Whitepaper

Sicherheit in IT-Projekten richtig umsetzen – Ein Leitfaden

IT-Security für Projektleiter

Trotz vieler anerkannter IT-Sicherheitsstandards scheitern viele IT-Projekte am Thema Sicherheit. Was es zu beachten gilt und welche Fehler man vermeiden sollte.

IT-Security in Projekten und Produkten

IT-Projekte beinhalten per Definition den Aufbau eines Systems der Informationstechnologie. Hierbei kann es sich um die reine Installation existierender Lösungen handeln oder die komplette Neuentwicklung eigener Komponenten. Auch eine Kombination ist möglich, etwa wenn Standard- oder Open-Source-Software mit eigenen Erweiterungen weiterentwickelt wird. Egal ob am Ende ein Produkt entsteht oder ein IT-System, welches anderweitig kommerziell genutzt wird, IT-Sicherheit spielt heutzutage eine zentrale Rolle für den Projekterfolg. Dies gilt auch für Systeme, bei denen IT nur eine untergeordnete Rolle für das Gesamtprodukt spielt, wie zum Beispiel die Bedienungsschnittstelle für die Zentralheizung. Auch Projekte wie Aufbau und Hosting eines Standard-Web-Shops betrifft das Thema IT-Sicherheit in gleichem Maße.

Das Thema IT-Sicherheit beschäftigt dabei Firmen aller Größen. Großkonzerne implementieren in den meisten Fällen bestimmte Sicherheitsstandards, die sie in die Lage versetzen in IT-Projekten auf standardisierte Weise höchste Sicherheitsanforderungen zu erfüllen. Kleinere und mittelständische Unternehmen haben es dabei erfahrungsgemäß schwerer. Meist alleine deshalb, weil knappe Budgets wenig Raum für Sicherheitsthemen lassen oder das entsprechende Know-how fehlt und nicht immer leicht beschafft werden kann.

IT-Sicherheit im Projekt durchsetzen

Die meisten IT-Projekte haben ein enges Budget. In den seltensten Fällen kann ein Projektleiter finanziell aus dem Vollen schöpfen. Das gilt für Projekte großer wie kleinerer Unternehmen gleichermaßen und wirkt in der Regel schwerer je kleiner das Unternehmen ist.

Wenn Sicherheit nicht als Verkaufsargument für ein Produkt oder für den Aufbau eines Systems genutzt werden kann, hat der Projektleiter es oft schwer, einen angemessenen Topf im Budget für Sicherheitsthemen vorzusehen. Denn:

- Sicherheit sieht man nicht (oberflächlich).
- Sicherheit macht das System nicht schneller.
- Sicherheit macht das System nicht einfacher zu bedienen.
- Sicherheit verkompliziert die Prozesse rund um den Betrieb.

Provokativ kann man also die Frage stellen: Warum Geld ausgeben für etwas, dass das Endprodukt verschlechtert. Erschwerend kommt hinzu, dass in den meisten Fällen die wenigsten Projektbeteiligten ein technisches Verständnis für das Thema Sicherheit haben oder schlimmer das sogenannte „gefährliche Halbwissen“. Das ist durchaus verständlich. IT-Sicherheit gehört zu den kompliziertesten Themen überhaupt. Ein geeigneter Spezialist in diesem Bereich benötigt nicht nur eine passende Ausbildung sondern auch jahrelange Praxiserfahrung, um Sicherheitsthemen sinnvoll und angemessen umsetzen zu können.

