Informationssicherheit

Informationssicherheit ist ein kontinuierlicher Prozess

Die heutigen Technologien bieten die Möglichkeit, Dienstleistungen rund um die Uhr anzubieten und zu nutzen. Wer von den Chancen der Digitalisierung nachhaltig profitieren will, muss die Risiken kontinuierlich bewerten und Sicherheitsvorkehrungen treffen.

Die Grundprinzipien des Datenschutzes und der Informationssicherheit, nämlich Vertraulichkeit, Verfügbarkeit und Integrität müssen jederzeit gewährleistet sein. Dafür müssen alle Funktions- und Managementstufen die auf die Sicherheit ausgerichteten Vorgaben und Prozesse erkennen und umsetzen.

Informationssicherheitskonzepte

Die Vorgaben und Richtlinien für eine integrale Informationssicherheit müssen auf der strategischen, taktischen und operativen Ebene erstellt und umgesetzt werden. Die Dokumente reichen von der Leitlinie zur Informationssicherheit über das Informationskonzept bis zu den Checklisten und Verträgen. Der Datenschutzbeauftragte stellt auf seiner Website eine Übersicht der Dokumente sowie weitere Vorlagen zur Verfügung.

Der Schutz der Privatsphäre als Standard in der Planung

Mit Privacy by Design werden der Datenschutz und der Schutz der Privatsphäre als Teil des Konzepts bereits bei der Planung konsequent beachtet, während bei Privacy by Default darauf geachtet wird, dass standardmässig die höchste Stufe des Schutzes der Privatsphäre gewählt wird. Diese beiden Ansätze gewährleisten den Datenschutz und die Informationssicherheit während der Umsetzung eines Vorhabens oder Projekts.

Sicherheit von Websites

Ein unsachgemässer Aufbau oder Betrieb einer Website kann zu Verletzungen von Datenschutz- oder Geheimhaltungsvorschriften führen. Daher müssen bestimmte Sicherheitsmassnahmen umgesetzt und periodisch kontrolliert werden.

Awareness und Sensibilisierung

Auch wenn die Sicherheitsmassnahmen implementiert, regelmässig kontrolliert und in einem geregelten Risikomanagementprozess überprüft werden, so bearbeiten letztendlich die Mitarbeitenden die Informationen. Sie sind oft das Ziel von Spam-, Phishing- und Social-Engineering-Attacken. Die Sensibilisierung der Mitarbeitenden reduziert diese Risiken.

Informationssicherheit ist ein kontinuierlicher Prozess, an dem sämtliche Funktionen und Mitarbeitenden beteiligt sein müssen. Nur so kann die Digitalisierung erfolgreich, sicher und zukunftsgerichtet umgesetzt werden.

Beispielhafte Informationssicherheit

Im Rahmen einer Beratung beurteilte der Datenschutzbeauftragte die Dokumente zur Informationssicherheit sowie die Notfallbetriebsplanung einer Hochschule. Der Datenschutzbeauftragte kam zum Schluss, dass die geprüften Dokumente eine gute Ausganglage für eine umfassende Informationssicherheit bilden.

In der Leitlinie für die Informationssicherheitsziele definierte die Hochschule die angestrebte Sicherheitskultur, Klassifizierungskriterien sowie die Sicherheitsorganisation. Die wichtigsten Verantwortlichkeiten und Aufgaben für die wichtigsten Rollen wurden wie folgt definiert:

Hochschulleitung

- Gesamte Verantwortung für Informationssicherheit und Datenschutz
- Genehmigt die Informationssicherheitsstrategie und die Ressourcen
- Abnahme der Risiken und des jährlichen Sicherheitsberichts

Informationssicherheitsausschuss

- Zuständig für die normative Informationssicherheit
- Entscheidet über Sicherheitsmassnahmen
- Bereitet den jährlichen Sicherheitsbericht für die Hochschulleitung vor
- Mitglieder sind die Verwaltungsdirektorin oder der Verwaltungsdirektor, die Datenschutzverantwortlichen und die Informationssicherheits-Verantwortlichen

Informationssicherheits-Verantwortliche

- Verantwortlich für die operative Informationssicherheit
- Zentrale Ansprechstelle für sämtliche Fragen der Informationssicherheit
- Beraten und schulen die Mitarbeitenden in sämtlichen Fragen der Informationssicherheit
- Begleiten und kontrollieren die Projekte sowie den Betrieb bei der korrekten Umsetzung und bei der Einhaltung der Sicherheitsmassnahmen
- Bei Sicherheitsvorfällen zuständig für die Information und die Eskalation an den Informationssicherheitsausschuss

Anwendungs- und Systemverantwortliche

- Gewährleisten die Sicherheit der in ihrer Verantwortung liegenden Werte der Hochschule
- Stellen die nötigen Sicherheitsmassnahmen auf der Basis anerkannter Standards wie ISO 27002 oder der Bausteine des BSI sicher
- Kontrollieren die Einhaltung und Umsetzung der Konzepte Privacy by Default und Privacy by Design

Termineinladungen mit E-Mail oder SMS

Ein Spital plante, den Patientinnen und Patienten die Termineinladung per E-Mail und die Erinnerung per SMS zu verschicken, und bat den Datenschutzbeauftragten, das Vorhaben aus datenschutzrechtlicher Sicht zu beurteilen.

