Informationssicherheits-, Cybersicherheits- und Datenschutzpolitik

Die Informations- und Telekommunikationstechnik unterstützt die ElringKlinger AG maßgeblich bei der Erfüllung ihrer Leistungen. Die dazu notwendigen Prozesse, Informationen und Systeme stellen für das Unternehmen erhebliche Werte dar und spielen eine Schlüsselrolle bei der Erfüllung der Unternehmensmission. Um diese Werte zu schützen, hat der Vorstand beschlossen, ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001, ein Datenschutzmanagementsystem (DMS) und ein Cybersicherheitsmanagementsystem (CSMS) basierend auf der ISO 21434 einzuführen. Ziel ist es, ISMS, DMS und CSMS als ein integriertes Managementsystem zu führen.

Grundsätzliches Ziel der Aktivitäten im Bereich Informationssicherheit ist der angemessene Schutz des Geschäfts der ElringKlinger AG und der genutzten Unternehmenswerte vor Gefährdungen in allen wesentlichen Teilbereichen. Unternehmenswerte, die es zu schützen gilt, sind u.a.:

- das geistige Eigentum der ElringKlinger AG, der Kunden und Partner,
- spezielles Führungs- und Planungswissen,
- das Wissen und die Fähigkeiten der Mitarbeiter*innen,
- personenbezogene Daten von Mitarbeiter*innen sowie von Partnern und Kunden,
- die Marken der ElringKlinger-Gruppe bzw. die Reputation des Unternehmens und sonstige Sachwerte

Ebenso ist es das Ziel der ElringKlinger AG, alle gesetzlichen Anforderungen zum Datenschutz und zur Informationssicherheit einzuhalten und somit die Risiken für die Rechte und Freiheiten von betroffenen Personen auf ein akzeptables Niveau zu senken und jederzeit die Wahrung des informationellen Selbstbestimmungsrechts sicherzustellen.

Alle Mitarbeiter der ElringKlinger AG sind für die Einhaltung datenschutz- und informationssicherheits- bzw. cybersicherheitsrelevanter Maßnahmen entsprechend ihrem Tätigkeitsbereich verantwortlich. Die Mitarbeiter und alle im Auftrag der ElringKlinger AG tätigen Personen sind zur Einhaltung der Gesetze sowie zur Wahrung der Geschäftsgeheimnisse verpflichtet. Der Vorstand der ElringKlinger AG ist verantwortlich für die Einhaltung gesetzlicher Vorgaben im Datenschutz, der Informationssicherheit und Cybersicherheit sowie die Bereitstellung der dafür notwendigen Ressourcen. Verantwortlich für die Erstellung und Umsetzung der Richtlinien und Maßnahmen der Informationssicherheit ist der Konzern-Informationssicherheitsbeauftragte (CISO), im Datenschutz der Konzern-Datenschutzbeauftragte oder in der Cybersicherheit der Chief Cybersecurity Officer (CCSO).

Die Einhaltung des Datenschutzes, der Informationssicherheitsrichtlinien und der Richtlinien zur Cybersicherheit soll die Vertraulichkeit, Verfügbarkeit und Integrität von Daten in Netzen, auf Systemen, im Entwicklungs- und Produktionsprozess sicherstellen. Daten sind vor Verlust zu sichern und falls gesetzlich vorgeschrieben, hat auch eine Archivierung zu erfolgen. Ebenso ist die datenschutzgerechte Entsorgung und Löschung von Informationen sicherzustellen. Vertragspartner haben, sofern sie einer Auftragsverarbeitung unterliegen, die Anweisungen der ElringKlinger AG umzusetzen. Bei der Verarbeitung von personenbezogenen Daten oder vertraulichen Daten sind von Partnern Normen wie die EU-DSGVO/ISO27701, VDA-TISAX/AIAG-TPISR, ISO 21434, ISO 27001 oder vergleichbar einzuhalten.

Über den gesamten Produktlebenszyklus von der Entwicklung bis zur Außerbetriebnahme setzt die ElringKlinger AG die gesetzlichen und kundenspezifischen Forderungen im Rahmen eines Cybersicherheit-Managementsystems um. Hierbei liegt die übergreifende Verantwortung für den Aufbau beim CCSO. Auf Produktebene ist der Cybersecurity Manager für die Absicherung gegen Cyberangriffe verantwortlich. Dazu wird er vom Functional Safety Manager und den Fachbereichen unterstützt.

Die Begrenzung des Zugriffs auf Informationen, je nach Klassifizierung, ist durch Berechtigungen und dem Stand der Technik zu sichern und zur Sicherstellung der Nachvollziehbarkeit datenschutzkonform zu protokollieren.

Die relevanten Unternehmenswerte sind gegen höhere Gewalt (Naturkatastrophen/Krieg), Pandemien, Brand, Wasser und Diebstahl zu schützen. Informationssicherheits-Risiken sind regelmäßig zu bewerten und bei akuten Bedrohungslagen schnellstmöglich entsprechende Gegenmaßnahmen einzuleiten.

Für alle Unternehmensbereiche sind Risiken definiert, die in regelmäßigen Abständen intern und extern bewertet werden. Falls erforderlich sind dazu passende Gegenmaßnahmen festzulegen und die Wirksamkeit dabei nachzuweisen.

2024

THOMAS JESSULAT

REINER DREWS

DIRK WILLERS