Der Mehrwert von IT-Sicherheit lässt sich nicht kurzfristig betrachten. Eine Microsite für eine einwöchige Werbekampagne etwa kann von Hackern völlig unbeachtet bleiben. Dennoch wäre es fahrlässig, IT-Sicherheit bei einem solchen Projekt gezielt auszuklammern. Umgekehrt muss man betrachten, was passiert, wenn Projekten Sicherheit fehlt. Ein erfolgreich gestarteter Web-Dienst zum Beispiel, der nach

einiger Zeit des Erfolgs unvermeidlich Hacker anlocken wird, kann sehr schnell an Reputation verlieren, wenn Sicherheitslücken offengelegt werden. Wurde Sicherheit im Projekt zu wenig beachtet, kann es sehr schwer werden, Lücken im Nachhinein nachhaltig zu schließen. In der Folge könnte der Dienst aus den Negativschlagzeilen für einige Zeit nicht herauskommen und gar eine Neuentwicklung notwendig werden, weil ein Sicherheitskonzept im vorhandenen System nicht sinnvoll umsetzbar ist.

Mittel- und langfristig setzen sich Produkte durch, die die Sicherheit ihrer Nutzen und deren Daten ernst nehmen. Lücken sind unvermeidlich – wie mit diesen umgegangen wird, ist entscheidend. Des Weiteren lassen sich aus diversen Gesetzen Mindestanforderungen an Systeme und Produkte ableiten, um auch als Geschäftsführung nicht in den Bereich der Fahrlässigkeit zu geraten und haftbar für Angriffe Dritter zu werden. Dies sollte auch für jeden Projektleiter Grund genug sein, sich mit dem Thema IT-Sicherheit auseinanderzusetzen. Die jeweilige Geschäftsführung muss dazu die Grundlagen bereit- und sicherstellen – auch aus eigenem Interesse.

IT-Sicherheit im Projekt: Von Anfang an!

Der kritische Faktor für das Thema Sicherheit bei IT-Projekten ist der Zeitpunkt. Zu oft werden Projekte aus kaufmännischer oder funktionaler Sicht betrachtet und als Proof-of-Concept realisiert, ohne Sicherheitsthemen auch nur in Betracht zu ziehen. Erfolgsaussichten und finanzielle Forecasts werden erstellt. Dann kommt es zur Realisierungsphase in welcher Sicherheitsanforderung und Datenschutzanforderungen auf welche Weise auch immer zum Vorschein kommen. Diese können im schlimmsten Falle den gesamten Business Case zerstören. Gewöhnlich sind zumindest Anpassungen vonnöten, die den Projektplan beeinflussen werden und für Projektbeteiligte zum Störfaktor werden können. Je nach dem wie weit der Proof-of-Concept als technische Basis für die tatsächliche Realisierung dienen soll, kann aufgrund der Sicherheitsanforderung eine komplette Neuentwicklung notwendig sein.

Sollte man Sicherheitsanforderung auf das nächste Release nach dem Go-Live verschieben wollen, vergrößern sich die Probleme massiv. Dies macht sich selbstverständlich auch beim Budget entsprechend bemerkbar. Ein scheidender Projektleiter kann so auch seinem Nachfolger eine entsprechende Bürde „vererben“. Jegliche Kompromisse in der Realisierung werden sich langfristig als nicht-tragbar und letztendlich teuer erweisen wie die Praxis zeigt.

Sollten bereits Verträge mit Lieferanten und anderen Partnern – zum Beispiel für Entwicklungs- oder Hosting-Leistungen – geschlossen worden sein, bevor Sicherheitsanforderung betrachtet wurden, entstehen ebenfalls massive Probleme für das Gesamtprojekt. Alle Lieferanten müssen nämlich auf die Sicherheitsanforderungen vertraglich verpflichtet werden, Standard-Verträge müssen entsprechend inhaltlich geprüft sein. Sollten diese ohnehin nicht anpassbar sein, etwa weil man Verträge mit einem größeren Unternehmen macht und eine gewisse Abhängigkeit besteht, muss selbstständig Vorsorge getroffen werden, schlimmstenfalls durch das eigene Risikomanagement. Viele Web-Agenturen beispielsweise, die knappe Preiskalkulationen vornehmen, um konkurrenzfähig sein zu können, werden Anforderungen aus Sicherheitskatalogen gesondert berechnen müssen. Auch hier ist wichtig, entsprechende Planungen frühzeitig in das Projekt zu übernehmen.

