framatome

Sicherheitsstatement

Einleitung

Dieses Sicherheitsstatement soll Ihnen Auskunft über unsere Sicherheitskultur und -praktiken in der Informationssicherheit liefern.

Die Sicherheit unserer Daten und der Daten unserer Kunden und Partner hat für uns hohe Priorität. Wir unternehmen gezielte Maßnahmen, um sicherzustellen, dass alle Daten, die uns zur Verfügung gestellt werden, sicher verarbeitet und gespeichert werden. Die Sicherheit unserer IT-Systeme, unserer Produkte und aller Daten ist daher für uns selbstverständlich und Teil der Unternehmenskultur.

Unsere Datenschutzerklärung mit weiteren Informationen darüber, wie wir z.B. mit den von uns erhobenen personenbezogenen Daten umgehen, finden Sie neben dem Impressum auf der Framatome GmbH Homepage.

Ziele und kontinuierliche Verbesserung

Unsere Hauptziele in der Informationssicherheit sind

Vertraulichkeit, Integrität, Verfügbarkeit und Nachverfolgbarkeit.

Kontinuierlich erweitern wir unser Informationssicherheits-Managementsystem (ISMS) und orientieren uns dabei an internationalen Standards wie z.B. ISO/IEC 27001. Kontinuierlich arbeiten wir an der Verbesserung der Informationssicherheit und orientieren uns dabei an aktuellen Erkenntnissen und Entwicklungen.

Informationssicherheitsrichtlinien (Policy) und Organisation

Das Unternehmen verfasst schriftliche Informationssicherheitsrichtlinien, die eine breite Palette von sicherheitsrelevanten Themen abdeckt; von allgemeinen Standards für jeden Beschäftigten, wie Passwortrichtlinie, Nutzung der IT-Systeme oder Gebäudesicherheit, bis hin zu spezielleren Sicherheitsstandards für spezifische Anwendungen und Informationssysteme.

Die Pflichten der Beschäftigten und die zulässige Nutzung der Informationssysteme sind definiert. Jeder Mitarbeiter hat uneingeschränkten Zugriff auf relevante Anweisungen sowie weiterführende Dokumente und Links im unternehmensweiten Intranet.

Framatome unterhält eine Sicherheitsorganisation mit entsprechend besetzten Stabstellen und klarer Rollenverteilung. Spezielle Teams (bspw. SOC=Security Operation Center, CERT=Computer Emergency Response Team) sind für die Kontinuität und Sicherheit während des Betriebes sowie für die Reaktion und Aufklärung bei Vorfällen verantwortlich.

Personensicherheit / Awareness

Framatome führt zum Zeitpunkt der Neueinstellung eine Sicherheitsüberprüfung durch. Darüber hinaus kommuniziert Framatome seine Informationssicherheitsrichtlinien an alle Beschäftigte, welche diese anerkennen müssen. Zusätzlich wird von allen Mitarbeitern erwartet, eine Geheimhaltungserklärung zu unterzeichnen. Alle Beschäftigten werden jährlich hinsichtlich Datenschutz und Informationssicherheit geschult. Wir achten stets auf ein hohes Niveau an Sicherheitsbewusstsein gegenüber aktuellen Angriffsszenarien und Risiken.

Bei besonders sensiblen, strategischen und sicherheitsrelevanten Positionen finden regelmäßig wiederholte Sicherheitsüberprüfungen statt.

Asset Management

Framatome verfügt über eine Asset Management Richtlinie, die die Identifizierung, Klassifizierung, Aufbewahrung und Entsorgung von Informationen und Vermögenswerten umfasst. Firmeneigene Geräte sind mit Festplattenverschlüsselung und aktueller Applikation gegen Schadsoftware ausgestattet.

Nur freigegebene oder firmeneigene Geräte dürfen auf Unternehmens- und Produktionsnetzwerke zugreifen. Private Geräte sind für die dienstliche Benutzung nicht zugelassen.

Schwachstellenmanagement und Penetrationstests

Framatome unterhält ein dokumentiertes Programm zum Management von Schwachstellen, das regelmäßige Scans, die Identifizierung und Behebung von Sicherheitslücken auf Servern, Workstations, Netzwerkgeräten und Anwendungen umfasst. Alle Netzwerke, einschließlich Test- und Produktionsumgebungen, werden regelmäßig gescannt. Kritische Patches werden priorisiert angewendet.

Wir führen auch regelmäßige interne und externe Penetrationstests durch und reagieren entsprechend auf die gefundenen Ergebnisse nach erfolgter Risikoanalyse.

