Sicherheit für interaktive Portale

Fit gegen Angriffe aus dem Internet

Sicherheit für Portallösungen muss ganzheitlich betrachtet werden

Bildquelle: fotolia.com

Web-Portale, die dem Austausch sensibler Daten dienen, müssen höchst sicher sein, um Angriffsversuchen aus dem Internet Stand zu halten. Das Thema Sicherheit ist dabei ganzheitlich zu betrachten. Es beginnt bei der Schulung der Entwickler, geht über die Architektur, die Entwicklung bis hin zum Test und zur Reaktion auf eingetretene Sicherheitsvorfälle. Im folgenden Artikel werden vier wesentliche Pfeiler eines Sicherheitskonzepts für Portale mit hohem Sicherheitsbedürfnis vorgestellt.

Viele Banken und Versicherungen bieten ihren Kunden und Geschäftspartnern interaktive Inhalte im Internet an. In der Regel werden diese über sogenannte Portale im Web zur Verfügung gestellt. Die rein fachliche Implementierung von Webanwendungen stellt heute keine große Herausforderung mehr dar. Schwierig und spannend wird es dann, wenn es um Portallösungen im Umfeld komplexer Branchen geht.

Autor:
Björn Kibbel

Manager Development und Integration Services bei der innobis AG

Hier sind Internetportale meist keine Selbstläufer mehr, sondern mit Risiken und damit hohen Sicherheitsanforderungen und Betriebskosten behaftet. Dies ist deshalb der Fall, da Kunden und Geschäftspartnern der Zugriff auf Echtdaten aus dem Bestandssystem ermöglicht wird. So können sie Daten der laufenden Geschäftsvorfälle live im Internet ‘beobachten‘ oder sich als Partner mit Geschäftsvorfällen direkt in die internen Prozesse integrieren. Vor dem Hintergrund der Berichterstattung über Datenklau von Millionen von Zugangsdaten kommt dann schnell die Frage auf, wie solche Szenarien abzusichern sind, so dass alle Sicherheitsbedürfnisse erfüllt sind und das eigene Unternehmen nicht auch in die Schlagzeilen gerät. Im folgenden Artikel zeigt Björn Kibbel, Manager Development und Integration Services bei der innobis AG, einige Ansätze auf, sich dieser Frage zu nähern und stellt ein paar grundlegende Maßnahmen vor, die zur Absicherung gegen Angriffsversuche aus dem Internet dienen. Dabei gelten die folgenden Ausführungen für eine SAP-Landschaft als auch für jede andere IT-Gesamtarchitektur, in die sich die Portallösung integriert.

Ganzheitlicher Ansatz beim Thema Sicherheit

Das Thema Sicherheit spielt auf allen Ebenen des späteren Portalszenarios eine Rolle. Es beginnt bei der Schulung der Entwickler vor Projektbeginn, geht über die Architektur und die Entwicklung bis hin zum Test, umfasst aber auch den Software-Betrieb, vertragliche Bestandteile zum Beispiel mit Rechenzentrums-Dienstleistern und die Reaktion auf eingetretene Sicherheitsvorfälle (siehe Abb. 1). Dabei ist es auf keiner der Ebenen möglich, eine absolute Sicherheitsstufe zu erreichen bzw. alle erdenklichen Risiken auszuschalten. Vielmehr geht es immer darum, Sicherheitsnutzen und die dazu gehörigen Kosten für die Umsetzung oder den Aufbau von entsprechenden Maßnahmen gegeneinander abzuwägen, sich bewusst in die eine oder andere Richtung zu entscheiden und die getroffenen Entscheidungen zu dokumentieren. Die Sicherheit muss also als ganzheitliches Thema im Projektverlauf betrachtet werden und darf nicht nur vereinzelt auftauchen.

Vier wesentliche Teilbereiche eines Sicherheitskonzepts

Um in einem Portalprojekt die sicherheitsrelevanten Aspekte von Beginn an vollständig im Griff zu behalten, empfiehlt es sich, parallel zur Designphase ein Sicherheitskonzept zu erstellen. An diesem lassen sich alle späteren Entscheidungen mit Sicherheitsauswirkungen verproben. Sicherheit gehört damit in den Verantwortungsbereich des Projektleiters.

Abb. 1: Die Sicherheit von interaktiven Portalen ist ganzheitlich zu betrachten

Bildquelle: innobis AG

Grundsätzlich wird das Thema Sicherheit wie folgt behandelt:

1. Ermittlung des Schutzbedarfs auf allen Ebenen des umzusetzenden Szenarios
2. Ermittlung der möglichen Bedrohungsszenarien, die sich für das geplante Szenario ergeben können
3. Zuordnung von Schutzmaßnahmen für alle Bedrohungsszenarien, die den Bedarf decken und die Kosten in erträglichem Rahmen halten
4. Ableitung von Checklisten und Prüfpunkten aus den umzusetzenden Schutzmaßnahmen für die einzelnen Projektphasen