Ein praktisches Beispiel: In einem IT-Projekt soll ein Web-Shop unter Verwendung einer Standard-Software aufgebaut werden. Dies umfasst unter anderem Installation und Hosting. Änderungen an der Shop-Software seien nicht vereinbart. Das Hosting muss neben einer Härtung des Systems auch ein Patch-Management vorsehen. Dieses muss für die gesamte Betriebszeit des Web-Shops vorgesehen sein und bei kritischen Sicherheitsupdates der Shop-Software zeitnah erfolgen. Sollte dies vertraglich nicht vereinbart sein, werden Mehrkosten entstehen. Alternativ muss der Inhaber des Shops einen eigenen Prozess dafür betreiben und entsprechend Personal abstellen.

Als Erfahrung aus der Praxis lässt sich beobachten, das selbst bei Unternehmen mit einer eigenen Sicherheitsorganisation, diese oft zu spät genutzt wird. Meetings von potentiellen Projektteams sollten beispielsweise durch einen Sicherheitsberater – und übrigens auch einen Datenschutzberater – begleitet werden. So können frühzeitig auf entsprechende Sicherheits- und Datenschutzanforderungen hingewiesen und No-Gos vermieden werden. Auch sind Sicherheitsberater aufgrund ihrer Projekterfahrung meist in der

Lage einfachere technische Alternativen vorzuschlagen. Die Begleitung durch einen Sicherheitsberater kann auch bei reinen Meetings zur Ideenentwicklung ohne technischen Charakter ratsam sein.

Scheitern Projekte an Thema IT-Sicherheit, dann in der Regel an lange existierenden aber dem Projektteam unbekannten oder nicht-beachteten Anforderungen.

Sicherheit ist immer als Prozess zu verstehen

IT-Sicherheit verursacht laufende Kosten. IT-Sicherheit benötigt permanent Personal. Letzteres muss nicht zwangsläufig Vollzeit sein. Wieso ist das so? - Sicherheit ist ein Prozess! Dies gilt für alle Arten von IT-Projekten. Es folgen einige Beispiele.

Beispiel A

Eine eigens entwickelte Web-Anwendung wird in Betrieb genommen. Im Laufe des Betriebs werden Sicherheitslücken gemeldet. Es muss ein Prozess existieren, diese Meldungen entgegenzunehmen, zu prüfen und zu bereinigen. Ist die Software selbst-entwickelt, muss dieser Prozess im Unternehmen selbst etabliert werden. Handelt es sich bei der Software um eine externe Auftragsleistung, muss mit dem Lieferanten eine entsprechende Vereinbarung getroffen sein. Die Schnittstelle der internen und externen Prozesse muss definiert sein, ebenso wie entsprechende Service Level Agreements, etwa zur maximalen Bearbeitungsdauer und generellen Kostenübernahme.

Beispiel B

Eine Standard-Anwendung wird im Internet gehostet. Die Systeme wurden initial gehärtet. Durch das Auftreten neu entdeckter Sicherheitslücken in Standard-Software muss ein Patch-Management-Prozess etabliert sein. Dieser beinhaltet unter anderem die Sichtung und Einspielung von Patches. Sicherheitskritische Patches müssen zeitnah gesichtet und vorgenommen werden können. Je nach der Komplexität der Anwendung ist hierfür ein gesondertes Test-System neben dem eigentlichen Produktivsystem notwendig, um die einwandfreie Funktionsweise des Systems nach dem Patchen garantieren zu können. Auch sollte ein regelmäßiger Penetrationstests obligatorisch sein, um sicherzustellen, dass keine Komponente beim Patchen ausgelassen wird.