Protokollierung und Überwachung

Anwendungs- und Infrastruktursysteme protokollieren Informationen in einem zentral verwalteten Protokoll-Repository zur Fehlerbehebung, Sicherheitsüberprüfung und Analyse durch autorisiertes Framatome-Personal. Protokolle werden gemäß gesetzlicher Anforderungen aufbewahrt.

Incident Management

Framatome lebt einen Prozess zur Reaktion auf Sicherheitsvorfälle in der Informationssicherheit zusammen mit dem Datenschutz. Dieser umfasst die anfängliche Reaktion auf den Vorfall, die Klassifizierung und Priorisierung, die Untersuchung, die Benachrichtigung der Kunden, die öffentliche Kommunikation und die Behebung. Dieser Prozess wird regelmäßig überprüft und alle zwei Jahre getestet.

Benachrichtigung über Verstöße

Trotz aller Anstrengungen ist keine Methode der Übertragung aus dem Internet und keine Methode der elektronischen Speicherung absolut sicher. Wenn Framatome jedoch von einer Sicherheitsverletzung erfährt, benachrichtigen wir die betroffenen Stakeholder, um geeignete Schutzmaßnahmen ergreifen zu können. Unsere Verfahren zur Meldung von Verstößen stehen im Einklang mit unseren Verpflichtungen gemäß geltender Gesetze und Vorschriften der Länder sowie allen für uns geltenden Branchenregeln oder Standards. Wir informieren und unterstützen unsere Kunden bei Sicherheitsvorkommnissen und stellen alle relevanten Informationen zur Verfügung, die sie zur Erfüllung ihrer eigenen regulatorischen Berichtspflichten benötigen.

Risikomanagement und Audits

Maßnahmen in der Informationssicherheit basieren auf einem systematischen risikobasierten Ansatz. Eine jährliche Überprüfung und Bewertung der Risiken werden durchgeführt. Regelmäßige interne und externe Audits führen zu einer kontinuierlichen Verbesserung unserer Informationssicherheit.

Produktentwicklung

Unser Entwicklungsteam verwendet sichere Codierungstechniken und Best Practices gemäß anerkannter Standards. Entwickler werden bei der Einstellung und regelmäßig in der Entwicklung sicherer Anwendungen geschult.

Entwicklungs-, Test- und Produktionsumgebungen sind getrennt. Alle Änderungen werden von Experten überprüft und zu Leistungs-, Audit- und forensischen Zwecken vor der Bereitstellung in der Produktionsumgebung protokolliert.

Physische Sicherheit

Framatome verfügt über Richtlinien, Verfahren und Infrastruktur, um sowohl die physische Sicherheit seiner Rechenzentren als auch der Umgebung, von welcher die Rechenzentren betrieben werden, zu gewährleisten.

Sowohl Informationssysteme als auch die technische Infrastruktur von Framatome werden in state-of-the-art Rechenzentren gehostet, die geografisch getrennt sind, um Framatome und seinen Kunden eine hohe Verfügbarkeit und Redundanz zu gewährleisten. Physische Sicherheitskontrollen in diesen Rechenzentren umfassen eine rund um die Uhr Überwachung mittels Kameras, elektronische Zugangskontrollsysteme, Besucherprotokolle, Zugangsbeschränkungen, Brandmelde- und Löschanlagen.

Die Firmengelände, Gebäude und Anlagen von Framatome sind durch verschiedene physische, organisatorische und technische Maßnahmen gegen Einbruch, Diebstahl und Vandalismus geschützt. Dazu gehören z.B. der Werkschutz, Videoüberwachung, Zutrittskontrollmechanismen über Vereinzelungsanlagen oder der Empfang.

Je nach Sensibilität der Tätigkeiten und der verarbeiteten Informationen existieren unterschiedliche physisch getrennte Bereiche: öffentlicher (Besucher) Bereich, Büro-Bereich, Server- und IT-System-Bereiche.

Business Continuity Management

Framatome verwendet eine umfangreiche Backup-Strategie für alles Systeme, um minimale Ausfallzeiten und Datenverlust zu gewährleisten. Der Business Continuity Plan wird regelmäßig getestet und aktualisiert, um seine Wirksamkeit im Katastrophenfall sicherzustellen. Backups werden verschlüsselt gespeichert, um ihre Vertraulichkeit und Integrität zu wahren.

Server verfügen über redundante interne und externe Netzteile. Rechenzentren verfügen über Backup-Stromversorgungen und können Strom von Dieselgeneratoren und USVen beziehen.

Informationssicherheit bei unseren Partnern

Unsere hohen Anforderungen in der Informationssicherheit sind integraler Bestandteil in den Verträgen mit unseren Unterlieferanten, Servicepartnern, Stakeholdern und anderen Partnern. In Audits überwachen wir die Einhaltung und Umsetzung unsere Grundsätze.