|  |  |
| --- | --- |
|  | **Kai Thiemrodt,**  **Diplomwirtschaftsingenieur**  **Senior** |

Kai Thiemrodt absolvierte den Diplomstudiengang „Wirtschaftsingenieurwesen“ mit den Schwerpunkten Elektrische Anlagentechnik, Logistik und Wirtschaftsrecht an der Helmut-Schmidt-Universität, Universität der Bundeswehr Hamburg.

Als ehemaliger Offizier der Bundeswehr verfügt Herr Thiemrodt über mehr als 15 Jahre Projekt- und Managementerfahrung durch unterschiedliche Führungspositionen in nationalen, sowohl militärischen als auch zivilen Einrichtungen des öffentlichen Dienstes, davon mehr als 8 Jahre Berufserfahrung im Bereich der Informationssicherheit.

Insbesondere durch seine Tätigkeit als Informationssicherheitsbeauftragter und Sachgebietsleiter IT-Service-Bereitstellung und Informationssicherheit eines Fähigkeitskommandos der Bundeswehr erwarb Herr Thiemrodt umfassende Kompetenzen in verschiedenen Bereichen der Informationstechnik. Hierzu zählen umfangreiche Fach- und Methodenkenntnisse in den Bereichen IT-Projekt- und IT-Security Accreditation Management, IT-Grundschutz, IT-Security Awareness sowie grundlegende Kenntnisse in den Bereichen Datenschutz nach DSGVO und Geheimschutz.

Durch seine langjährige Führungserfahrung im Bereich des öffentlichen Dienstes ist Herr Thiemrodt bestens mit der Aufbau- und Ablauforganisation der öffentlichen Verwaltung, der Stabsarbeit sowie der Konzept- und Grundlagenarbeit vertraut.

Derzeit ist Herr Thiemrodt als Berater im Bereich Cyber Security in Public Sector Projekten tätig, wobei er im Schwerpunkt für die Implementierung von Informationssicherheitsmanagementsystemen gemäß ISO 27001 auf Basis BSI IT-Grundschutz zuständig ist.

Während seiner bisherigen Laufbahn erwarb Kai Thiemrodt die folgenden Qualifikationen:

* Zertifizierter IT-Grundschutz-Berater (BSI)
* PRINCE2® Foundation Certificate in Project Management (AXELOS)
* PRINCE2® Practitioner Certificate in Project Management (AXELOS)
* ITIL Foundation Certificate in IT Service Management (AXELOS)
* Geprüfter Sicherheitsberater (PwC Cert)
* Geprüfter Datenschutzbeauftragter (PwC Cert)
* Geprüfter SAVe 6-Anwender (INFODAS)
* Zertifizierter Qualitätsmanager ISO 9001 (DAkkS)
* IT- und IT-Sicherheitsoffizier (Bundeswehr)

Neben Deutsch als Muttersprache beherrscht Herr Thiemrodt zudem English verhandlungssicher in Wort und Schrift.

Des Weiteren wurde Herr Thiemrodt im Rahmen seiner militärischen Laufbahn einer erweiterten Sicherheitsüberprüfung gemäß Sicherheitsüberprüfungsgesetz (Stufe Ü3) unterzogen.

**Ausgewählte Referenzprojekte**

|  |  |
| --- | --- |
| Mandant | Bayrisches Landesamt für Steuern |
| Rolle | Fachverantwortung |
| Aufgaben | * Beratung im Bereich Informationssicherheitsmanagement gemäß ISO 27001 auf Basis von BSI IT-Grundschutz. * Design, Implementierung und Dokumentation eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO 27001 auf Basis von BSI IT-Grundschutz * Erstellung von Informationssicherheitskonzepten verschiedener Fachverfahren gemäß BSI-Standard 200-2 und 200-3 unter der Zuhilfenahme des Grundschutz-Tools DocSetMinder, dazu Durchführung von   + Strukturanalysen   + Abgrenzungen von IT-Verbünden   + IT-Grundschutzchecks   + Risikoanalysen * Erstellen von Richtlinien zur Informationssicherheit * Unterstützung bei der Erstellung von Schulungsinhalten zu den Themen Informationssicherheit und IT-Security-Awareness |
| Zeitraum | seit 03/2021 |
| Dauer | 12 Monate |
| Aufwände | 200 Personentage |