Beispiel C

Ein System erlaubt nicht nur Systemadministratoren sondern auch bestimmten applikativen Rollen Zugriff auf Kundendaten. Dazu wurde ein angemessenes Logging von Zugriffsaktionen umgesetzt. Selbst wenn ein Automatismus etabliert wurde, der eine Missbrauchserkennung beinhaltet, muss eine entsprechende Detektion an eine Person gemeldet und von dieser geprüft werden. Hierfür ist ein Prozess vorzusehen. Unabhängig davon sind regelmäßige Audits alleine aus Datenschutzsicht durchzuführen.

Beispiel D

Für das Hosting von Systemen wird eine Intrusion Detection eingerichtet. Diese erlaubt ein Monitoring über ungewöhnliche Ereignisse und potentielle Angriffe. Von gewissen Automatismen abgesehen, ist es notwendig, dass geeignetes Personal dieses Monitoring überwacht und gegebenenfalls Gegenmaßnahmen einleitet.

Neben diesen praktischen Beispielen gilt beim Thema IT-Sicherheit das gleiche wie in allen anderen Bereichen: Mit jedem neuen Projekt lernt man dazu und passt die eigene Prozesse entsprechend an.

Sicherheitsstandards

Möchte man einen IT-Sicherheitsprozess für ein Projekt oder ein ganzen Unternehmen aufsetzen, so muss und darf man nicht bei Null anfangen. Es gibt viele anerkannte Sicherheitsstandards, auf denen man aufbauen kann. Dies gilt auch für kleinere Projekte und kleinere Unternehmen. Große Unternehmen haben in der Regel bereits einen zertifizierten IT-Sicherheitsprozess und geben Projektleitern konkrete technische und nicht-technische Anforderungen für die IT-Sicherheit wie auch den Datenschutz vor. Man sollte sich ebenfalls informieren, ob branchenspezifische Standards vorliegen, die es einzusetzen gilt.

Möchte man den „großen Schritt“ eines Sicherheitsprozesses und den Aufbau einer eigenen Sicherheitsorganisation, also eines sogenannten „Informationssicherheits-Managementsystems“ (ISMS) nicht gehen, was vor allem für kleinere Unternehmen ein verständliches Problem darstellt, helfen Sicherheitsstandards dennoch: Entweder für die eigene Software-Entwicklung oder im Umgang mit Lieferanten und Partnern.

Ein Vorteil der einschlägigen Sicherheitsstandards ist, dass sie in Verträgen als Referenz verwendet werden können. Dies garantiert zumindest ein gewisses Mindestniveau an Sicherheit. Sind die projektbeteiligten Unternehmen nach etablierten Sicherheitsstandards zertifiziert und werden diese für das Projekt auch angewendet, sollte man sich das ebenfalls vertraglich zu sichern lassen.

Ein kleiner Überblick über einige ausgewählte Sicherheitsstandards, selbstverständlich ohne einen Anspruch auf Vollständigkeit zu erheben:

- ISO/IEC 27001: Der vermutlich am meisten genutzte, internationale Standard für unternehmensweite Informationssicherheitsorganisationen. Die konkrete Ausprägung ist unternehmens- und branchenspezifisch.
- BSI IT-Grundschutz: Ein konkreter Umsetzungskatalog für ISO/IEC 27001 herausgegeben vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI). Der IT-Grundschutz enthält ebenfalls einen öffentlich verfügbaren Katalog an konkreten technischen Sicherheitsanforderungen auf Spezifikationsniveau für unterschiedlichste Software- und Hardware-Komponenten.
- Zertifizierungen des TÜV: Unterschiedliche Unterorganisationen des TÜVs führen verschiedene technische und nicht-technische Prüfungen von IT-Systemen durch. Je nach Art der gewählten Prüfung werden allgemeine oder TÜV-eigene Zertifizierungen ausgesprochen.
- Common Criteria for Information Technology Security Evaluation: Ein internationaler Standard, der die Prüfung und Zertifizierung von Sicherheitsanforderungen in konkreten Produkten ermöglicht. Eine solche Prüfung ist in der Regel sehr umfangreich und kostenaufwendig.
- PCI-DSS und PCI-PA-DSS: Hierbei handelt es sich um Standards der Kreditkarten-Industrie, die Unternehmen erfüllen müssen, welche mit Kreditkartendaten in Berührung kommen. Diese sind öffentlich einsehbar und können aufgrund ihrer hohen Anforderungen auch sinnvoll auf andere Daten bezogen und somit in eigenen Projekten verwendet werden. Die Sicherheitskataloge enthalten konkrete technische wie organisatorische Umsetzungsmaßnahmen. Beim Standard PA-DSS geht es im Speziellen um Eigenentwicklung, die Kreditkartendaten verarbeiten.
- OWASP Top Ten Project: Das Open Web Application Security Project (OWASP) gibt als Non-Profit-Organisation Sicherheitsrichtlinien (und mehr) zur freien Verwendung heraus. Insbesondere das sogenannte „Top Ten Project“ kann als Referenz für Mindestanforderungen an sichere Web-Anwendungen verwendet werden.

