Wie sicher sind Applikationen und Geschäftsprozesse?

Sicherheitsanforderungen einer Applikation (Programm) sollen bereits zu Entwicklungsbeginn ermittelt und abgestimmt werden. Eine nachträgliche Implementierung ist bedeutend teurer und bietet meist weniger Schutz als Sicherheit, die von Beginn an im Systementwicklungs- oder Auswahlprozess integriert wurde.

Wolfgang Sidler

Sicherheit sollte daher integrierter Bestandteil des gesamten Lebenszyklus einer Applikation (SDLC) bzw. Produktes sein. Eine aktuelle Studie der Fachgruppe Security (fgsec) der Schweizerischen Informatikgesellschaft zeigte auf, dass sieben von zehn Unternehmen, die SAP einsetzen, die Kommunikation zu Themen der SAP-Security als ungenügend bewerten. In fünf von zehn Unternehmen sind die Benutzer mit zu vielen Authentifizierungsmechanismen konfrontiert. In jedem zweiten Unternehmen findet sich ein zu sorgloser Umgang mit den elektronischen Dokumenten beim Export aus dem SAP-System und beim Druckprozess.

Eine Applikation (Programm) besitzt ein Umfeld, in welchem sie betrieben wird. Ein sich ereignender Systemprozess (Geschäftsprozess) stösst eine Applikation zur Bearbeitung an (Anfrage). Diese erfüllt die angeforderte Dienstleistung und gibt ein erarbeitetes und erwartetes Ergebnis (Resultat) zurück. Dabei greifen die Funktionen einer Applikation über ein logisches und physisches Datenmodell auf die Daten zu.

In diesem Verfahren gibt es verschiedene Bereiche, die kontrolliert ablaufen müssen. Nebst der Qualität der Applikationsfunktionen (korrekte Abläufe, Berechnungen, Konsolidierungen, Aufbereitung, Bedienung, Inhalte, etc.) sind dabei verschiedene Sicherheitskriterien zu erfüllen.

Diese Kriterien können durch die Umsetzung der folgenden Sicherheitsbereiche erfüllt werden:

Innere Applikationssicherheit (Funktionssicht)
- Sicherheitsadministration (Rechtevergabe, -verwaltung und Accounting)
- Internes Kontrollsystem IKS (Verarbeitungskontrolle von Transaktionen, Eingabekontrollen, Zurückweisung von Daten, Nachvollziehbarkeit und Überwachung – Audit Trail)
- Sicherheitsdienste und -mechanismen der Applikation
- Sicherheit in lokalen, vernetzten und verteilten Applikationen
- Datenschutzgesetz (DSG)

Äussere Applikationssicherheit (Verwendungssicht)
- Zugriffsschutz
- Schnittstellen zu anderen Applikationen
- Problem- und Change-Management Prozess
- Datensicherungsverfahren
- Qualität der verwendeten Plattformen und im Netzwerk
- Urheber und Lizenzrechte (URG)
- Archivierung und Printing
- Outsourcing

Typische Sicherheitsanforderungen, die an ein gesamtes IT-System oder auch an eine Einzelkomponente oder ein Produkt gestellt werden, seien im folgenden kurz erläutert:

Identifizierung und Authentisierung
Beim Schutz der Identität geht es darum, dass sich niemand für das System oder einen seinen Benutzer ausgeben und entsprechende Aktionen im System unter einer falschen Identität auslösen kann. Die Benutzer des Systems, die Systemkomponenten und ihre Kommunikationspartner sollten jederzeit korrekt authentifiziert werden. Bei den vom System entgegengenommenen und im System gespeicherten Daten sollte der Erzeuger stets identifiziert werden können. Dazu muss nicht nur die behauptete Identität des Benutzers festgestellt, sondern auch die Tatsache nachgeprüft werden, dass der Benutzer tatsächlich die Person ist, die er zu sein vorgibt. Dies geschieht, indem der Benutzer dem System Informationen liefert, die fest mit dem betreffenden Benutzer verknüpft sind.

Zugriffskontrolle, Integrität und Vertraulichkeit
Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass Benutzer und Prozesse daran gehindert werden, Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben oder für die keine Notwendigkeit zu einem Zugriff besteht. Desgleichen wird es Anforderungen bezüglich der unbefugten Erzeugung, Änderung oder Löschung von Informationen geben. Dies trifft auch für die mit dem System oder innerhalb des Systems ausgetauschten Daten während der Übertragung über Netzwerke zu.