|  |  |
| --- | --- |
| Mandant | Deutsche Börse |
| Rolle | Fachverantwortung |
| Aufgaben | * Beratung zur Aktualisierung der bestehenden Informationssicherheitsdokumentation * Unterstützung bei der Sicherstellung der IT-Compliance insbesondere hinsichtlich BAIT, MaRisk * Unterstützung bei der Erstellung von fehlenden Informationssicherheitsrichtlinien und -konzepten |
| Zeitraum | 11/2020 bis 03/2021 |
| Dauer | 5 Monate |
| Aufwände | 75 Personentage |

|  |  |
| --- | --- |
| Mandant | Unternehmensgruppe Gretsch-Unitas GmbH |
| Rolle | Fachverantwortung |
| Aufgaben | * Beratung und Unterstützung beim Aufbau eines Informationssicherheitsmanagementsystems gemäß ISO 27001 * Sichtung und Auswertung von Netzplänen und vorhandenen IT-Dokumentationen * Durchführung von Risikoanalysen nach BSI-Standard 200-3 und ISO 27005 * Identifikation, Einstufung und Bewertung von Gefährdungen für unterschiedliche Zielobjekte sowie Ableitung von erforderlichen Maßnahmen * Abstimmungen und Durchführung von Interviews mit Informationssicherheits- und technischem Administrationspersonal * Beratung zur Implementierung/zur Entwicklung von Sicherheitsmaßnahmen * Beratung und Unterstützung bei der Erstellung von Konzepten, Richtlinien und Dokumentationen sowie bei der Umsetzung der technischen Cybersecurity |
| Zeitraum | 11/2020 bis 02/2021 |
| Dauer | 4 Monate |
| Aufwände | 54 Personentage |

|  |  |
| --- | --- |
| Mandant | Verband der Reservisten der Deutschen Bundeswehr e.V. |
| Rolle | Fachverantwortung |
| Aufgaben | * Beratung im Bereich Informationssicherheitsmanagement gemäß ISO 27001 auf Basis von BSI IT-Grundschutz. * Design, Implementierung und Dokumentation eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO 27001 auf Basis von IT-Grundschutz   + Erstellung eines Informationssicherheitskonzeptes.   + Erstellen von Richtlinien zur Informationssicherheit   + Abgrenzen des Informationsverbundes |
| Zeitraum | 10/2020 bis 11/2020 |
| Dauer | 2 Monate |
| Aufwände | 25 Personentage |

|  |  |
| --- | --- |
| Mandant | Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (obere Bundesbehörde) |
| Rolle | Fachverantwortung |
| Aufgaben | * Leitung des Projektmanagementoffice * Unterstützung beim Projektcontrolling * Design, Implementierung und Dokumentation eines ISMS gemäß ISO 27001 auf Basis von BSI IT-Grundschutz   + Erstellen von Richtlinien zur Informationssicherheit   + Abgrenzen des Informationssicherheitsverbundes   + Prüfung der Anwendbarkeit von IT-Grundschutzbausteinen auf die Zielobjekte des Informationsverbundes (Modellierung)   + Planung, Durchführung und Auswertung von IT-Grundschutz-checks auf Basis vorhandener Dokumentationen und in Form von Workshops   + Durchführung von Strukturanalysen, Schutzbedarfsfeststellung und Risikoanalysen von Geschäftsprozessen, Anwendungen, IT-Systemen und Infrastrukturkomponenten   + Entwicklung, Analyse, Überprüfung und Umsetzung von Maßnahmen zur Absicherung (Realisierungsplanung) * Unterstützung bei der Vorbereitung der Zertifizierungsreife einer sicheren, Cloud-basierten Kommunikations- und Kollaborations-plattform * Implementierung eines Risikomanagementprozesses * Behandlung von Risiken und Entwicklung von Informationssicher-heitsmaßnahmen * Mitwirkung an der Implementierung eines kontinuierlichen Verbesserungsprozesses im Unternehmen |
| Zeitraum | 03/2020 bis 10/2020 |
| Dauer | 8 Monate |
| Aufwände | 145 Personentage |