Für Datenschutz gilt dasselbe!

Dieser Artikel bezieht sich in erster Linie auf IT-Sicherheit. Jedoch gelten die meisten dargestellten Problematiken gleichermaßen für Datenschutzanforderungen. Von Gesetzen und sonstigen Regelungen abgeleitete Anforderungen des Datenschutzes an IT-Projekte müssen ebenfalls so früh wie möglich in IT-Projekte getragen und umgesetzt werden. Aufgrund von nicht-verhandelbaren Gesetzesregelungen können beispielsweise fehlende Vertragsvereinbarungen regelrechte, selbst-verschuldete „Projektkiller“ werden. So wie für IT-Sicherheit ein entsprechender Spezialist benötigt wird, wird auch für den Datenschutz ein geeigneter Spezialist benötigt – im Idealfall mit Erfahrungen auch auf technischer Seite. Für die technische Umsetzung von Datenschutzanforderungen kann im weiteren Projektverlauf ein IT-Sicherheitsspezialist zu Rate gezogen werden.

Checkliste für Projektleiter

Die folgende Checkliste soll IT-Projektleitern als Orientierung dienen, um die oftmals unterschätzten Themen der IT-Sicherheit im Projekt umzusetzen. Die Liste erhebt keinen Anspruch auf Vollständigkeit. IT-Projekte unterscheiden sich erheblich in ihren Anforderungen. Sollten unternehmensweite Anforderungen gelten, sind diese selbstverständlich an erster Stelle zu beachten. Bei internationalen Projekten müssen gegebenenfalls länderspezifische Anforderungen, insbesondere auch an den Datenschutz, geprüft werden.

Ebenen der IT-Sicherheit

Sicherheitsanforderungen werden auf verschiedenen technischen Ebenen eines Projektes definiert. Da sich IT-Projekte stark unterscheiden, soll die folgende Aufstellung lediglich als Hilfe dienen, um frühzeitig bestimmte Sicherheitsthemen in einem Projekt aufzugreifen. Sie kann je nach Projekt nur teilweise oder auch gar nicht zutreffend sein. Ein vollständiges Sicherheitskonzept jedoch sollte mindestens all diese Ebenen abdecken.

Technische Ebenen:

Ähnlich des OSI-Schichtenmodells müssen die verschiedenen technischen Ebenen untersucht werden, die für ein Projekt zutreffend sein können.

- Netzwerkebene: Hierzu zählen das Netzwerkkonzept (zum Beispiel die passende Segmentierung) und alle Netzwerkkomponenten wie Switches, Router, Netzwerk-Firewalls, VLAN-Einstellungen und WLAN-Access-Points. Erweiterte Komponenten könnten Intrusion-Detection- oder Intrusion-Prevention-Systeme sein (IDS/IPS).
- Virtualisierungs-Ebene: Sollten virtualisierte Komponenten zum Einsatz kommen, muss die Virtualisierungsmanagement-Software geeignet konfiguriert und gehärtet werden. Es muss ebenfalls überprüft werden, ob durch die Virtualisierung ein für das Projekt angemessenes Sicherheitsniveau erreicht werden kann.
- Betriebssystemebene & Applikationsebene: Neben der eigentlichen Anwendungen zählen hierzu auch verwendete Bibliotheken, Erweiterungen, Laufzeitumgebungen, Server-Komponenten (zum Beispiel Web-Server) und Middleware-Komponenten. Hierbei muss der Betrieb aktueller und sicherer Software genauso sichergestellt werden wie die sichere Konfiguration aller Komponenten (zum Beispiel Web-Server-Konfiguration), im Allgemeinen spricht man von der System-Härtung. Ebenfalls in diese Kategorie gehören erweiterte Sicherheitskomponenten wie Application-Level Firewalls.

