy, and vulnerabilities and exposures. Analytics are applied so that the administrators and business owners are presented with actionable intelligence relative to the risk to their business. The defect is then corrected, before security can be breached.

In contrast to reactive systems, proactive systems have the advantage of providing valuable intelligence about an organization’s network and networked devices even when they are not under attack. Of course, proactive systems work best when complemented with appropriate reactive systems. This provides organizations with a layered approach to network security where vulnerabilities are detected and dealt with on multiple levels.

So, why are reactive measures more common than proactive ones? First, there is an illusion of immediacy to reactive measures: A company only reacts if it recognizes that it’s been attacked. This makes reactive measures seem more urgent, and often more easily justified. On the other hand, a company may never know exactly what attacks its proactive measures prevented, so the immediacy of the value of those measures isn’t as obvious.

Reactive measures and technologies are better understood as they have been around longer and are widely deployed. The initial costs involved with a reactive security program are much lower than those associated with creating a proactive system. However, while making the move to a proactive system requires a substantial investment in building and maintaining a database of vulnerabilities and remedies, this preventative stance will save your organizations money in the long run. The benefits easily outweigh the additional work and investment - damage is prevented before it happens and more of the network is understood and protected. An ounce of prevention is worth a pound of cure.

6. Proactive Security in Detail



There is no realistic possibility of eliminating all threats. The very nature of the basic architecture of TCP/IP and the inevitable complexity of applications makes this impossible. True success consists in proactively reducing risks to the network.

Each organization has its own level of risk tolerance, embodied in its policies and practices. In looking at reactive network security, the focus is on *detective measures* and *recovery measures*. These detective measures try to identify incident or loss resulting in some level of recovery. No system is 100% accurate so detective and recovery measures complement the proactive measures much like how fire safety has both fire-fighting and fire-prevention.

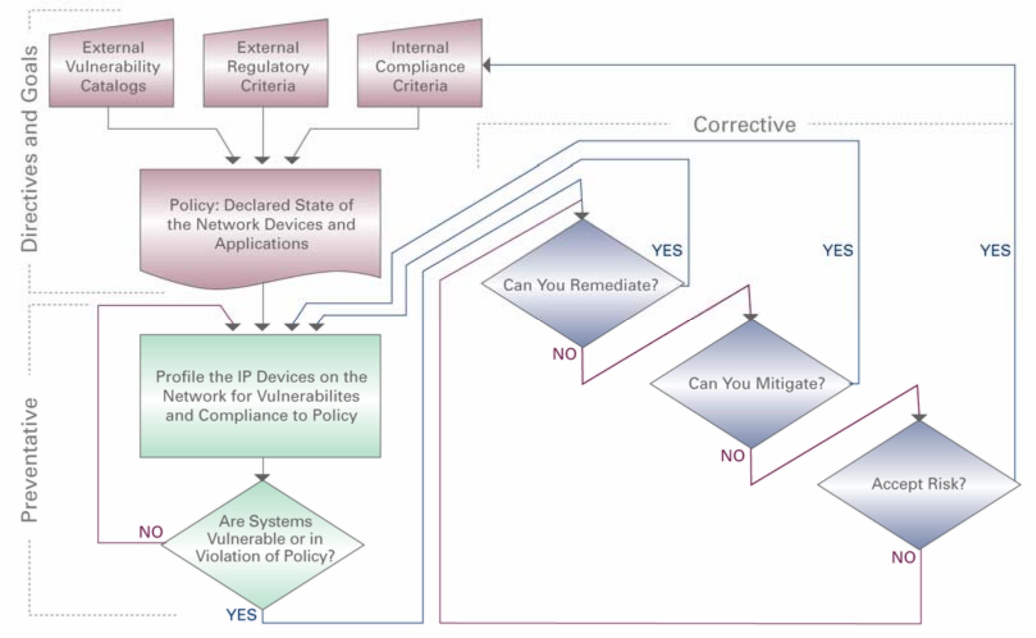
To take a proactive stance to network security, organization must make the shift from using only detective and recovery measures and include the following:

1. *Directive measures* state the goals of “how things should be or how things should be done”. Directive measures are usually known as security policy.

2. *Preventative measures* go out and evaluate “what is” and compare it to “what should be”

3. *Corrective measures* which are the result of preventative measures and are focused on bringing these defects or outliers back in to the norms of operations.

Implementing such proactively focused measures is not about deploying a point-solution or point-product. It is a lifecycle product involving technology, processes and people and the types of proactive measures discussed above. Let’s look at the major steps in this lifecycle represented by this workflow diagram.


Directives and Goals
Preventative
Corrective
External Vulnerability Catalogs
External Regulatory Criteria
Internal Compliance Criteria
Policy: Declared State of the Network Devices and Applications
Profile the IP Devices on the Network for Vulnerabilites and Compliance to Policy
Are Systems Vulnerable or in Violation of Policy?
NO
YES
Can You Remediate?
YES
NO
Can You Mitigate?
YES
NO
Accept Risk?
YES
NO

6.1 Directive Measures - Security Policy: What should be on my network

A sound security policy begins with an assessment of the standards and processes by which it is going to measure compliance. This is influenced by three sources, two external to the organization and one internal, which are as follows:

- The *External Vulnerability Catalog* lists the known external threats. Catalogs such as the Common Vulnerability and Exposures (CVE), Bugtraq (Symantec), Vigilinx (TruSecure), and iDefense list all known vulnerabilities of every piece of software.
- *External Regulatory Criteria* within regulated industries establish a framework for auditors so that security can be measured in a uniform manner. Examples include HIPAA, GLBA, and FIPS-199.
- Enterprises usually have various working groups and committees that create policies designed to make the network and software environment secure.   These are closely aligned with the business’s tolerance for risk and change as the business changes.

