APPLICATION SECURITY CHEAT SHEET

BY: Hrishikesh Sivanandhan

Deploying application in a secure manner has become more critical today then ever before. Enterprises deploy several applications at very short notice. Business demands increased automation and more Internet enabled applications. Security is often considered after the application has been developed and is about to go live or in some cases even after the systems have gone live. This article takes a look at some of the critical factors that needs to be looked at for securing applications.

There are several security considerations that need to be met at different stages in the application life cycle.

PHASE 1: DEVELOPMENT STAGE

Identify and document Application security requirements: Majority of the concerns with respect to security of an application can be addressed during the *development* stage itself. The software development team (either in-house or outsourced) should be presented with the necessary security requirements. As an example if the security policy states that "Password complexity should be enabled for all user accounts", this control cannot be enforced if the application does not support this feature. The software development team should ensure that the security requirements are implemented in the applications to be developed.

The security requirements should be part of the RFP provided to the application vendor, along with the functional requirements. This will ensure that security features are considered at product design and development stage.

Ideally the application security requirements should include controls in the following areas.

1.	Authentication & Authorization	6.	Session management
2.	Auditing & Logging	7.	Data encryption
3.	Password controls	8.	Interaction with other applications
4.	Input validation	9.	Error handling
5.	Web application controls	10.	Documentation

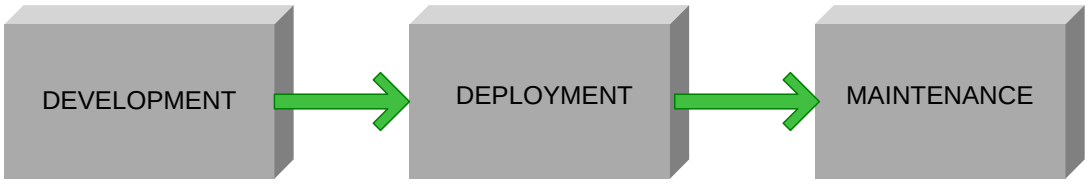

Fig: Application Security Life Cycle

PHASE 2: DEPLOYMENT STAGE

1. ***Make the Application owner responsible***: Typically, multiple teams are involved in deployment and maintenance of an application viz. the software vendor, the facilities management team, the technical support team etc. Often it becomes difficult to enforce security controls, as there is no single person accountable for the same. Identify a person (referred to as Application owner) who can co-ordinate with various teams (internal or outsourced) to implement the security controls. This person should have sufficient authority to drive security initiatives for the respective application.
2. ***Conduct application security testing before going live*:** There should be a security assessment conducted to ensure that the controls specified in the application security requirements have been properly implemented. Security testing of the application should be conducted through an independent third party or by the software vendor. All the gaps found during the testing should be plugged before moving the application into the production environment.
3. ***Conduct application load testing***: This is relevant only for applications catering to large number of users e.g. an internal SAP system or an Internet Banking application. For such large applications, absence of load testing might lead to unforeseen system failure under excessive load.
4. ***Secure the OS, database and related components***: It is important to ensure that the OS and database supporting the application are also secured as per vendor recommendations. As an example if there is no anti virus installed to protect the OS then the application data can get easily corrupted due to a virus attack.

5. ***Provide Firewall protection***: All applications including those serving internal users and Internet users should be protected by a network level Firewall. This will help to reduce the risk of attack since the access would be limited only to essential users and relevant ports.
6. ***Document all the settings***: Application owner should ensure that detailed documentation is available for the application including the following:
    a. Application installation
    b. Configuration settings
    c. Backup and recovery procedure

    This will ensure that systems can be recovered easily in the event of failure and can also assist in streamlining system administration.(person-independent)

PHASE 3: MAINTENANCE

1. ***Apply Security patches and updates regularly***: Once deployed in production, it should be ensured that all necessary security patches and updates are regularly tracked and applied. This will include security patches for the application software, supporting OS, database and any other software components. Care should be taken to ensure that adequate testing is conducted prior to deployment of these patches.
2. ***Review and take action on security logs***: Security logs often contain critical information. The benefits of security logs are obtained only if there is a system for analyzing the logs. The application owner should ensure that there is a process for periodic analysis of logs and corrective actions are taken whenever required.
3. ***Ensure changes do not affect security***: Unplanned or undocumented changes often lead to insecure systems. Before any critical changes (e.g. incorporating new feature into the application) are made to the application or supporting infrastructure it should be analyzed for possible security implications. Any identified security risks should be mitigated before implementing the change.
4. ***Manage user accounts securely***: Ensure that all application users are created after proper authorization and are provided privileges on a need to have basis. The user provisioning process should ensure that all access is revoked when a user quits.

SUMMARY

Security is a continuous process, which needs to be addressed during each stage of application lifecycle. Security cannot be an afterthought; it should be built into the application (right from start-retrofit). Key ideas presented in this article can be used for strengthening the application security at development, deployment and maintenance stage. Though there are more areas that need to be looked at in a comprehensive application security exercise, this can be used as an initial checklist.