Weitere Themen, die das Projekt für jeweils alle technischen Ebenen beinhalten muss, sind

- Rollen und Berechtigungen
- Monitoring und Logging (etwa Systemverhalten, Login- und Zugriffsmuster)
- Anmeldemethoden für ein angemessenes Sicherheitsniveau (zum Beispiel Passwort-Authentifizierung, Zwei-Faktor-Authentifizierung)
- Verschlüsselungskonzept: Es ist zu klären, ob für ein angemessenes Sicherheitsniveau ein Verschlüsselungskonzept notwendig ist, etwa durch die Nutzung von Datenbank-, Datei-, Festplatten- oder E-Mail-Verschlüsselungslösungen.
- Betriebssicherheit und Ausfallsicherheit
- Zugangsschutz / Zutrittsschutz bei physischem Zutritt zu IT-Systemen

Eigenentwicklungen (Secure Programming)

- Bei Eigenentwicklungen, unabhängig davon ob diese Inhouse stattfinden oder beauftragt werden, müssen zusätzlich Maßnahmen ergriffen werden, die ein „Secure Programming“ sicherstellen. Dazu

sollte man auf die zuvor genannten Sicherheitsstandards zurückgreifen. Die Anforderungen, die sich hier ergeben, sind stark abhängig vom jeweiligen Entwicklungskontext und der gewählten Programmierumgebung. So unterscheiden sich beispielsweise die Sicherheitsanforderungen an Windows-Programme, mobile Apps, Web-Anwendungen oder ABAP-Anwendungen für SAP im Vergleich erheblich. Selbst bei mobilen Apps alleine muss man abhängig von den unterschiedlichen mobilen Betriebssystemen verschiedene Sicherheitskonzepte vorsehen (zum Beispiel für iOS, Android oder Windows).

- Es können auch branchenspezifische Sicherheitsanforderungen existieren, etwa PCI-PA-DSS für Kreditkarten-Applikationen. Bei Web-basierten Anwendungen können die allgemeinen Standards des zuvor genannten OWASP herangezogen werden.

Projektidee und Projektentwicklung

- Nach der Entstehung der Projekt- oder Produktidee werden erste Entwürfe mit IT-Sicherheitsspezialisten und Datenschutzspezialisten diskutiert.
- Anforderungen und Anmerkungen der Spezialisten werden aufgenommen und im Projektteam vorgestellt. Daraus entstehende Fragen und abgeänderte Realisierungsideen werden gegebenenfalls mit den Spezialisten erneut diskutiert.

Projekt-Kick-Off

- Zum Projekt-Kick-Off werden alle Projektbeteiligten geladen inklusive der Sicherheits- und Datenschutzspezialisten. Im Idealfall dienen die Spezialisten dem Projektteam als direkt oder zumindest als indirekte Ansprechpartner über den gesamten Projektzeitraum.

