Sicherheit im Projektmanagement

Veröffentlicht am 24. Juli 2024

Ihre Ansprechpersonen: Barbara Moser

Tags: Fachbeiträge, Banken und Versicherungen, Energie und Infrastruktur, Gesundheitswesen, Handel, Transport und Logistik, Industrie, Technologie und Dienstleistung, Öffentliche Verwaltung, Digitalisierung in KMU, Projektmanagement

Wie die Statistiken des Bundesamtes für Cybersicherheit (BACS) zeigen, gingen in den letzten 12 Monaten wöchentlich zwischen 526 und 2’490 Meldungen von der Bevölkerung und von Unternehmen zu Cybervorfällen ein. Neue Schwachstellen, Ransomware-Angriffe sowie bspw. DDoS-Attacken sind regelmässig Gegenstand von Medienmitteilungen.

Die Entwicklung neuer Technologien sowie die zunehmende Digitalisierung und Vernetzung verstärken die Exposition gegenüber Cyberbedrohungen.

Neue Informatikmittel werden oft im Rahmen eines Projektes konzipiert, realisiert und eingeführt. Doch welche Bedeutung haben Informationssicherheit, Datenschutz, IT-Sicherheit und Cybersicherheit im Kontext des klassischen Projektmanagements?

Bevor wir uns der Beantwortung dieser Frage widmen, wird nachfolgend kurz auf die verschiedenen Begrifflichkeiten eingegangen.

Informationssicherheit

Gegenstand der Informationssicherheit ist eine sichere Bearbeitung von Informationen (Datensicherheit) im Kontext der Geschäftsprozesse und der sichere Einsatz der dazu benötigten Informatikmittel. Die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sowie deren Nachvollziehbarkeit im Falle der Bearbeitung muss entsprechend ihrem Schutzbedarf sichergestellt werden.

Die Risiken für die Informationssicherheit sind kontinuierlich zu identifizieren, zu bewerten und mit entsprechenden Massnahmen zu minimieren. Die Informationssicherheit umfasst sowohl technische, organisatorische, personelle wie auch physische Massnahmen zum Schutz der Informationen sowie Informatikmittel.

Auf Stufe Bund dient bspw. das Informationssicherheitsgesetz (ISG) sowie die Informationssicherheitsverordnung (ISV) der Gewährleistung der Informationssicherheit.

Datenschutz

Ziel des Datenschutzes ist der Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden. Der Schutz gilt somit der betroffenen Person. Dies im Gegensatz zur Informationssicherheit, wo es um den Schutz von Informationen und Informatikmittel im Allgemeinen geht.

Unter Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen zu verstehen. Das Bearbeiten von Personendaten schliesst insbesondere deren Beschaffung, Speicherung, Aufbewahrung, Verwendung, Veränderung und Bekanntgabe mit ein. Auch hier gilt es die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Personendaten mittels technischen und organisatorischen Massnahahmen entsprechend ihrem Schutzbedarf sicherzustellen.

Gesetzlich wird dies im Datenschutzgesetz (DSG) sowie in der Datenschutzverordnung (DSV) geregelt.

IT-Sicherheit

Der Fokus der IT-Sicherheit liegt auf den technischen Massnahmen zum Schutz der Informatikmittel und den damit verarbeiteten elektronischen Informationen. Unter Informatikmittel sind unter anderem folgende Komponenten zu verstehen:

- Hardware (bspw. Server, Storage und Endgeräte)
- Software (bspw. Betriebssysteme und Anwendungen)
- Netzwerkkomponenten (bspw. Router und Switches)

Technische Massnahmen können bspw. Netzwerksegmentierungen, Firewalls, Systemhärtung, Patches sowie Back-ups sein.

Cybersicherheit

Die Cybersicherheit kann als eine Erweiterung der IT-Sicherheit betrachtet werden. Die Bedrohung ergibt sich aufgrund der digitalen Vernetzung bzw. der Nutzung des Internets. Durch präventive (bspw. Schwachstellenscans) und detektive (bspw. Network Detection & Response Lösungen) Massnahmen sowie Sensibilisierung der Mitarbeitenden gegenüber Cyberbedrohungen, können Schwachstellen beseitigt und so die Informatikmittel und die damit verarbeiteten elektronischen Informationen vor Cybervorfällen geschützt werden.

