Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

awareness, quality assurance, security, techniques, implement, sans, white paper

Successful companies have found a way to offer something that people want, at a price they are willing pay, in a way that will make money in the transaction. Highly successful companies offer quality products and services in this exchange, and keep the quality high, so that the customer will return the next time he/she wants to purchase. This paper discusses how quality is the responsibility of the whole organization and security is a part of the totality of quality of a system, implicit in customers' expectations. Qua...

Copyright SANS Institute

Author Retains Full Rights

AD

Elizabeth (Liz) Stanton
GSEC Practical Assignment
Version 1.2e

Title: Fortify Security through Quality Assurance Practices

Successful companies have found a way to offer something that people want, at a price they are willing pay, in a way that will make money in the transaction. *Highly* successful companies offer quality products and services in this exchange, and keep the quality high, so that the customer will return the next time he/she wants to purchase.

Quality has been defined as: "The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs. Not to be mistaken for "degree of excellence" or "fitness for use" which meet only part of the definition."[i]
By this definition, security is a component of quality.

The American Society for Quality has made the following statements about quality[ii]:

- Quality is not a program; it is an approach to business.
- Quality is a collection of powerful tools and concepts that is proven to work.
- Quality tools and techniques are applicable in every aspect of the business.
- Quality increases customer satisfaction, reduces cycle time and costs, and eliminates errors and rework.
- Results (performance and financial) are the natural consequence of effective quality management.

Security is defined by the American Heritage Dictionary in their on-line database as: 1) Freedom from risk or danger; safety; 2) Freedom from doubt, anxiety, or fear; confidence; 3) Something that gives or assures safety, as: a) A group or department of private guards; b) Measures adopted by a government to prevent espionage, sabotage, or attack; c) Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault. [iii]

These definitions, taken together, can demonstrate that 1) quality is the responsibility of the whole organization; and 2) security is a part of the totality of quality of a system, implicit in customers' expectations. Quality should be a part of how business gets done. This includes software quality, but also encompasses everything the organization does, including protecting its assets, physical and virtual. Security, as a component of quality, must be addressed throughout an organization; in the definition of strategy, the development of policy, and the implementation and monitoring of both.

In general, "there is a high correlation between business success and disciplined quality management fundamentals.[iv]" Fortifying security surely can enhance this success. Applying the tools, concepts and techniques proven to work in the quality assurance field to security should result in increased customer satisfaction, reduced rework and increased results.

Ms. Evelyn Labbate has addressed one aspect of improving product quality, in her SANS Certification Practical. She argues well that "increasing the quality of software will in turn reduce the risk of introducing vulnerabilities into a system."[v] She touches on how not only

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

individual developers can address security issues in software, but how teams can work together to address it as well, through code reviews, coding in pairs, and using independent test teams.

Yet the need for quality plays in an organization is larger than just the software development process. Security is not limited to application software. Both quality and security must be pervasive in an organization for true depth of impact to be obtained. Security and quality both should be built in from a projects inception. Just as companies attempt to 'test quality in', so do companies view "…security [as] the last thing we cobble together and bolt on. And as a result, it's usually the messiest, ugliest, most user-unfriendly part of our systems…The best solution - the one we can't afford, of course - would be to rebuild everything, our entire IT infrastructure, applications, the works, with security designed and built into it down to the core."[vi] Note that Mr. Hayes includes "the works". This can includes strategies, policies, organizational structure, training, etc.

Using the American Society for Quality[vii] as a reference point, we can see some examples of ways that quality tools and techniques can assist the security professional in improving security through people, process and technology.

People

Security awareness in an organization can be a critical success factor in building its security defenses. People subvert security mechanisms because of human nature, not typically because they are trying to be malicious. A user receives an email that says "ILOVEYOU", and naturally they want to open it. They receive an executable that lets them watch "dancing gophers", and of course they want to see it. They see someone at the door, with their hands full of pizza and soda, and can't get in, they want to help, and open the door for them – and let them right in. This is especially true when they are being asked to do something that doesn't maybe seem quite right by someone in authority (or appearing to be in authority), or someone angry with them. The help desk worker may be tempted to give out a password over the phone if they believe it is the "big boss" at the other end (and boy is she mad!).

These are examples of people following natural curiosity, common courtesy and a sense of self-preservation. A good security awareness program, in combination with a strong policy, will give them the tools to appropriately deal with each of these situations. The security professional can provide the content required to train users. The quality professional can link that content overall with the needs of the organization and determine the appropriate methods for getting the word out. They can also assist in evaluating the effectiveness of the training – allowing the technical security professional to spend their time where they are most needed.