Definieren des Sicherheitskonzeptes

- Sind Sie Teil eines großen Unternehmens mit etabliertem IT-Sicherheitsprozess, dann werden Sie bereits die Sicherheitsanforderungen für IT-Projekte kennen. In der Regel muss für jedes IT-Projekt ein passender Katalog an Anforderungen zusammengestellt werden, da sich IT-Projekte in Art und Inhalt stark unterscheiden und daher nicht alle Anforderungen für alle Projekte gelten. Auch können Projekte aufgrund ihrer Thematik neue Anforderungen notwendig machen, etwa um gesetzliche Auflagen zu erfüllen.
- Haben Sie keine vorgegebenen Sicherheitsanforderungen, müssen Sie selbst einen Anforderungskatalog erstellen oder durch externe Hilfe erstellen lassen. Dabei ist es ratsam, die Rolle des Sicherheitsspezialisten von der ausführenden Rolle zu trennen. Es macht zum Beispiel keinen Sinn, eine Web-Agentur ihre selbst-definierten Sicherheitsanforderungen kontrollieren zu lassen. Dies ist für die Agentur intern natürlich sinnvoll, aber für Sie als Abnehmer einer Dienstleistung keineswegs. Beachten Sie, dass in der Regel ein externer Sicherheitsspezialist den kleinsten Anteil an Ihrem Gesamtprojektbudget haben wird. Definieren Sie den Katalog an Sicherheitsanforderungen selbst, können Sie sich an einem der zuvor genannten etablierten Sicherheitsstandards orientieren oder sich auf diesen beziehen. Je nach Projektumfang kann eine bestimmte Untermenge sinnvoll sein. Alternativ können Sie auch nach weiteren, in Ihrer Branche etablierten Sicherheitsstandards suchen.
- Als kleineres Unternehmen beispielsweise, dass sich von einer Web-Agentur einen Web-Shop realisieren lässt, sollte die zuvor genannte „OWASP Top Ten“ als Mindestanforderung in den Vertrag aufnehmen. Dazu kommen Fragen nach der Sicherheit beim Web-Hosting: Hostet die Agentur selbst oder wird dafür ein etablierter Dienstleister genutzt? Wer setzt das Patch-Management um (Betriebssystemebene, Applikationsebene)?

Externe Dienstleister

- Werden externe Dienstleister für das Projekt eingebunden, zum Beispiel für Hosting, Aufbau, Installation, Software-Entwicklung oder Lieferung von Standard-Software, werden diese auch auf IT-Sicherheit vertraglich verpflichtet. In der Ausgestaltung der Verträge sollten gewisse Mindestanforderungen konkret spezifiziert werden. Sollten Sicherheitslücken nach Inbetriebnahme auftreten, muss – gegebenenfalls unter Berücksichtigung zusätzlicher Kosten – ein entsprechendes Bugfixing vorgesehen werden. Sollte etwa gelieferte Software schon bei Abnahme gegen die vereinbarten Sicherheitskriterien verstoßen, sollte eine für den Auftraggeber kostenfreie Behebung der Sicherheitslücken vorgesehen sein.

Technische Abnahme

- Egal ob selbst-entwickelt oder geliefert durch externe Dienstleister, jedes Projekt muss abgenommen werden. Neben der funktionalen Abnahme ist die technische Sicherheitsabnahme ein Muss in jedem IT-Projekt. Hierzu zählt mindestens die stichprobenartige Überprüfung von Versionsständen, um zum Beispiel veraltete Software zu identifizieren und gegebenenfalls daraus sogar die grundsätzliche Qualität der abgelieferten Leistung einzuschätzen. Im Idealfall dient zur Abnahme ein echter Penetrationstest. Dieser kann im übrigen nicht nur bei Web-basierten Applikationen erfolgen, in entsprechend angepasster Form gibt es auch Sicherheitstests für Desktop-Anwendungen, mobile Apps und Server-Dienste wie Mail-Server.
- Die Abnahme bezieht sich stets auf die zuvor vereinbarten Sicherheitsanforderungen. Was nicht vereinbart wurde, kann auch nicht eingefordert werden oder verursacht Mehrkosten.