Prüfbarkeit, Nachvollziehbarkeit und Beweissicherung
Für Geschäftsvorfälle sollten verbindliche Daten vorhanden sein, die auch eine Beweisbarkeit des Geschäftsvorgangs unterstützen. Das Abstreiten eines Geschäftsvorgangs sollte dadurch nicht möglich sein. Bei vielen Systemen wird es erforderlich sein sicherzustellen, dass über Handlungen die von Benutzern bzw. von Prozessen im Namen solcher Benutzer ausgeführt werden, Informationen aufgezeichnet werden, damit ihre Folgen später dem betreffenden Benutzer zugeordnet werden können und der Benutzer dafür verantwortlich gemacht werden kann.

Verfügbarkeit und Zuverlässigkeit
Das System sollte jederzeit zur Informationsverarbeitung und zum Dialog mit seinen Benutzern verfügbar sein. Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass zeitkritische Aufgaben genau zum erforderlichen Zeitpunkt durchgeführt werden, also nicht früher oder später, und es wird sicherzustellen sein, dass zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können.
Im logischen Aufbau von Systemen zur Informationsverarbeitung kann man Sicherheitsfunktionen zu Diensten zusammenfassen. Dabei wird unterschieden zwischen Rechnerebene, der Netzwerke und der Anwendungsebene. Daraus ergeben sich folgende grundsätzliche Sicherheitsdienste:

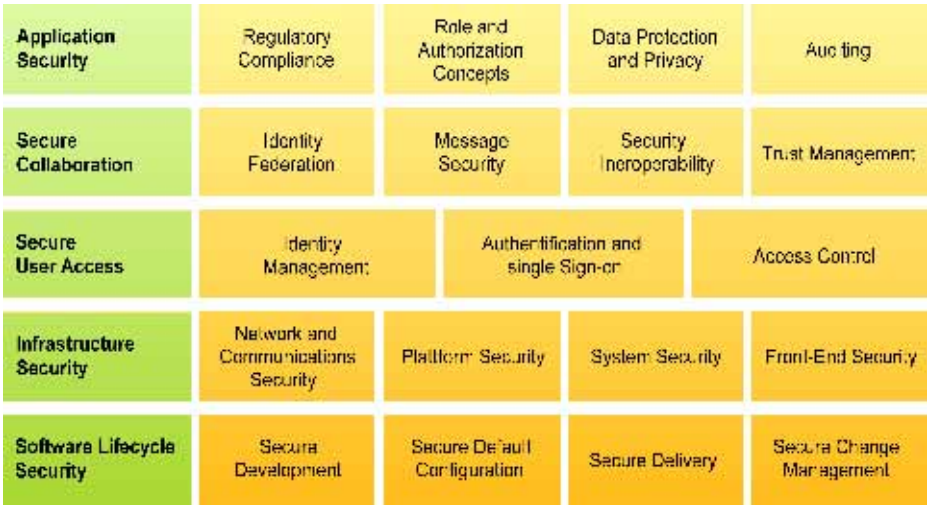

Abbildung 1: Die Sicherheitsmodule einer Applikation.

Kommunikationsdienst (Netzwerksicherheit)
Der Kommunikationsdienst verbindet die einzelnen Rechner im Unternehmen und gewährleistet bei der Übertragung von Daten zwischen Betriebssystem- und Anwenderprozessen ihre Integrität. Durch Verschlüsselung kann der Kommunikationsdienst auch Vertraulichkeit auf der Netzwerkebene, zwischen den einzelnen Rechnern, gewährleisten. Die Sicherung von Integrität und Vertraulichkeit bei der Datenübertragung kann aber auch auf der Transportebene zwischen Anwendungsprozessen oder sogar innerhalb der Anwendungsebene stattfinden.

Beweisssicherungsdienst (Auditing und Logging)

Beweissicherung zu Systemvorgängen wird durch Log-Dateien auf Betriebssystem- und Netzwerkebene erreicht. Dabei können je nach gewünschtem Grad der Detaillierung Dateizugriffe, Verbindungsaufbauwünsche, Netzwerkadressen oder Art und Dauer des Zugriffs aufgezeichnet werden. In betriebswirtschaftlichen Systemen wird das Erzeugen von Belegen insbesondere die Revision des Systems unterstützt. Ein hoher Beweiswert für elektronische Geschäftsvorfälle wird durch den Einsatz digitaler Signaturen auf Anwendungsebene erreicht.