Durch einen Cybervorfall wird die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von Informationen beeinträchtigt. Wird der Cybervorfall absichtlich ausgelöst, spricht man von einem Cyberangriff. Die Widerstandsfähigkeit der Schweiz gegenüber Cyberbedrohungen soll durch das neue Informationssicherheitsgesetz (ISG) erhöht werden.

Bedeutung für das klassische Projektmanagement

Was bedeutet dies nun konkret für das klassische Projektmanagement bei der Einführung neuer Informatikmittel?

Bereits während der Projektphasen ist die Berücksichtigung dieser Themen unerlässlich. Nachfolgend werden je HERMES Phase (Projektmanagementmethode des Bundes) einige Beispiele erläutert, inwiefern Informationssicherheit, Datenschutz sowie IT- und Cybersicherheit Anklang finden sollten.

Die Integration der Informationssicherheit ins Projektmanagement wird bspw. im Rahmen der ISO-Norm 27001:2022 explizit erwähnt (Anhang A, organisatorische Kontrolle 5.8). Einige Beispiele beziehen sich auf die Projektmanagementmethodik an sich, andere auf die einzuführenden Informatikmittel.

Während der Phase Initialisierung

Schutzbedarfsanalyse erarbeiten

Im Rahmen der Schutzbedarfsanalyse (SCHUBAN) sind die Anforderungen des Schutzobjektes an die Vertraulichkeit, Verfügbarkeit, Integrität sowie Nachvollziehbarkeit der Informationen (Daten) zu erheben.

Ebenso zum Zeitpunkt der SCHUBAN ist durch Bundesorgane neu die Risikovorprüfung vorzunehmen. Mittels dieses Instrumentes soll bestimmt werden, ob die geplante Bearbeitung von Personendaten ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen kann. Bei einem hohen Risiko

muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden.

Projektmanagementplan erarbeiten

Im Rahmen des Projektmanagementplans ist Bezug auf das Daten- und Dokumentenmanagement während des Projektes zu nehmen. Folgende Punkte sollten u.a. adressiert werden:

- Klassifizierung von Daten/Dokumenten (INTERN, VERTRAULICH und GEHEIM) gemäss Art. 13 ISG
- Sicherstellung, dass Informationen entsprechend ihrem Schutzbedarf nur Berechtigten zugänglich gemacht werden (Art 6. Abs. 2 Bst. a ISG). Für VERTRAULICH oder höher klassifizierte Daten/Dokumente ist bspw. eine geeignete Verschlüsselungssoftware einzusetzen.
- Etablierung regelmässiger Überprüfungen des Kreises der Berechtigten auf Daten- und Dokumentenablagen

Des Weiteren ist im Projektmanagementplan vorzugeben, ob für Projektmitarbeitende eine Grundsicherheitsprüfung oder eine erweiterte Personensicherheitsprüfung gemäss Art. 30 ISG erforderlich ist.

Ebenso ist zu definieren, ob durch die Projektmitarbeitenden eine Geheimhaltungserklärung unterschrieben werden muss.

Während der Phase Konzept

Lösungsanforderungen / Lösungsarchitektur erarbeiten

Bei der Erarbeitung der Lösungsanforderungen sind bspw. Vorgaben an Datenschutz und Informationssicherheit, an IKT-Grundschutz sowie spezifische Anforderungen an Georedundanz, Netzwerksegmentierung, Systemhärtung, Air Gap geschützte Umgebungen, Kryptografie, digitale Zertifikate oder Privilege Access Management (PAM) zu berücksichtigen. Die erhobenen Anforderungen sind bei der Erarbeitung der Lösungsarchitektur zu berücksichtigen.

Betriebssicherheitsverfahren durchführen

Bei öffentlichen Aufträgen mit sicherheitsempfindlichen Tätigkeiten ist die Einleitung eines Betriebssicherheitsverfahren zu beantragen (Art. 52 Abs. 1 ISG).

Ausschreibung / Vereinbarung erarbeiten

Die erarbeiteten Lösungsanforderungen müssen bei der Ausschreibung einfliessen. Nicht zu vergessen sind die Anforderungen an Datenschutz und Informationssicherheit. Diese sollten anschliessend auch in den Verträgen mit externen Lieferanten aufgenommen werden. So kann bspw. für den Lieferanten eine umgehende Meldepflicht im Falle eines Cybervorfalls vorgesehen werden.