1. Schutzbedarfsermittlung

Um die eigenen Schutzziele zu ermitteln, werden die BSI-Standards 100-2 zur Vorgehensweise im IT-Grundschutz herangezogen. Sie teilen den Schutzbedarf in drei Grundwerte ein: Verfügbarkeit, Vertraulichkeit und Integrität. Jeder dieser drei Grundwerte ist mit einer von drei sogenannten Schutzbedarfskategorien bewertet:

- Normal: Das schwerwiegendste Schadensszenario wirkt sich nur auf einzelne Externe oder Mitarbeiter aus.
- Hoch: Das schwerwiegendste Schadensszenario wirkt sich auf Teilbereiche der nationalen Öffentlichkeit aus oder hat im eigenen Bereich nur schwerwiegende Auswirkungen.
- Sehr hoch: Das schwerwiegendste Schadensszenario wirkt sich auf eine breite deutsche Öffentlichkeit aus und/oder hat im eigenen Bereich existenzbedrohende Auswirkungen.

Die vermeintliche Schlichtheit des Schemas mag dazu verführen, alle drei Grundwerte mit der Bedarfskategorie ‘sehr hoch‘ zu bewerten. Mit Blick auf die daraus resultierenden Projektkosten ist jedoch eine sehr sorgfältige Betrachtung ratsam, bedenkt man, dass hinter einer sehr hohen Verfügbarkeit weltweit verteilte Servercluster stehen können. Eher Firmen wie Google oder Amazon sollte in diesem Zusammenhang die Bedarfskategorie ‘sehr hoch‘ vorbehalten bleiben. Zur sorgfältigen Bewertung sind für jede Schutzbedarfskategorie die möglichen Schadensszenarien zu betrachten – wie ‘Verstoß gegen Gesetze und Vorschriften‘ oder ‘negative Innen- und Außenwirkung‘ – und die möglichen Auswirkungen zu ermitteln.

2. Identifikation von Bedrohungen

Spätestens an diesem Punkt sollten sich die Verantwortlichen externe Unterstützung ins Projekt holen, sofern intern keine ausgewiesenen Experten zur Verfügung stehen. Auf Sicherheitsaspekte spezialisierte IT-Dienstleister ermitteln für das gegebene IT-Szenario mögliche Bedrohungen. Hier werden Begriffe wie Spoofing (Verwendung fremder Identitäten), Tampering (unbefugtes Verändern

von Informationen) oder Information Disclosure (Zugriff auf vertrauliche Informationen) genannt. Die Bedrohungen werden nach Wahrscheinlichkeiten sortiert und dabei Bewertungskriterien wie notwendiger Skill-Level (Wissenstand), Motivation, Gelegenheit und Größe des Angriffs bewertet.

3. Konkrete technische Maßnahmen zum Schutz vor Bedrohungen

Aus den oben beschriebenen Vorüberlegungen ergeben sich je nach Szenario unterschiedlichste Maßnahmen. Das Projekt durchläuft von der Anforderungsanalyse über den Systemaufbau bis hin zum Betrieb mehrere Phasen. Sicherheitsaspekte sind bei jedem Schritt zu berücksichtigen. Zwar stechen die Architektur und die Betriebsinfrastruktur aus der Liste der Maßnahmen heraus, da sie offen sichtbar sind und eigene Kostenpositionen ausweisen. Gleichwohl lassen sich Fehler in der Entwicklung oder mangelhafte Tests nicht durch die sicherste Architektur oder den sichersten Betrieb ausgleichen. Microsoft veröffentlichte im Jahre 2004 den Trustworthy Development Security Lifecycle (SDL), der als Quasi-Standard bei der Umsetzung eines sicheren Softwareentwicklungsprozesses hilft.

Je nach Sicherheitsanforderungen ergeben sich unterschiedliche Architekturen. Bei sehr hohen Anforderungen an die Verfügbarkeit werden die Aufgaben so auf die Server verteilt, dass ein Ausfall nicht den kompletten Service unterbricht. Dafür werden Server x-fach redundant gehalten und mit Load-Balancern die Last zwischen den verfügbaren Servern aufgeteilt.

Liegen die Anforderungen weniger auf Verfügbarkeit, sondern eher im Bereich Vertraulichkeit, sind häufig dreistufige Architekturen vorhanden, die es ermöglichen, das Bestandssystem im Back-End von der Zugriffsschicht im Web zu entkoppeln. Dabei übernimmt der Internet-Layer die Aufgabe, die Benutzeroberfläche bereit zu stellen. Die Schicht hält keine eigenen Daten, sondern sendet ihre Datenanforderungen an den Application-Layer. Die Entkopplung vom Back-End übernimmt ein Mechanismus, der asynchron Daten zwischen Application Layer und Back-End synchronisiert. Das Intervall kann frei gewählt werden – von täglichen bis hin zu minütlichen Synchronisierungen für den Near-Online-Betrieb. Ein Durchgreifen über zwei Schichten ist in dieser Architektur nicht erlaubt. Der Verbindungsaufbau erfolgt ausschließlich aus dem Back-End, d. h. der Application Layer darf keine Verbindung zum Back-End-Layer herstellen. (s.h. Abb. 2)