In order to get security work done, people need to work together. No one person can secure a business. Quality assurance professionals, along with other groups in a company, like human resources, have training in defining effective structures within which work can be done – including reporting relationships, responsibilities, and authority. For example, QA could assist in defining security organizational structures that put responsibility for all forms of security beneath one high level executive, with multiple branches of security under him or her (physical, internal network, external network, access control, etc). Alternatively, for a particular

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

organization with specific cultural needs, there needs to be separation of duties for checks and balances within security. Using input from security staff, the culture, and strategic direction of the company, a structure can be implemented that meets each group's goals.

Process

Quality assurance and quality management includes strategic planning and deployment of quality policies in an organization.[viii] This should incorporate security policy in support of the security staff. QA can advocate that security be an integral part of the business strategy at the highest level of the organization. With the business strategy understood, sound security policy can be written.

Examining and articulating security policies at an organizational level forces executives in the enterprise to work through the difficult task of determining what risks are acceptable, and what are not. This includes defining those things that only the "enterprise" can accept, and those that a particular business unit or department may be able to accept on behalf of the enterprise. Understanding that the enterprise can't have both 100% security and 100% functionality, the risk versus the reward to be had can be factored into decisions about particular connectivity. Acceptable risk also then requires conversation on risk mitigation practices and options. The security professional should be able to discuss at an appropriate level with business managers what type of threats exist when networks are connected to 'unknown' networks, including the Internet. These factors will help define what the risk, and how it can be alleviated. How the risk can be reduced leads to discussion of what processes should be in place.

Security is a process, not a product.[ix] A process may be defined as a set of interrelated or interacting activities that transforms inputs into outputs.[x] Processes define what needs to be done, by whom, and when. They take specific activities, possibly using technology, and together begin to form the barriers that serve as security for an organization. Well-documented security policies, processes and procedures allow people to take necessary actions without fear of reprisal.[xi] Even without well-documented policy (although having it is always preferable), processes can be designed to improve security.

Many quality professionals can also assist in documenting the specific procedures needed to design, implement, support and monitor security measures. Working closely with security experts, they can help to document and define the actions that need to be taken by systems staff, users, and business people to support those polices and processes on a day-to-day basis. Like policies, procedures may be subject to change when technologies change, when the business reorganizes or a new system in implemented, but it allows the policy to serve as the macro document to provide direction. Policy can remain broader, and at a higher level, while procedures are used to address who does what, when. Well-documented and closely followed procedures should identify responsibility and provide an audit trail at a time of a potential breach.

Because security technology's and vulnerabilities change so fast, procedures must be built with some flexibility to allow a job to get done quickly, in response to a threat facing the company. For example, notifications of emergency changes shouldn't be set so rigidly that an appropriate

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

protective or responsive measure is not taken because the "one right" person couldn't' be contacted. In cases like this, the combination of procedures and policy should allow the person with the expertise to do the right thing without fear. Executives everyday are required to make decisions with limited information and high potential risk. Security professionals must do the same, and be trusted to make the right choice, based on company policy.

Technology

In a cooperative effort to strengthen security in an organization, the technical focus clearly belongs with the security professional. The creation of processes and policy with a clear technical base from security will help meet the goal of increased security. However, in the use of technology by people, there are opportunities for QA to support their consistent, repeatable handling. The following are examples of technical security best practices that can be supported through QA techniques.

To preserve network integrity, and that of the systems and information on the network, measures must be taken that both prevent entry from attacks and detect attacks as they occur. Network and security engineers use multiple tools to watch, log and analyze traffic that flows across the network. One method for interpreting the results is to compare what they are seeing with normal IP behavior. In many cases, network and security engineers will also create tools or scripts to use to understand the data. There are tools, such as tcpdump and nmap that can provide substantial data about what is happening on the network and on systems.

However the use of these tools may not be consistent from one engineer to the next. The interpretation of the tools may also vary from person to person. The custom tools that are used may not actually give the results expected, because of simple logic errors, bugs or misconfiguration. The results are interpreted based in many cases on what the engineer thinks he or she is seeing, as opposed to being assessed against a baseline.

Baseline understanding of what "normal" network traffic is for a particular organization should be documented to allow for these comparisons. These baselines should exist not just for what is normal IP traffic, but also should exist for systems on the network. Packet traffic may continue to look normal on the "wire" but there is a malicious payload that those packets carry, and may be set off when it hits a server or system. This may modify a systems registry file, add new files (as with Trojans) or give the hacker access to the system. He/She could then come into the network via expected network traffic, and gain root access to a system, making modifications at will. Knowing how a system looks in a known "safe" state provides a necessary point of reference for doing system forensics following a breach.