ISDS-Konzept erarbeiten

Innerhalb der Bundesverwaltung ist für jedes Informatikschutzobjekt der IKT-Grundschutz zu erarbeiten. Er legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich fest. Ergab die SCHUBAN einen erhöhten Schutzbedarf ist zudem ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) inklusive Risikoanalyse zu erarbeiten. Im ISDS-Konzept sind auch die Zugriffsberechtigungen zu thematisieren. Alternativ kann ein separates Berechtigungskonzept erstellt werden.

Des Weiteren ist zu prüfen, ob ein Bearbeitungsreglement erstellt werden muss (Art. 6 DSV). Bei automatisierten Bearbeitungen muss dies bspw. erstellt werden, wenn besonders schützenswerte Personendaten bearbeitet werden, ein Profiling durchgeführt wird oder Datenbestände miteinander verknüpft werden (bspw. über mehrere Verwaltungseinheiten).

Im Kontext des Business Continuity Managements (BCM) ist zudem zu prüfen, ob ein Notfallkonzept erstellt werden muss.

Während der Phase Realisierung

ISDS-Konzept realisieren

Die im ISDS-Konzept definierten Schutzmassnahmen sind umzusetzen. Im Rahmen der Vorabnahme sind diese zu überprüfen.

System realisieren

Im Rahmen der Realisierung des Informatikmittels nicht umgesetzte Sicherheitsanforderungen können zu Schwachstellen führen.

Systemintegration vorbereiten

Im Rahmen der Anbindung der Umsysteme sollen nur die effektiv erforderlichen Firewall Regeln umgesetzt werden.

Das einzuführende Informatikmittel ist an das bestehende Sicherheits-Monitoring anzubinden (bspw. an eine SIEM-Lösung).

Entscheid Vorabnahme treffen

Vor dem Entscheid zur Betriebsaufnahme sollte ein Schwachstellenscan und Penetrationstest durchgeführt werden. Im Rahmen eines Schwachstellenscans werden Informatikmittel meist automatisiert auf Schwachstellen untersucht. Ein Penetrationstest geht noch einen Schritt weiter. Es wird ein Cyberangriff simuliert und gezielt versucht, Schwachstellen auszunutzen. Oft ist es eine Kombination aus automatisierten und manuellen Massnahmen. Als kritisch eingestufte Schwachstellen müssen vor dem go live behoben werden. Schwachstellen, welche akzeptiert werden, müssen als Risiko im ISDS-Konzept ausgewiesen werden.

Während der Phase Einführung

Einführungsmassnahmen durchführen

Bei Bedarf sind im Rahmen der Einführung Sensibilisierungsmassnahmen vorzusehen, um das Bewusstsein der Betriebs- und Anwendungsorganisation für die Informationssicherheit, den Datenschutz sowie die IT- und Cybersicherheit zu stärken.

ISDS-Konzept überführen

Vor dem Entscheid zur Betriebsaufnahme ist das ISDS-Konzept bzw. sämtliche Sicherheitsdokumente in die Stammorganisation zu überführen. Die Sicherheitsdokumente müssen während der Nutzungsphase der Informatikmittel stets aktuell gehalten werden. Bei sicherheitsrelevanten Änderungen muss eine Überarbeitung der Sicherheitsdokumentation, insbesondere eine Neubeurteilung der Risiken erfolgen.

Während der Phase Abschluss

Die Projektorganisation wird aufgelöst. Die Betriebs- und Anwendungsorganisation übernimmt. Es ist sicherzustellen, dass die Informatikmittel während der Nutzungsphase regelmässig gewartet werden und Back-ups von Daten und Konfigurationen erstellt werden. In letzterem Fall sollte auch das Restoring getestet werden.

Viele dieser Beispiele decken sich mit den organisatorischen, personellen, physischen und technischen Informationssicherheitskontrollen aus Anhang A der ISO-Norm 27001:2022 - Informationssicherheitsmanagementsystem.

Möchten Sie mehr über dieses spannende Thema erfahren oder wissen, wie die APP auch Sie bei einem herausfordernden Vorhaben unterstützen kann? Wir freuen uns auf Ihre Kontaktaufnahme.

Hilfreiche Links

- Datenschutzgesetz (DSG)
- Datenschutzverordnung (DSV)
- Informationssicherheitsgesetz (ISG)
- Änderung Informationssicherheitsgesetz (ISG) (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen)
- Informationssicherheitsverordnung (ISV)