Der vorgesehene Inhalt der elektronischen Mitteilungen umfasste die Datumsangaben des Termins, die medizinischen Vorbereitungen wie «nüchtern» oder «mit voller Blase», Informationen zur Behandlung oder zur Untersuchung wie die Aufklärung über die Gefahren einer Darmspiegelung sowie einen Fragebogen und einen personifizierten Link zur Einverständniserklärung für die Behandlung.

Der Datenschutzbeauftragte stellte fest, bereits die Tatsache, dass sich eine Person bei einem Spital in medizinischer Behandlung befindet, falle unter die ärztliche Schweigepflicht. Für eine Termineinladung und -erinnerung per E-Mail oder SMS muss die Patientin oder der Patient deshalb in die Aufhebung der Schweigepflicht einwilligen (sogenanntes Opt-in). Die Wahlmöglichkeit zwischen der herkömmlichen Einladung und Erinnerung per Post und der digitalen Kontaktaufnahme muss weiterhin bestehen.

Entscheidet sich eine Patientin oder ein Patient für die digitale Kommunikation mit dem Spital, so wäre ein möglicher datenschutzkonformer Ansatz, Statusmeldungen per SMS oder E-Mail zu verschicken und die eigentlichen Informationen über eine geschützte Website anzubieten. Vor dem Zugang zur Information müsste sich die Patientin oder der Patient eindeutig identifizieren. Beim Aufbau einer solchen Lösung sind die Sicherheitsmassnahmen durch eine Risikoanalyse, die anerkannten Standards und die Best Practices zu definieren, um Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit und Authentizität zu gewährleisten. Informationen, die Rückschlüsse auf die Gesundheit einer Person zulassen, müssen grundsätzlich mit starker Verschlüsselung und Zwei-Faktor-Authentifizierung geschützt werden.

Webchecks decken Schwachstellen auf

Im Jahr 2017 hat der Datenschutzbeauftragte zahlreiche Sicherheitsüberprüfungen von Websites öffentlicher Organe, sogenannte Webchecks, durchgeführt.

Dabei werden die Websites mit Programmen gezielt auf bekannte Sicherheitslücken und Schwachstellen durchleuchtet. Komplexe Schwachstellen überprüft der Datenschutzbeauftragte zusätzlich manuell.

Die Liste der Schwachstellen, die durch die Webchecks gefunden wurden, deckt sich weitgehend mit der Schwachstellen-Top-10 des Open Web Application Security Project (OWASP).

So speicherten drei der geprüften Websites die Passwörter im Klartext – eine Schwachstelle mit grossem Missbrauchspotenzial. Moderne Anwendungen speichern Passwörter immer in verschlüsselter Form.

In zwei weiteren Fällen wurden Schwachstellen gefunden, die es Angreifern ermöglichen, eigene Befehle in die SQL-Datenbank einzuschleusen. Mit einer sogenannten SQL Injection können die gespeicherten Daten ausgespäht und verändert werden. Angreifer können selbst die Kontrolle über den Server übernehmen.

Der Datenschutzbeauftragte forderte die Website-Betreiber auf, diese gravierenden Sicherheitslücken umgehend zu schliessen.

Sensibilisierungs-veranstaltung für Mitarbeitende

Ein öffentliches Organ wollte seine Mitarbeitenden für Fragen der Informationssicherheit sensibilisieren und bat den Datenschutzbeauftragten um Unterstützung. Er bot eine einstündige Schulung vor Ort an, während der die Teilnehmerinnen und Teilnehmer die Risiken, Gefahren und möglichen Massnahmen interaktiv erarbeiteten.

Nachdem die Bedeutung des Schutzes der Persönlichkeit und der Privatsphäre erklärt worden war, lernten die Teilnehmenden konkrete Strategien und Hilfsmittel kennen, welche die Informationssicherheit im Alltag verbessern.

Vorgestellt wurden:

- Möglichkeiten der sicheren Datenübermittlung mit IncaMail oder WebTransfer ZH
- Hilfsmittel für den Umgang mit Passwörtern wie der Passwortcheck oder verschiedene Passwortmanager
- Sicherheitsvorkehrungen für Smartphones und mobile Geräte