ILLUSTRATION: CW/THÜ

Sicherheit von Anfang an

In einem Systementwicklungsprozess oder in einem Evaluationsverfahren für ein Produkt sollte zuerst an die Sicherheit gedacht werden. Das ist billiger und sicherer als die nachträgliche Implementierung von Security-Massnahmen. **VON WOLFGANG SIDLER**

Sicherheit sollte ein integrierter Bestandteil des gesamten Lebenszyklus einer Applikation beziehungsweise Produktes sein – und daher bereits zu Beginn der Entwicklung ermittelt und abgestimmt werden. Eine aktuelle Studie der ISSS (Information Security Society Switzerland, vormals fgsec) zeigt, 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. Ebenfalls in jedem zweiten Unternehmen wird mit den elektronischen Dokumenten beim Export aus dem SAP-System und beim Druckprozess allzu sorglos umgegangen.

Eine Applikation besitzt ein Umfeld, in dem 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. Neben der Qualität der Applikationsfunktionen (korrekte Abläufe, Berechnungen, Konsolidierungen, Aufbereitung, Bedienung, Inhalte, etc.) sind dabei verschiedene Sicherheitskriterien zu erfüllen. Diese können durch die Umsetzung folgender Sicherheitsbereiche erfüllt werden:

- Sicherheitsadministration (Rechtevergabe und -verwaltung gemäss RBAC-Modell)
- Internes Kontrollsystem IKS (Transaktionskontrolle, Eingabekontrollen, Nachvollziehbarkeit)
- Sicherheit in lokalen, vernetzten und verteilten Applikationen
- Datenschutzgesetz, Urhebergesetz (DSG, URG)
- Zugriffsschutz, Authentisierung

Wolfgang Sidler ist Senior Security Consultant bei Infoguard und Mitautor des «Sicherheitshandbuches für die Praxis».

- Schnittstellen zu anderen Applikationen und Outsourcing-Partner
- Problem- und Change-Management-Prozess
- Datensicherungsverfahren (Backup, Disaster-Recovery, BCM)
- Qualität der verwendeten Plattformen und im Netzwerk (Hardening)
- Archivierung und Printing

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

Identifizierung und Authentisierung: Beim Schutz der Identität geht es darum, dass sich niemand für das System oder einen seiner 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, ob der Benutzer tatsächlich die Person ist, die er zu sein vorgibt. Dazu liefert der Benutzer dem System Informationen , die fest mit dem jeweiligen 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 beziehungsweise von Prozessen im Namen solcher Benutzer ausgeführt werden, Informationen aufgezeichnet werden, damit die Folgen solcher Handlungen später dem betreffenden Benutzer zugeordnet werden können und dieser für seine Handlungen verantwortlich gemacht werden kann.

Protokollauswertung: Bei vielen Systemen wird sicherzustellen sein, dass sowohl über gewöhnliche als auch aussergewöhnliche Vorgänge ausreichend Informationen aufgezeichnet werden. So kann durch Nachprüfungen später festgestellt werden, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.

Verfügbarkeit und Zuverlässigkeit: Das System sollte jederzeit zur Informationsverarbeitung und zum Dialog mit seinen Benutzern verfügbar sein. Bei vielen Systemen wird es auch erforderlich sein, sicherzustellen, dass zeitkritische Aufgaben genau zu jenem Zeitpunkt durchgeführt werden, zu dem es erforderlich ist, nicht früher oder später. Darüber hinaus wird sicherzustellen sein, dass zeit-unkritische Aufgaben nicht in zeitkritische Aufgaben umgewandelt werden können.

Übertragungssicherung: Dieser Begriff umfasst alle Funktionen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind: Authentisierung, Zugriffskontrolle, Datenvertraulichkeit, Datenintegrität sowie Sende- und Empfangsnachweis. ■

Checkliste

- ✓ Sind Dateneigentümer und Applikations-Verantwortlicher bestimmt?
- ✓ Sind die Anforderungen bezüglich Verfügbarkeit, Datenschutz und Datensicherheit definiert?
- ✓ Sind die im Zusammenhang mit Schnittstellen verbundenen Risiken bekannt und durch geeignete Massnahmen entschärft?
- ✓ Sind die Aufbewahrungsfristen für die verschiedenen Daten in Form von Listen, Bändern, Fichen oder optischen Speichern definiert?
- ✓ Sind alle bekannten Risiken und Schwachstellen 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?
- ✓ Hat die Applikation eine Schnittstelle zum Microsoft Active Directory 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, Bufferoverflow-Schutz etc.)?
- ✓ Kann die Applikation in eine Single-Sign-On-Umgebung integriert werden?
- ✓ Muss der Datenverkehr zwischen Anwender und Applikation über das Netzwerk verschlüsselt werden (Vertraulichkeit)?
- ✓ 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 Zweifaktor-Authentifizierung (Secure-ID Token)?
- ✓ Ist es notwendig, dass der Lieferant/Hersteller der Applikation einen Remote-Access-Zugang hat? 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?