Wird diese Architektur in den Betrieb übernommen, helfen diverse Infrastrukturkomponenten den Schutz vor unerlaubten Zugriffen auf der Netzwerk-Ebene zu erhöhen. Für einen sicheren Datenverkehr insbesondere zwischen Web- und Internet-Layer sorgen zertifikatsbasierte Verschlüsselungen. Ein Reverse Proxy als Einfallstor erlaubt die Kontrolle der Aufrufe und leitet diese intern an die verarbeitenden Server weiter. Unverzichtbar ist ein Virenscanner, wenn die Möglichkeit besteht, Dokumente hochzuladen. Ein sogenanntes Intrusion-Detection-System untersucht den Netzwerkverkehr auf ungewöhnliche Muster, die sich aus Angriffen ergeben und sperrt temporär den Zugriff von bestimmten Internetadressen. Neben dem sicheren Aufbau der Infrastruktur sind kontinuierlich Überwachungen und Updates des Systems notwendig. In regelmäßigen Zyklen veröffentlichen die Hersteller von Betriebssystem-Software, darunter auch die SAP AG, sicherheitskritische Hinweise auf deren Basis regelmäßig Patches eingespielt werden müssen. Spezielle Sicherheitstests sorgen nach Änderungen an dem System dafür, dass sich nicht versehentlich ein Bug als sicherheitskritisch erweist.

4. Ableitung von Checklisten und Prüfpunkten aus den umzusetzenden Schutzmaßnahmen für die einzelnen Projektphasen

Die aus der Sicherheitsanalyse abgeleiteten Maßnahmen müssen im Laufe des Projekts operativ umgesetzt werden. Da es meist unmöglich ist, alle Projektmitarbeiter ausreichend in Sicherheitsfragen zu schulen, helfen Check- und Prüflisten dabei, die notwendigen Maßnahmen mit der erforderlichen Qualität umzusetzen.

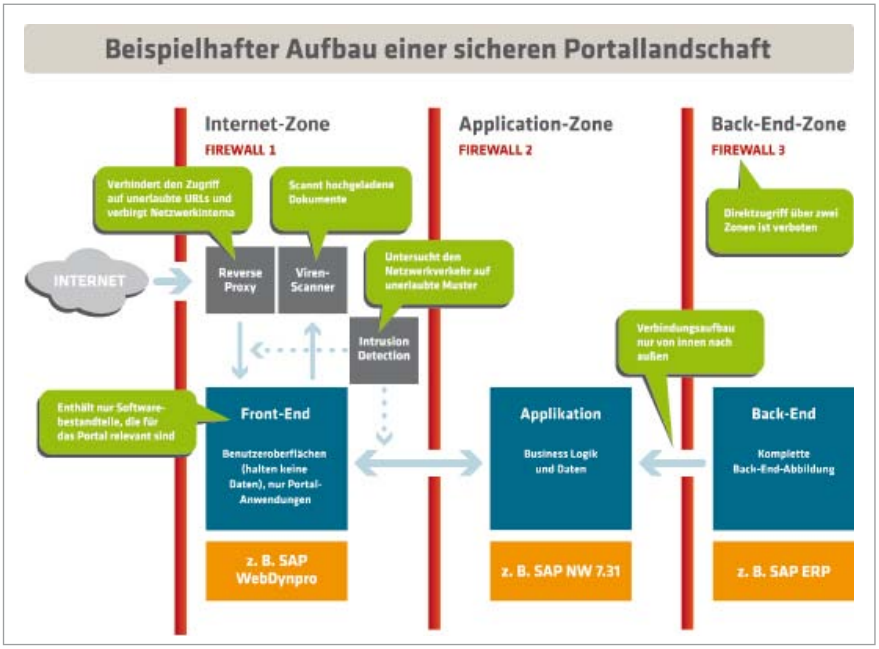

Abb. 2: Möglicher Aufbau einer sicheren Portallandschaft mit normalen Ansprüchen an die Verfügbarkeit

Bildquelle: innobis AG

Fazit

Das Thema Sicherheit für interaktive Anwendungen im Internet ist von der ersten Idee bis hin zum laufenden Betrieb ganzheitlich zu betrachten und in jeder Phase des Lebenszyklus der Software zu berücksichtigen. Ein absolutes Maß oder eine Skala für Sicherheit gibt es ebenso wenig wie die auf alle Anforderungen passende Lösung. Der eigene Schutzbedarf muss gründlich ermittelt und entsprechende IT-Maßnahmen gegen mögliche Bedrohungen eingeleitet werden. Dabei dürfen Kostengründe für eine Entscheidung durchaus eine Rolle spielen, sofern sich die Verantwortlichen der Auswirkungen und Risiken bewusst sind und ihre Entscheidungen schriftlich fixiert haben.