Cybersecurity im Lifecycle von Anwendungen

Veröffentlicht am 27. August 2020

Ihre Ansprechpersonen: Jana Papritz

Tags: Erfolgsgeschichten, Banken und Versicherungen, Öffentliche Verwaltung, Projektmanagement, Prozessoptimierung und -management, Schulung und Training, Strategieberatung

Die Informationssicherheit und der Datenschutz müssen über den ganzen Lifecycle einer Anwendung aufrechterhalten werden. Dazu müssen Projektleiter, ISDS- und Anwendungsverantwortliche ihre Aufgaben, Kompetenzen und Verantwortung genaustens kennen. Mit einer ersten Veranstaltung innerhalb der Awareness Kampagne im BLV hat die Leitung Informatik gemeinsam mit dem Informationssicherheitsbeauftragten und der APP einen ersten Schritt in diese Richtung getätigt.

Aber warum gerade Projektleiter, ISDS- und rtliche?



Zu Beginn des Lifecycles einer Anwendung

– in der Initialisierungs- und Konzeptphase - entstehen eine Reihe von ISDS-Dokumenten, welche

keineswegs als Papiertiger im Archiv landen dürfen, sondern als Grundlage für die Umsetzung von Schutzmassnahmen im weiteren Verlauf des Projekts dienen sollen. Aktuelle Erkenntnisse müssen in geeigneter Form laufend in der ISDS-Dokumentation geführt werden. Die Verantwortung für diese Dokumente trägt der Projektleiter gemeinsam mit dem ISDS-Verantwortlichen.

Werden im Verlauf des Betriebs – bei Releasewechseln, Changes, Betreiberwechsel und Weiterentwicklungsprojekten - Änderungen an Anwendungen realisiert, müssen die Sicherheitsanforderung überprüft und Schutzmassnahmen davon abgeleitet, umgesetzt und dokumentiert werden. Dafür verantwortlich ist der Anwendungsverantwortliche.

Organisatorische Massnahmen

Hilfreich dabei ist eine stabile, gut dokumentierte Prozesslandschaft und eine funktionierende Organisation. Die Schnittstellen zwischen der Stammorganisation und der Projekt- und Betriebsorganisation müssen zwangsläufig funktionieren.

So muss ein Sicherheitsvorfall zeitnah bei der richtigen Stelle gemeldet und von den Verantwortlichen bearbeitet werden können. Wird bei einer Anwendung ein Betreiberwechsel vorgenommen, müssen die richtigen Ansprechpersonen – darunter im Minimum der Informationssicherheitsbeauftragte – hinzugezogen werden.

Massnahmen zur Wahrung der Informationssicherheit und des Datenschutzes sind somit keinesfalls nur technischer Natur – Gefahren und Risiken muss man interdisziplinär entgegenwirken. Mit Hilfe von Awareness Kampagnen lassen sich gezielt auch Nicht-Informatiker zum Thema Informationssicherheit und Datenschutz sensibilisieren. Damit können alle Mitarbeiter im Unternehmen bzw. der Organisation ihren Beitrag leisten.
Mit der ersten Veranstaltung konnte das BLV Wissenslücken – insbesondere bei den Anwendungsverantwortlichen aus den Fachbereichen – schliessen. Mit dem Feedback der Mitarbeiter konnten prozessuale und organisatorische Mängel behoben und das Informationssicherheitsmanagement weiter professionalisiert werden.

Mittels gelebten Prozessen, einer funktionierenden Organisation und den dazu eingeleiteten Schulungsmassnahmen ist es möglich, den Papiertiger zum Leben zu erwecken!

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.