SANS SOFTWARE SECURITY with Frank Kim

Secure Coding.
Practical steps to defend your web apps.

Copyright SANS Institute

Author Retains Full Rights

This paper is from the SANS Software Security site. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Secure Coding: Developing Defensible Applications (DEV536)"
at http://software-security.sans.orghttp://software-security.sans.org/events/

Building Security into the System Development Life Cycle (SDLC)
A Case Study

James E. Purcell CISSP, GSEC, GCIH, PMP, MCSE

Building Security into the System Development Life Cycle (SDLC)
A Case Study

I. Introduction

The purpose of this paper is to help the CISSP student understand the vital role that security plays in the System Development Life Cycle (SDLC). The paper goes through each step of the SDLC and gives real-world examples to show how to build security into each of the SDLC phases. If security is built into each SDLC phase, then the resulting information system is secure by default, and later system changes are less likely to compromise overall security. The SDLC illustrated is the one defined by NIST in Special Publication 800-64 REV. 1 "Security Considerations in the Information System Development Life Cycle." Terms and definitions are taken from that document.

The case study is a customer information system for GIAC Bikes. GIAC Bikes is a company that designs and sells custom trail bikes, both at its retail store and over the GIACBikes.com web site. In the custom trail bike market, Bad Bikes is GIAC Bikes' main competitor.

Note: Bad Bikes has attempted to steal bike designs and take down the GIAC Bikes web site in the past. See "Attacking and Defending Microsoft Small Business Server 2003" (http://www.giac.org/certified_professionals/practicals/GCIH/0537.php) for a description of the GIAC Bikes network and the attack.

II. The Five SDLC Phases

The five phases of the SDLC, as defined by NIST SP 800-64, are as follows:

- Initiation—In the initiation phase of the SDLC, the primary activity is to determine the need for the information system. The system sponsor is identified, the system is linked to one or more organizational goals, and an initial definition of a problem that can be solved by an information system is documented. Steps in this phase include establishing the basic system idea, preliminary requirements definition, feasibility assessment, technology assessment, and management signoff to continue to the next phases.
- Acquisition/Development—In the acquisition/development phase, system requirements are gathered and verified. Some system components may be acquired from vendors and some components may be built in-house. The bulk of security planning takes place at this phase.
- Implementation—In the implementation phase, the new information system is tested and put into initial production mode.

- Operations/Maintenance—In the operations and maintenance phase, the information system is running in normal production, and changes and updates to the system are managed.
- Disposition—Finally, in the disposition phase, the information system is removed from production and retired.

Security issues and activities for each phase are discussed in the following sections.

III. Initiation Phase

Case Study: In the initiation phase of the SDLC, GIAC Bikes determines the need for the customer information system. GIAC Bikes' need for the system is to enable it to better track customer buying habits and preferences in order to better plan future bike designs and marketing plans.

The security activities the GIAC Bikes system development team performs in this phase is a security categorization based on a preliminary risk assessment for the information system. The security category indicates the importance of the confidentiality, integrity, and availability (CIA) of the customer information system to GIAC Bikes.

The design team looks at several risk areas, including sensitivity of information collected; criticality of the system to GIAC Bikes; security risks common to customer information systems; and regulatory, legal, and privacy issues pertinent to customer information systems. The system design team assigns high, medium, and low risk values to each area of risk. For instance, because GIAC Bikes does business in Europe (where privacy laws are very strong) and the customer information system collects personal data, risk and impact of the confidentiality of the system information is high. Another example is that although the customer information system is very important to GIAC Bikes, business could continue if the system became unavailable for a long period of time. So, the design team assigns a low risk value for system availability. GIAC Bikes also knows that Bad Bikes has attacked its computer systems in the past, so GIAC Bikes expects that there will be future attacks.

Doing the preliminary risk assessment as part of establishing the need for the system helps identify any security show stoppers before much time and effort goes into the next SDLC phases. It also gets the design team thinking about security issues early in the design process. Based on the preliminary risk assessment, the team puts the GIAC Bikes customer information system in a high risk category.

IV. Acquisition/Development Phase

Case Study: In the acquisition/development Phase of the SDLC, GIAC Bikes begins designing the complete customer information system. Detailed requirements are gathered and verified. Acquisition and development alternatives are considered and the best alternative is chosen. Based on its analysis of the system requirements and the available alternatives, GIAC Bikes begins a Request for Proposal (RFP) process to acquire a customer information system from a third-party vendor.

As more detailed system requirements are gathered and verified, GIAC Bikes expands on the preliminary risk assessment to include the new detailed requirements. Because the decision was made to buy an outside product, GIAC Bikes adds security requirements into the Service Level Agreement (SLA) section of the RFP. For instance, GIAC Bikes decides to implement separation of duties within the customer information system by using a role-based access control system for users of the application, so that requirement is documented in the RFP. GIAC Bikes also specifies internal security controls to reduce risks. Administrators of the system will have new background checks. Backups of the system will be encrypted because sensitive customer information will be collected. An intrusion prevention system (IPS) will be added to the GIAC Bikes network to prevent network-based attacks against the customer information system. GIAC Bikes also develops a test plan in this phase to ensure that all the planned security controls function as specified.