Laufende Sicherheitsprozesse

Als grober Überblick über die gängigen Sicherheitsprozesse im operativen Bereich von IT-Systemen soll folgende Aufstellung dienen:

- Patch-Management: Für alle verwendeten Komponenten des Gesamtsystems müssen Patchstände überwacht und aktualisiert werden sofern dies Sicherheitsrelevanz besitzt. Dazu zählen zum Beispiel: Firewalls, Betriebssysteme, Middleware-Komponenten, Web-Server, Application-Server, Runtimes, Anwendungen allgemein.
- Regelmäßiger Penetrationstests: Aufgrund sich ändernder Gefahrenlagen und neuer Angriffe sollte ein regelmäßiger Penetrationstest Teil des Betriebs sein. Die Häufigkeit hängt vom jeweiligen Projekt ab, empfehlenswert ist jedoch einmal jährlich. Es empfiehlt sich dabei, den ausführenden Penetrationstester in gewissen Intervallen zu wechseln, um monotones Testverhalten zu meiden. Für Nachtests ist es selbstverständlich zeit- und kosteneffizient, den gleichen Penetrationstester zu beauftragen.
- Monitoring von sicherheitsrelevanten Zugriffen: Operative Zugriffe wie Administrator-Aktionen sowie Logs von Sicherheitskomponenten wie Intrusion-Detection-Systemen, Application-Level Firewalls oder ähnlichem müssen regelmäßig gesichtet werden. Sicherheitskritische Ereignisse müssen an geeignetes Personal geleitet und von diesen bearbeitet werden.
- Monitoring von applikativen Zugriffen gegen Missbrauch: Datenzugriffe, etwa auf Kundendaten, durch Mitarbeiter müssen auditierbar sein, aber auch bei konkreten aktuellen Verdachtsfällen zeitnah erkannt werden. Daher müssen eingerichtete Zugriffskontrollen auf Applikationsebene in einem für das Projekt sinnvollen Prozess überprüfbar gemacht werden.

Betriebssicherheit

- Falls Sie Maßnahmen zur Ausfallsicherheit und Hochverfügbarkeit benötigen, werden Sie in der Regel einen weiteren Spezialisten im administrativen Bereich benötigen. Zumindest sollte im Projekt

definiert sein, wo die maximal tolerierbaren Ausfallzeiten für die verwendeten IT-Systeme liegen. Sind Vertragspartner für diese Fälle vorgesehen, müssen diese vertraglich auf die entsprechenden Wiederherstellungsprozesse und Service Level Agreements verpflichtet werden.

- Ein weiteres, zentrales Thema der Betriebssicherheit ist Backup & Wiederherstellung. Dazu zählen insbesondere alle sich ändernden (Nutzer-)Daten aus Datenbanken, NAS und sonstigen Speicherorten. Auch wenn es aufwendig ist, das korrekte Funktionieren eines Backups kann nur getestet werden, in dem eine Wiederherstellung auf einem nicht-installierten System versucht wird. Nur so kann man sicherstellen, für den Ernstfall vorbereitet zu sein. Wenngleich man diesen Prozess nicht regelmäßig durchführen möchte, sollte er zumindest einmalig vor dem Go-Live durchgeführt werden.

Fazit

IT-Sicherheit ist ein komplexes Unterfangen. Selbst erfahrenste Projektleiter können dieses Thema nicht alleine stemmen und benötigen fachliche Unterstützung. In kleinen Unternehmen kann die Budgetknappheit die Notwendigkeit ergeben, das Thema Sicherheit selbst stemmen zu müssen. Hier können Sicherheitsstandards helfen, um Lieferanten und Partner entsprechend zu steuern. Dabei müssen die genannten zentralen Themen berücksichtigt werden. Im Allgemeinen müssen jedoch unbedingt für das jeweilige Projekt entsprechend passende Anforderungen definiert werden.

IT-Projekte aller Größen müssen den Grundsatz beachten, schon in der Frühphase der Entstehung IT-Sicherheit und Datenschutzanforderungen in das Projekt zu integrieren. Versäumnisse in diesem Bereich können Projekte scheitern lassen oder zumindest zu hohen Folgekosten führen.