|  |  |
| --- | --- |
| Mandant | Statistisches Bundesamt (DESTATIS) |
| Rolle | Fachverantwortung |
| Aufgaben | * Beratung im Bereich Informationssicherheitsmanagement gemäß ISO 27001 auf Basis von BSI IT-Grundschutz. * Design, Implementierung und Dokumentation eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO 27001 auf Basis von IT-Grundschutz   + Erstellen von Richtlinien zur Informationssicherheit   + Abgrenzen des Informationssicherheitsverbundes   + Prüfung der Anwendbarkeit von IT-Grundschutzbausteinen auf die Zielobjekte des Informationsverbundes (Modellierung)   + Durchführung von IT-Grundschutzchecks auf Basis vorhandener Dokumentationen und in Form von Workshops   + Erfassen aller notwendigen Assets des Informationsverbundes (Strukturanalyse)   + Durchführung der Schutzbedarfsfeststellung für alle Assets im Zertifizierungsverbund   + Risikoanalyse   + Entwicklung, Analyse, Überprüfung und Umsetzung von Maßnahmen zur Absicherung (Realisierungsplanung) * Implementierung eines Risikomanagementprozesses * Behandlung von Risiken und Entwicklung von Informationssicherheitsmaßnahmen * Mitwirkung an der Implementierung eines kontinuierlichen Verbesserungsprozesses im Unternehmen |
| Zeitraum | 12/2019 bis 04/2020 |
| Dauer | 5 Monate |
| Aufwände | 72 Personentage |

|  |  |
| --- | --- |
| Mandant | Stab Logistikkommando der Bundeswehr |
| Rolle | Projektleitung |
| Aufgaben | * Durchführen einer IST-Analyse hinsichtlich der Aufbau- und Ablauforganisation der Informationssicherheit inklusive Dokumentation zur Problemidentifikation (Lösungsansatz: Einführung eines ISMS nach BSI IT-Grundschutz für die Dienststelle) * Erstellen eines Projektplans für die Konzeption und Einführung und Etablierung eines dienststellenweiten ISMS sowie dessen kontinuierliche Verbesserung und interner Audits * Erstellung und Fortschreibung eines IT-Sicherheits- sowie Notfallmanagementkonzeptes inkl. Einführung neuer Qualitätsmanagementprozesse unter Zuhilfenahme eines IT-Grundschutztools * Vorbereitung von Vorstandsbeschlüssen und Beratung der Leitungsebene bezüglich der Informationssicherheit * Etablierung eines dienststellenweiten Informationssicherheitsmanagementsystems * Verfolgung und Auswertung von IT-Sicherheitsvorfällen sowie Beratung der Leitungsebene bezüglich zu treffender Sicherheitsmaßnahmen * Management von Risiken in Bezug auf die Informationssicherheit * Erstellung von Plänen und Grundsatzdokumenten zur IT-Systemakkreditierung * Sicherstellen der Kryptosicherheit * Mitarbeit am Datenschutzkonzept |
| Zeitraum | 03/2019 bis 09/2019 |
| Dauer | 6 Monate |
| Aufwände | ca. 100 Personentage |