These are some of the places that QA has experience with testing and measure techniques. Specific ways in which QA can assist are:

- Use solid testing techniques to test the analysis tools to ensure the validity of the data.
- Support a walk through of the network and their systems to validate they are "clean."
- QA can document what is inspected, what is found, and what needs to be reexamined in the future, using what tools. This will help to lay the groundwork for comparison if a break-in does occur. One of QAI's four critical processes for their strategic process is to

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

"manage by fact.[xii]" If the facts don't support that there actually has been a change, the case is that much harder to make when going to the police, or FBI, or even management.

- Help define the process, not the tools, used to do the analysis; including who does it, when it is done (how often), what is reported, and how it is reported.
- Play the role of auditor of the process. This helps to ensure accountability.
- Set up processes to support a test lab where intrusions and hacking techniques can be tested. These processes should help reduce the risk that no "attack" will escape into the production environment.
- Create processes for obtaining approvals prior to scanning or testing assaults on the network.
- Implement processes and procedures, automated where possible, to do consistent scanning and mapping for common vulnerabilities and new exposures.

It is important to note that individual performing quality assurance activities and security activities can be the same person. Throughout this paper, it is assumed that the techniques that each discipline uses can be complimentary to the other. Possibly training security professionals in quality assurance tools and techniques would be a valuable way to begin the process. It certainly should be important that quality assurance professionals understand security essentials in order to bring that into all they do.

Much of what goes into security is not difficult, but does require discipline and vigilance. Maintaining quality of any type requires the same discipline. Putting procedures into place to support the quality and security of technology implementations builds this vigilance into the overall work structure.

Conclusions

As the Internet continues to grow, as companies have greater electronic connectivity to one another[xiii], as government works to establish privacy protection for Internet users[xiv] and consumers define for themselves more clearly what they want from on-line activity[xv], the quality and security of overall systems needs to respond to meet those needs.

As a closing example, Visa shows how businesses are beginning to define requirements for security at their partners' sites as well as for themselves. Visa is attempting to manage from end to end the security of customer data. Part of their '10 Commandments' is the requirement that merchants "regularly test security systems." [xvi] Having solid methods and tools to do this testing, and having overall quality assurance will put companies ahead of the pack when it comes to best practices, as well as government regulation, peer requirements, and customer expectation.

Quality assurance and security engineers can form a cooperative alliance to support business strategy. With security and quality as part of the way a company does business, a core attention can be spent on profitably meeting the customers needs and expectations.

---

[i] Howe, Denis. (1993-2001). The Free On-Line Dictionary.
URL: http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=quality.
[ii] American Society for Quality.
URL: http://www.asq.org/info/
iii http://www.dictionary.com/cgi-bin/dict.pl?term=security

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[iv] Sinha , Madhav N. (2000). "Saving the Internet Survivors." *Quality Progress*, Vol. 34, Issue 6.
URL: http://www.asq.org/pub/qualityprogress/past/0601/sinha.html
[v] Labbate, Evelyn. (March 30, 2001). "Vulnerability as a Function of Software Quality". SANS Institute.
URL: http://www.sans.org/infosecFAQ/code/quality.htm
[vi] Hayes, Frank. (July 9, 2001). "Big, Ugly Security." Computerworld.
http://www.computerworld.com/cwi/stories/0,1199,NAV47_STO62041,00.html
[vii] There are many quality groups in existence, just as there are many security groups. Quality groups include QSQ, SQE, QAI, ISO, etc.; Security groups include SANS, CERT, $(ISC)^2$, etc. Each has a slightly different focus, but in general the topics each address are the same, and the overall goals are the same. For the purposes of his paper, I will focus on the quality group the American Society for Quality and their Bodies of Knowledge for Certified Quality Engineer (http://www.asq.org/cert/types/cqe/bok.html) and Certified Quality Manager (http://www.asq-qmd.org/cqm_bok01.html). Other cites may be included as appropriate.
[viii] http://www.asq-qmd.org/cqm_bok01.html
[ix] Schneier, Bruce. (2000). *Secrets and Lies*. New York : Wiley Computer Publishing. (Page 85).
[x] Quality Glossary;
http://www.1stnclass.com/quality_glossary.htm#<%20P%20>
[xi] SANS Security Essentials. (May 2001). Training, Book; 1-1; page 5-4.
[xii] QAI; http://www.qaiusa.com/membership/index.html
[xiii] Bernstein, Peter L. (November, 1998). "Are Networks Driving the New Economy?" *Harvard Business Review.*
http://www.hbsp.harvard.edu/hbsp/prod_detail.asp?98602
[xiv] http://www.msnbc.com/news/599136.asp
[xv] Duffy Marsan, Carolyn. (September 11, 2000). "E-Shoppers Write Holiday Wish Lists". PC World.
http://www.pcworld.com/news/article/0,aid,18410,00.asp
[xvi] Trombly, Maria. (August 11, 2000) "Visa issues 10 'commandments' for online merchants." Computer World;
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48487,00.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced