Alexander Sternberg

# Mitarbeiterinformationen

1: Persönliche Daten

|  |  |
| --- | --- |
| Geburtsdatum | 17.07.1977 |
| Staatsangehörigkeit | Deutsch |
| Unternehmen | Ernst & Young GmbH Wirtschaftsprüfungsgesellschaf |

2: Ausbildung, Studium, Titel

|  |  |
| --- | --- |
| 09/2011 – 12/2016 | FOM Hochschule für Oekonomie & Management – University of Applied Sciences, Wirtschaftsinformatik  Bachelor of Science |
| 09/2001 – 06/2003 | Hochschule für Technik, Wirtschaft und Kultur Leipzig, Medieninformatik |
| 08/1997 – 01/2000 | Industrie- und Handelskammer zu Leipzig, Ausbildung zum Werbekaufmann  Werbekaufmann |

3: Beruflicher Werdegang

|  |  |
| --- | --- |
| Seit 10/2020 | EY Consulting GmbH, Manager Cybersecurity |
| 03/2018 – 09/2020 | PwC Certification Services GmbH, Auditteamleiter |
| 07/2017 – 09/2020 | PwC Cyber Security Services GmbH, Manager Cybersecurity |
| 04/2013 – 06/2017 | PERSICON consultancy GmbH, Senior Consultant Informationssicherheit |
| 07/2007 – 03/2013 | PERSICON AG, Marketing Manager |
| 08/2004 – 06/2007 | Nominell GbR, Gesellschafter |
| 09/2003 – 07/2004 | Revacom GmbH, Sales & Marketing |
| 02/2000 – 08/2001 | SP!EKERTEAM Communication GmbH, Assistent der Geschäftsführung |
| 08/1997 – 01/2000 | THOUET Werbeagentur GmbH, Auszubildender |

4: Weiterbildungen/Zertifikate

|  |  |
| --- | --- |
| BSI-ZGB-0062-2023 | IT-Grundschutz-Berater (BSI) |
| BSI-ZISR-0125-2024 | IS-Revisor (BSI) |
| 10/2020 | Certified Lead Auditor ISO/IEC 27001:2013 (EY) |
| 01/2016 | Geprüfter Datenschutzbeauftragter (SGS-TÜV) |
| 08/2015 | Geprüfter ISO 27001 Auditor (SGS-TÜV) |
| 03/2014 | Geprüfter IT-Sicherheitsbeauftragter (SGS-TÜV) |
| 07/2007 | Foundation Certificate in IT Service Management (ITIL) |

# Kurzbeschreibung

Alexander Sternberg studierte berufsbegleitend Wirtschaftsinformatik an der FOM Hochschule für Oekonomie & Management – University of Applied Sciences in Berlin mit dem Abschluss Bachelor of Science.

Er verfügt über mehr als 11 Jahre Erfahrung in der Beratung zu Themen der Informations- und Cybersicherheit. Seine Schwerpunkte liegen in der Unterstützung von Bundes- und Landesbehörden bei der Entwicklung und Umsetzung von Sicherheitskonzepten nach BSI IT-Grundschutz, der Implementierung von Informationssicherheitsmanagementsystemen (ISMS) sowie der Vorbereitung, Begleitung und Nachbereitung von Zertifizierungsaudits.

Im Laufe seiner Karriere hat Herr Sternberg auch wertvolle Erfahrungen als Auditteamleiter gesammelt. Er leitete Audits nach IT-Grundschutz und ISO/IEC 27001 und verfügt somit über eine umfassende Expertise sowohl in der Konzeption als auch in der Prüfung von Sicherheitsmaßnahmen.

Durch seine langjährige Tätigkeit in einer Vielzahl von Projekten der öffentlichen Hand verfügt Herr Sternberg über umfangreiche Kenntnisse der Aufbau- und Ablauforganisation der öffentlichen Verwaltung sowie deren besonderen Anforderungen.

# Projekterfahrungen

|  |  |
| --- | --- |
| Projekttitel: | Sicherheitskonzeption für die zentralen E-Government-Plattformen zweier Bundeslandes |
| Kunde: | Oberste Landesbehörden zweier Bundesländer |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes war die Erstellung von Sicherheitskonzepten nach BSI IT-Grundschutz für die E-Government-Plattformen zweier Bundesländer. Aufgrund der Kritikalität der verarbeiteten Daten war zusätzlich die Durchführung von Risikoanalysen nach BSI-Standard 200-2 erforderlich. Die Entwicklung und der Betrieb der Plattformen erfolgt durch spezialisierte Dienstleister, die ebenfalls in die Sicherheitskonzeption einbezogen wurden. |
| Zeitraum: | 04/2021 – heute |
| Dauer des Projekts: | 36+ Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Erstellung der Sicherheitskonzepte für zwei E-Government-Plattformen nach BSI-Standard 200-2 * Durchführung von Risikoanalysen nach BSI-Standard 200-2 * Abstimmung und Koordination der Dienstleister im Hinblick auf ein durchgängiges und grundschutzkonformes Sicherheitskonzept * Unterstützung bei der Entwicklung und Umsetzung von Maßnahmen zur Risikominderung * Durchführung von Penetrations- und Lasttests |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * Microsoft Office * HiScout * DocSetMinder * Microsoft Threat Modelling Tool |

|  |  |
| --- | --- |
| Projekttitel: | Unterstützung des Ressort-CISO |
| Kunde: | Oberste Landesbehörde |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes war die Unterstützung des Ressort-CISO beim weiteren Aufbau und Ausbau des ressortweiten Informationssicherheitsmanagementsystems. Dies umfasste die Bearbeitung von Themen und Anfragen aus dem Tagesgeschäft sowie die Begleitung von Projekten aus Sicht der Informationssicherheit. |
| Zeitraum: | 06/2021 – 10/2022 |
| Dauer des Projekts: | 17 Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Erstellung von Sicherheitskonzepten für ausgewählte Fachverfahren sowie Koordination der Erstellung der zugehörigen Datenschutzkonzepte * Begleitung der Umsetzung von Sicherheitsmaßnahmen gemäß Realisierungsplanung * Unterstützung bei der Koordination und Behandlung von Sicherheitsvorfällen * Konzeption und Durchführung von Informationssicherheitsschulungen für die Beschäftigten * Prüfung der im Rahmen von Verträgen zur Auftragsverarbeitung vereinbarten technischen und organisatorischen Maßnahmen * Inhaltliche Abstimmung mit dem DSB zu Schnittmengenthemen von Informationssicherheit und Datenschutz |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | Sicherheitskonzeption für eine Wissensplattform |
| Kunde: | Oberste Landesbehörde |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes war die Erstellung eines Sicherheitskonzeptes für die im Aufbau befindliche zentrale Wissensplattform, um dem erhöhten Wissensverlust durch das altersbedingte Ausscheiden von Wissensträgern entgegenzuwirken. Da parallel zur Erstellung des Sicherheitskonzeptes auch ein Datenschutzkonzept erarbeitet wurde, war es das Ziel, einen integrativen Ansatz zu wählen und die Anforderungen des Datenschutzes und der Informationssicherheit möglichst aufeinander abzustimmen beziehungsweise gemeinsam zu planen. |
| Zeitraum: | 08/2021 – 12/2021 |
| Dauer des Projekts: | 5 Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Erstellung eines integrierten Sicherheits- und Datenschutzkonzeptes nach BSI-Standard 200-2 sowie den geltenden Datenschutzbestimmungen |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | Sicherheitskonzeption für Verkehrsinformationssysteme |
| Kunde: | Oberste Landesbehörde |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes war die Erstellung von Sicherheitskonzepten für ausgewählte Verkehrsinformationssysteme, die Durchführung von Schulungsmaßnahmen zur Informationssicherheit sowie die Erhebung aller betriebenen Verkehrsinformationsdienste einschließlich der verarbeiteten Daten, Abhängigkeiten und Datenflüsse. |
| Zeitraum: | 09/2021 – 02/2023 |
| Dauer des Projekts: | 18 Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Erstellung von Sicherheitskonzepten nach BSI-Standard 200-2 * Durchführung von Risikoanalysen nach BSI-Standard 200-3 * Strukturanalyse aller im Verantwortungsbereich der Landesbehörde betriebenen Verkehrsinformationsdienste sowie Erstellung von Schnittstellenübersichten und Datenflussdiagrammen für die einzelnen Verkehrsinformationsdienste * Konzeption und Durchführung von Informationssicherheitsschulungen für die Beschäftigten |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | Sicherheitskonzeption für eine Verkehrsmanagementzentrale |
| Kunde: | Oberste Landesbehörde |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes ist die Erstellung eines Sicherheitskonzeptes nach BSI IT-Grundschutz für die im Aufbau befindliche Verkehrsmanagementzentrale (VMZ). Die VMZ soll zukünftig eine Schlüsselrolle bei der Steuerung und Überwachung des Straßenverkehrs einnehmen. Ein wesentlicher Bestandteil der VMZ ist die Tunnelleitzentrale, mit der zukünftig etwa 45 Tunnel mit einer Länge von mehr als 400 Metern überwacht werden. Darüber hinaus werden von der VMZ aus die vorhandenen Streckenbeeinflussungsanlagen auf den Bundesstraßen sowie die Lichtsignalanlagen und digitalen Informationstafeln gesteuert und überwacht. |
| Zeitraum: | 09/2021 – 02/2023 |
| Dauer des Projekts: | 18 Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Erstellung eines Sicherheitskonzeptes nach BSI-Standard 200-2 * Durchführung von Risikoanalysen nach BSI-Standard 200-3 * Begleitung des Planungsprozesses für den Aufbau der Infrastruktur, des Netzwerkes sowie den Betrieb der IT-Systeme und Anwendungen aus Sicht der Informationssicherheit * Beratung der Projektleitung in den sämtlichen Themen der Informationssicherheit |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * BSI-KritisV * DIN EN 50600: Einrichtungen und Infrastrukturen von Rechenzentren * HiScout * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | Sicherheitskonzeption für eine Plattform zur Entwicklung und Nachnutzung digitaler Bürgerdienste |
| Kunde: | Oberste Landesbehörde |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes war die Erstellung eines integrierten Sicherheits- und Datenschutzkonzeptes nach BSI-Standard 200-2 für eine Plattform zur Entwicklung und Nachnutzung digitaler Bürgerdienste im Sinne des Onlinezugangsgesetztes. Aufgrund der Kritikalität der verarbeiteten Daten war zusätzlich die Durchführung von Risikoanalysen nach BSI-Standard 200-2 erforderlich. Darüber war die Erstellung Notfallhandbuchs nach BSI-Standard 200-3 Teil sowie die Durchführung eines IS-Webchecks Teil der Beauftragung. |
| Zeitraum: | 11/2021 – 11/2022 |
| Dauer des Projekts: | 13 Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Erstellung eines Sicherheitskonzeptes nach BSI-Standard 200-2 * Bewertung des Umsetzungsstandes der Mindestsicherheitsanforderungen für iKfz4 des Kraftfahrtbundesamtes sowie Identifikation defizitärer Anforderungen * Unterstützung bei der sicheren Entwicklung der Plattform * Durchführung von Risikoanalysen nach BSI-Standard 200-3 * Dokumentation des Sicherheitskonzeptes in HiScout * Erstellung eines Datenschutzkonzeptes * Durchführung eines IS-Webchecks |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * HiScout * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | IT-Grundschutz-Checks für bauliche Infrastruktur |
| Kunde: | Landesanstalt |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes war es festzustellen, inwieweit die einschlägigen IT-Grundschutzanforderungen im Hinblick auf zwei in der Planung befindliche Büro- und Laborgebäude erfüllt wurden, beziehungsweise wo gegebenenfalls Defizite bestehen, die in der weiteren Planung berücksichtigt werden müssen (Soll-Ist-Abgleich). Der Umsetzungsstand wurde in Form von IT-Grundschutz-Checks ausführlich dokumentiert. Bei den Gebäuden handelte es sich um ein Bestandsgebäude, das umfassend saniert werden sollte, und ein Laborgebäude, das neu errichtet werden sollte und in dem unter anderem Gefahrenstoffe gelagert werden sollen. |
| Zeitraum: | 10/2022 – 03/2023 |
| Dauer des Projekts: | 6 Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Planung und Durchführung von Interviews sowie Sichtung bereitgestellter Planungsunterlagen und Konzepte zur Ermittlung des Erfüllungsgrades einschlägigen Sicherheitsanforderungen an die bauliche Infrastruktur * Dokumentation der Ergebnisse in Form von ausgefüllten IT-Grundschutz-Checks |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | Sicherheitsanalysen für Kommunen |
| Kunde: | Behörde für öffentliche Sicherheit |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes war die Entwicklung eines Konzepts zur Erfassung des Ist-Zustands der kommunalen Cybersicherheit, die Durchführung von Sicherheitsanalysen in ausgewählten Kommunen (Umsetzung des Konzepts) sowie die Ableitung individueller Maßnahmenpläne zur Erhöhung der Cyber-Resilienz. Darüber hinaus wurden Musterdokumente zu ausgewählten Sicherheitsthemen entwickelt, die Kommunen für die Erstellung eigener Richtlinien und Konzepte nutzen können. |
| Zeitraum: | 01/2023 – heute |
| Dauer des Projekts: | 18+ Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Entwicklung eines Konzeptes zur Erfassung des Ist-Zustandes der kommunalen Cybersicherheit * Durchführung von Sicherheitsanalysen in 50 Kommunen und Ableitung von Maßnahmenplänen zur Erhöhung der Cyber-Resilienz * Durchführung von Ergebnispräsentationen zur fach- und ebenengerechten Darstellung der Ergebnisse |
| Eingesetzte Tools und Methoden: | * IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung * Leitfaden Cyber-Sicherheits-Check (ISACA/BSI) * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | Unterstützung des CISO |
| Kunde: | Zentrale IT-Dienstleisterin einer Landesverwaltung |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes ist die Beratung und Unterstützung des CISO bei der Wahrnehmung seiner Aufgaben. Der Schwerpunkt der Beratungsleistungen liegt insbesondere in der Entwicklung von Konzepten und Entscheidungsvorlagen zu grundlegenden Themen der Informationssicherheit beziehungsweise der Anwendung des IT-Grundschutzes. |
| Zeitraum: | 08/2023 – heute |
| Dauer des Projekts: | 11+ Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Entwicklung eines Konzeptes für eine modulare Sicherheitskonzeption * Entwicklung eines Stufenplans zur Implementierung eines zertifizierungsfähigen Gesamtsicherheitskonzeptes * Entwicklung und Umsetzung eines Konzeptes zur Einführung von Jira/Confluence als Wissensplattform und Steuerungsinstrument für den Stab Informationssicherheit * Entwicklung eines Konzeptes für das Anbieten von IT-Services mit einer definierten Schutzbedarfseignung (Verzahnung Schutzbedarfseinstufung zwischen Kunde und IT-Dienstleisterin) * Entwicklung und Umsetzung eines Konzeptes für das ISMS Compliance Management |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * Jira * Confluence * Microsoft Office |

|  |  |
| --- | --- |
| Projekttitel: | Sicherheitskonzeption für sicherheitskritische Anwendungen |
| Kunde: | Behörde für öffentliche Sicherheit |
| Branche: | Öffentlicher Sektor |
| Rolle: | Projektleitung |
| Kurzbeschreibung des Projekts: | Ziel des Projektes ist die Entwicklung von Sicherheitskonzepten nach BSI IT-Grundschutz für diverse Fachanwendungen, unter anderem für eine Plattform, über die potenzielle Cybersicherheitsvorfälle gemeldet und Informationen zu aktuellen Ereignissen im Cyber-Raum bereitgestellt werden können, eine Infrastruktur zur verschlüsselten Kommunikation auf Basis von Matrix sowie eine E-Learning-Plattform auf der Basis von Moodle. |
| Zeitraum: | 04/2023 – heute |
| Dauer des Projekts: | 15+ Monate |
| Ausführliche Beschreibung der Aufgaben/Tätigkeiten im Projekt: | * Erstellung von Sicherheitskonzepten nach BSI-Standard 200-2 * Durchführung von Risikoanalysen nach BSI-Standard 200-3 * Dokumentation der Sicherheitskonzepte in HiScout |
| Eingesetzte Tools und Methoden: | * BSI IT-Grundschutz-Methodik * HiScout * Microsoft Office |