|  |  |
| --- | --- |
| Mandant | unterstellte Dienststellen im Kommandobereich des Logistikkommandos der Bundeswehr |
| Rolle | Projektleitung |
| Aufgaben | * Vorbereitung, Durchführung und Nachbereitung von Informationssicherheits- und Kryptosicherheitsaudits in mehr als 20 verschiedenen nachgeordneten Dienststellen inkl. Dokumentenaudits sowie ggf. notwendigen Vor- und Nachaudits * Vorbereitung von Vorstandsbeschlüssen und Beratung der Dienststellenleitung bei der   + Umsetzung von aufgezeigten Maßnahmen zur Erreichung bzw. Wiederherstellung der Informationssicherheit und Abstellung von Auditabweichungen   + Erstellung und Fortschreibung der Informationssicherheits-konzeption   + bei der Etablierung von ISMS   + Organisation, Gestaltung und Durchführung von Information Security Awareness Kampagnen und IT-Sicherheits-Schulungen * Begleitung und Beratung bei der Bearbeitung von Informationssicherheitsvorkommnissen * Prüfung von ISMS, inkl. IT-Grundschutzchecks, Risikoanalysen und dienststellenbezogenen IT-Sicherheitskonzepten, u.a. unter Zuhilfenahme des IT-Grundschutz-Tools SAVe * Erstellung von Auditberichten * Schulung von Informationssicherheitspersonal zur Durchführung von Informationssicherheitsaudits |
| Zeitraum | 07/2014 bis 08/2019 |
| Dauer | 5 Jahre, 1 Monat |
| Aufwände | ca. 450 Personentage |

|  |  |
| --- | --- |
| Mandant | Stab Logistikkommando der Bundeswehr |
| Rolle | Projektleitung |
| Aufgaben | * Organisation, Gestaltung und Durchführung einer mehrjährigen Information Security Awareness Kampagne und von IT-Sicherheits-Schulungen * Erstellen eines Projektplans in Anlehnung an die PRINCE2®-Methodik für die Durchführung sowie anschließende Umsetzung in einem über 20 Dienststellen umfassenden behördlichen Umfeld * Führung eines vierköpfigen Teams * Erstellen der Arbeitspakete für Planung, Durchführung und Nachbereitung des Projekts * Durchführung der Information Security Awareness Kampagne mit zugehöriger Schulung für alle Mitarbeiter der Behörde * Fachliche Verantwortung der Erstellung von Schulungsunterlagen |
| Zeitraum | 02/2015 bis 09/2019 |
| Dauer | 4 Jahre, 7 Monate |
| Aufwände | ca. 500 Personentage |

|  |  |
| --- | --- |
| Mandant | Stab Logistikkommando der Bundeswehr |
| Rolle | Fachverantwortung |
| Aufgaben | * Konzeption und Einrichtung sowie Vorbereitung der Akkreditierung eines Lagezentrums für die Verschlusssachen-Kommunikation * Erhebung und Abstimmung relevanter Vorgaben und Vorschriften zur IT-Sicherheit, insbesondere der IT-Grundschutz-Standards, der Kryptosicherheit und der Abstrahlsicherheit sowie Beratung der Dienststellenleitung diesbezüglich * Konzeption des Ausbaus und der Härtung des Lagezentrums * Planung, Begleitung und Auswertung von Schwachstellen-analysen, Abstrahlprüfungen sowie Veranlassung daraus abgeleiteter Sicherheitsmaßnahmen unter Verwendung der IT-Grundschutz-Vorgehensweise * Beratung der militärischen Sicherheit zu Vorgaben der Lauschabwehr * Erstellung von Plänen und Grundsatzdokumenten zur Systemakkreditierung * Beratung von Dienststellen im Kommandobereich bei Fragen zur Umsetzung in ähnlich gearteten IT-Projekten |
| Zeitraum | 08/2017 bis 03/2019 |
| Dauer | 1 Jahre, 8 Monate |
| Aufwände | ca. 80 Personentage |