Cyber Security Strategie der gibb

Studiengang: MAS Cyber Security

Aufgrund der zunehmenden Bedrohungen im Cyber-Bereich, benötigt die gibb eine solid aufgebaute Cyber-Sicherheitsorganisation, welche den aktuellen Bedrohungen gewachsen und organisatorisch verankert ist.

Ausgangslage

Die digitale Revolution hat die Art und Weise verändert, wie wir lernen und uns weiterbilden. Der Zugang zu neuen digitalen Lerninstrumenten und Remote-Zugriff ermöglicht es Bildungseinrichtungen, ihren Studierenden ein breiteres Angebot an Lehrinhalten anzubieten. Doch diese Entwicklungen bringen auch eine zunehmende Bedrohung durch Cyber-Kriminalität mit sich.
Die gibb, eine renommierte Bildungseinrichtung, ist sich dieser Gefahr bewusst und hat sich entschlossen, eine starke Cyber-Sicherheitsorganisation aufzubauen. Die neuen digitalen Lerninstrumente und die hochempfindlichen Studierendendaten machen die gibb zu einem Ziel für Hacker. In der Tat haben in den letzten Jahren zahlreiche Schweizer Hochschulen unter schweren Hackerangriffen gelitten, und die gibb war leider keine Ausnahme.
In dieser angespannten Situation muss die gibb den Bildungsbetrieb aufrechterhalten und gleichzeitig sicherstellen, dass die persönlichen Daten ihrer Studierenden geschützt sind. Darüber hinaus müssen auch die digitalen Lerninstrumente wie smartlearn abgesichert werden, um einen reibungslosen Betrieb zu gewährleisten.
Die gibb steht also vor einer enormen Herausforderung, die sie jedoch nicht alleine bewältigen kann. Eine Zusammenarbeit mit Experten auf dem Gebiet der Cyber-Security ist von entscheidender Bedeutung, um die Sicherheit der Studierenden und des Bildungsbetriebs zu gewährleisten.

Zielsetzung

Die gibb benötigt möglichst rasch eine funktionierende IT-Sicherheitsorganisation, um den aktuellen und zukünftigen Bedrohungen eine möglichst kleine Angriffsfläche zu bieten. Es müssen Prozesse erstellt werden, welche Verantwortlichkeiten definieren und einer klaren vorgegeben hierarchischen Linie folgen. Im Rahmen der neuen Sicherheitsorganisation möchte die gibb folgende Aufgabenpunkte mittelfristig organisatorisch und technisch klären:

- Analyse IST-Situation
- Verantwortlichkeiten und Kompetenzen in der gibb (Organisation) integrieren
- Erstellen Sicherheitsleitlinie (Information-Security Policy) und Sicherheitsstrategie
- Definieren von Massnahmen bei Sicherheitsrisiken
- Erstellen von regelmässigen Sicherheitsreports für die Führungs- und Leitungsebenen
- Weiterentwicklung der Sicherheit in der gibb (Organisation, System und Netzwerk)
- Security-Awareness
- CVE-Management

Lösungsansatz

Die gesamte Strategie ist auf vier Hauptphasen aufgeteilt. Phase 1 beinhaltet eine IST-Analyse auf organisatorischer und technischer Ebene. Hierbei wird unterteilt zwischen Prozesse & Organisation, Architektur & Technologie und dem Datenmanagement. Phase 1 ist initial die wichtigste Phase, da alle weiteren Handlungen sowie Empfehlungen auf dieser aufbauen.
Aufgrund der in Phase 1 (Audit) erarbeiteten Bewertungen, geht es in der zweiten Phase primär um die strategische Verankerung der IT-Security in der Organisation. Anhand der Erkenntnisse in Phase 1, ist die Tätigkeit in Phase 3, eine Leitlinie zur Informationssicherheit zu erstellen. Diese umfasst die Infrastruktur, Technologie, Kommunikation und rechtlichen Aspekte.
In der letzten Phase wird das SOLL-Bild dargestellt, mittels Umsetzungspläne von den zuvor definierten Massnahmen und Awareness-Kampagnen. Die fachliche Stärkung und ständige Weiterbildung der Mitarbeitenden spielt hier eine zentrale Rolle.
In den Handlungsempfehlungen ist eine Roadmap erstellt, welche eine Auflistung der noch durchzuführenden Arbeiten der IT und Direktion beschreibt.

Michael Arslan

michail.arslan@protonmail.ch