Administrations- und Überwachungsdienst

Eine grosse Bedeutung über alle Ebenen hinweg kommt dem Administrations- und Überwachungsdienst zu. Das gesamte Funktionieren der IT-Landschaft wird hier organisiert und kontrolliert. Anfallende Aufgaben sind über eingesetzte Werkzeuge und Administratoren auf die verschiedenen Ebenen verteilt, sollten aber idealerweise an einer Stelle konzentriert und über eine gemeinsame Systemmanagement-Konsole angeboten werden.

Konzept

Für intern entwickelte oder eingekaufte Applikationen, Lösungen und Systeme erfolgt eine phasenweise Begleitung durch den IT-Sicherheitsbeauftragten. Somit können alle sicherheitsrelevanten Bereiche in enger Zusammenarbeit mit dem Projektteam rechtzeitig und proaktiv identifiziert und anforderungsgerechte Kontrollmassnahmen (IKS) vorgeschlagen werden. Für eine Betriebsaufnahme von Applikationen die ohne oder nur mit marginaler interner Begleitung entwickelt worden sind, ist als zwingende Voraussetzung für die Betriebsaufnahme die Erstellung eines Sicherheits-Konzepts bzw. eine Stellungnahme des IT-Sicherheitsbeauftragten erforderlich.

Checkliste

- Sind Dateneigentümer und Applikations-Verantwortlicher bestimmt?
- Sind die Anforderungen bezüglich Verfügbarkeit, Datenschutz und Datensicherheit definiert worden?
- Sind die im Zusammenhang mit Schnittstellen verbundenen Risiken bekannt und durch geeignete Massnahmen entschärft worden?
- Sind die Aufbewahrungsfristen für die verschiedenen Daten in Form von Listen, Bändern, Fichen oder optischen Speichern definiert worden?
- Sind alle bekannten Risiken und Schwachstellen bekannt und dokumentiert und dem Management kommuniziert? Welches sind die akzeptablen Restrisiken?
- Wie erfolgt die Überwachung des Systems bezüglich möglicher Sicherheitsverletzungen und wie sind die Eskalationen bei Verstössen?
- Wie ist die Benutzerverwaltung (ID-Management) konzipiert worden?
- Hat die Applikation eine Schnittstelle zum Microsoft Active-Directory (ADS) bzw. LDAP?
- Hat die Applikation ein User Login und Passwort Management?
- Welche Applikations-Architektur wird von der Applikation unterstützt?
- Wurden bereits bei der Entwicklung der Applikation sicherheitsrelevante Module berücksichtigt (z. B. Verschlüsselung, Buffer overflow Schutz etc.)?
- Muss der Datenverkehr zwischen Anwender und Applikation über das Netzwerk verschlüsselt werden (Vertraulichkeit)?
- Kann die Applikation in eine Single-Sign-On (SSO)-Umgebung integriert werden?
- Wurden die rechtlichen Aspekte berücksichtigt und eingehalten?
- Sind alle internen und externen Kommunikationswege dokumentiert und entsprechend gegen Missbrauch geschützt?
- Wie werden Applikations- und Sicherheits-Updates eingespielt?
- Wurde ein Disaster-Recovery-Konzept erstellt?
- Sind die Abhängigkeiten der Applikation zu den Geschäftsprozessen bekannt?
- Wie sieht das Backup/Restore-Konzept aus?
- Ist Remote-Access für externe und/oder interne Mitarbeiter notwendig bzw. sicher mit einer 2-Factor Authentifizierung (SecureID Token)?
- Braucht der Lieferant/Hersteller der Applikation einen Remote-Access Zugang? Wenn ja, ist die Sicherheit gewährleistet?
- Wurde die Funktionalität der Applikation durch den Auftraggeber inkl. Sicherheitsbeauftragten abgenommen (User Acceptance Test)?
- Sind die Lizenz- und Wartungsverträge vorhanden?
- Wurde der Quellcode hinterlegt (Escrow-Vertrag)?
- Ist die Applikation gut dokumentiert?
- Gibt es ein klar definiertes und integeres Installations- und Deinstallations-Vorgehen? ■