It is important to keep in mind that enterprise security policies are not carved into stone and will evolve and change over time. Sometimes a vulnerability will be deemed acceptable, or a new vulnerability will emerge that requires “patching” the policies (e.g., “Henceforth, handheld computers cannot be left unattended in the restrooms”).   The critical element here is that business owners have ownership over their computing environment and accept the responsibility and accountability of the vulnerabilities and exposures their infrastructure brings to the business.

6.2 Preventative Measures: What is on my network, analyzed in the context of my business

Once policies state what is acceptable and what is not acceptable, an organization assesses its existing network infrastructure, comparing “what should be” to “what is.” This assessment must encompass not only the search for known vulnerabilities but also the violations to system and network baselines sometimes referred to as ‘gold standards’. This can be done intermittently, with the risk of being vulnerable to attack in between assessments, or it can be done continuously. When vulnerabilities are found, they are presented to the enterprise, preferably in prioritized, easily understood reports so that the information is fully actionable.

6.3 Corrective Measures: Correct the flaw and return us to our operational goals

If an organization finds something on its network that is either a violation to policy or a vulnerability, there are only three actions that can take place: Remediate, mitigate or accept the flaw. It is important at this point that someone take ownership over the flaw itself. If the business owner chooses to accept the flaw, the internal security policy must be modified to represent this exception and the workflow continues.

Accountability and Transparency

Accountability and transparent progress tracking are the most important properties regarding the corrective measures. The Federal Information Security Management Act (FISMA) is an example of this process becoming less of an option and much more mandatory. The Office of Management and Budget requires that all Federal Agencies report on a quarterly basis how many new vulnerabilities were found, how many were fixed as planned, how many are delayed.

To those familiar with Quality Management methodologies like Six Sigma, this workflow will look familiar. If one takes violations of policy and vulnerabilities as defects, then the reduction of defects per million on an ongoing basis will improve the effectiveness of the security program and ultimately the business. The results are measurable on a daily basis, unlike the reactive measures that can only make claims such as “162 days without a security breach.”
This is important because measuring security by the number of incidences, attacks and loss misjudges the importance and effect of security systems. It is more realistic and helpful to measure security spending based on the acceptable risk to the business. Proactive security provides not only continuous, preventive security but also gives the business a more detailed, complete and realistic way of assessing the effect of security on its operations and financial picture.

7. Summary

When comparing Information Technology security practices to mature systems like fire safety that dates back to 300 BC, we see how immature the industry really is. It is a safe bet that the industry will continue to evolve as change is happening at the threat level, at the technical level, and at the business level. The most significant shift in your organization’s strategy will be moving from the reactive side of the incident line to the proactive side. This is true with any other system that has an active opponent. Many organizations have already made the shift and experience positive results on a daily basis. It is time to make your position unassailable.

Security and Game Theory
At nCircle, we like to look at security as a game much in the same way that game theory has made its way in to financial strategies. This may be the result of our collective experience (especially those of us coming from the gaming industry) but from our perspective, information security is nothing more than Information Technology (IT) with an active opponent. Instead of just waiting for a power supply to fail, or a network link to go down because of some noise on the line, there is an active opponent that is watching your every move. In fact, your opponent is calculating their strategy every day based on intelligence that they gather. How can you run your business while satisfying these game-like dynamics that keeps your opponent guessing, knowing less than you do about your environment, having less and less opportunity for attack, and perform these tactics without impacting your organizations business growth and opportunities? The answer is in your own intelligence - about your environment, and equally as importantly about your adversaries, and your ability to make sound business decisions based on this information. nCircle delivers proactive security solutions for large enterprises and is committed to helping customers gain an unfair advantage against their attackers in this game we call information security.

About nCircle

nCircle is a leading provider of enterprise-class vulnerability and risk management solutions. Global enterprises and government agencies rely on nCircle's proactive security solutions to identify, measure, manage and reduce security risk on their worldwide networks. nCircle has won numerous industry awards for its rapid growth, innovation and technology leadership and has been named one of the top 100 best places to work in the San Francisco Bay Area. nCircle is headquartered in San Francisco, California, with regional offices throughout the U.S. and in London, Toronto and Tokyo. Additional information about nCircle is available at www.nCircle.com.

nCircle Network Security
101 2nd Street, Suite 400
San Francisco, CA 94105
(888) 464 2900
www.nCircle.com

References:

http://mi2g.net
http://isen.com/stupid.html
http://www.reed.com/Papers/EndtoEnd.html
http://www.cert.org/
http://www.isc.org/
http://www.cert.org/octave/
http://www.whitehouse.gov/homeland/