Because the new customer information system needs to integrate into other GIAC Bikes information systems (such as the accounting system), GIAC Bikes examines all the integration points and looks for new security risks that are introduced. New and improved controls are planned for dealing with any integration issues. For instance, the decision is made to use IPSEC to authenticate and encrypt any data that passes from the customer information system server to the accounting server.

Note that GIAC Bikes made the decision to buy a customer information system in this case study. See “Defining and Understanding Security in the Software Development Life Cycle” (http://www.giac.org/resources/whitepaper/application/342.php) for a case study in which GIAC Bikes decides to develop the customer information system internally.

V. Implementation Phase

Case Study: In the implementation phase, GIAC Bikes installs the new customer information system and begins testing all of the system functionality. This testing includes checking that all security controls specified in the acquisition/development phase operated as designed. All integration points with other GIAC Bikes systems are tested. Users of the customer information system receive training on the new system. This training includes updated security

awareness training. In the case of GIAC Bikes, the employees receive training about how to protect private customer information. In particular, they receive training on how to recognize and resist social engineering attacks. The GIAC Bikes risk assessment revealed that social engineering to get personal customer information is a major risk.

After the GIAC Bikes customer information system undergoes a shakedown period and all system functionality (including security) is certified through testing and verification, GIAC Bikes senior management formally accepts (accredits) the system to go into production.

VI. Operations/Maintenance Phase

Case Study: In the operations/maintenance phase, GIAC Bikes begins regular production operation of the customer information system. Because GIAC Bikes bought its customer information system from an outside vendor, a big part of this phase is monitoring system performance to make sure that the system meets the SLAs that were specified when the system was purchased. Updates and enhancements to the system also must be evaluated and applied when necessary.

Specific security actions that take place in this phase for GIAC Bikes make sure that any changes to the system are applied through the GIAC Bikes configuration management process. GIAC Bikes monitors and audits the customer information system for any unauthorized changes to the system. Any proposed changes to the system are evaluated for security impacts. For example, the vendor releases a system upgrade that requires a new version of the system's Oracle database. GIAC Bikes determines that the new version will require a new database server. GIAC Bikes will have to make sure that the new database server is hardened to meet the customer information system security requirements. Another type of system change that GIAC Bikes monitors is user roles. GIAC Bikes implemented role-based access control to meet the security requirement of separation of duties in the system. So, GIAC Bikes monitors user access changes to make sure "access creep" does not occur and a user does not gain more access than required to do his job (least privilege).

Finally, through the IPS system, GIAC Bikes continuously monitors for attacks against the system. Any detected attacks can trigger the GIAC Bikes incident response plan.

VII. Disposition Phase

Case Study: Any time a part of the GIAC Bikes customer information system is upgraded or replaced, GIAC Bikes carries out disposition phase security activities. For example, when the old database server is replaced by the new model for the Oracle database upgrade, GIAC Bikes verifies that the old data was successfully transferred to the new system and that no customer information

or transaction was lost or converted incorrectly. Before the old database server is re-purposed or disposed of, GIAC Bikes sanitizes the disk drives to remove all traces of the customer information system data. Another important part of the disposition phase is proper handling of old backup media. Backup tapes that have been used up to their expiration lives are destroyed and are not reused for any reason.

VIII. Summary

This case study went through the System Development Life Cycle (SDLC) of the customer information system for GIAC Bikes. Security activities at each step of the SDLC were illustrated. It is important to note that neglecting these security activities at any step of the SDLC will severely compromise the system's security.

A good source of a comprehensive list of security controls that can be applied throughout the SDLC is NIST SP 800-53 "Recommended Security Controls for Federal Information Systems" (http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf).

Last Updated: June 20th, 2013

Upcoming SANS App Sec Training

SANS vLive - DEV544: Secure Coding in .NET: Developing Defensible Applications	**DEV544 - 201307,**	**Jul 15, 2013 - Aug 07, 2013**	**vLive**
Community SANS Halifax	**Halifax, NS**	**Jul 22, 2013 - Jul 27, 2013**	**Community SANS**
Network Security 2013	**Las Vegas, NV**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS vLive - DEV541: Secure Coding in Java/JEE: Developing Defensible Applications	**DEV541 - 201310,**	**Oct 08, 2013 - Oct 31, 2013**	**vLive**
Community SANS Paris @ HSC - DEV522	**Paris, France**	**Oct 14, 2013 - Oct 18, 2013**	**Community SANS**
SANS Dubai 2013	**Dubai, United Arab Emirates**	**Oct 26, 2013 - Nov 07, 2013**	**Live Event**
SANS South Florida 2013	**Fort Lauderdale, FL**	**Nov 04, 2013 - Nov 09, 2013**	**Live Event**
SANS vLive - DEV544: Secure Coding in .NET: Developing Defensible Applications	**DEV544 - 201311,**	**Nov 04, 2013 - Nov 27, 2013**	**vLive**
South Florida 2013 - DEV522: Defending Web Applications Security Essentials	**Fort Lauderdale, FL**	**Nov 04, 2013 - Nov 09, 2013**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**