Betreibt das Unternehmen ein Informationssicherheits -Management -System (ISMS)?

Ja, das Unternehmen RECPLAST GmbH betreibt ein Informationssicherheits-Management-System (ISMS), das dem Regelwerk "IT-Grundschutz" des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügt. Zentraler Bestandteil eines ISMS ist u.a. die Leitlinie zur Informationssicherheit und regelmäßige Kontrolle durch ein internes ISMS-Audit.

Betreibt das Unternehmen ein Cyber Security Management System (CSMS)?

Ja, das Unternehmen betreibt ein Cyber Security Management System (CSMS).

Betreibt das Unternehmen ein Software Update Management System (SUMS)?

Ja, das Unternehmen betreibt ein Software Update Management System (SUMS).

Bestehen für diese(s) System(e) eine Zertifizierung, zum Beispiel nach ISO 21434 oder eine Prüfung nach den Anforderungen des Kraftfahrtbundesamtes (KBA)?

Nein, es gibt keine Zertifizierung nach ISO 21434 oder eine Prüfung nach den Anforderungen des Kraftfahrt-Bundesamtes (KBA) für diese Systeme.

Existiert im Unternehmen ein benannter Cyber Security Manager?

Ja, es existiert im Unternehmen ein benannter Cyber Security Manager (Informationssicherheitsbeauftragter).

Gibt es im Unternehmen eine Cyber Security Management Richtlinie?

Ja, gibt es im Unternehmen eine Cyber Security Management Richtlinie.

Wie werden die Mitarbeiter über die Gefahren beim Umgang mit cyber -security relevanten Informationen und deren Verarbeitung informiert? (Schulungen, Informationstage o.ä.)

Die Mitarbeiter werden über die Gefahren beim Umgang mit cyber-security relevanten Informationen und deren Verarbeitung informiert durch Schulungen, Informationstage etc. Sie erhalten Checklisten, um einen Sicherheitsvorfall zu erkennen. Der Leiter der Informationstechnik ist für die Ausbildung und Beratung zuständig.

Werden Mitarbeiter geschult und sensibilisiert? (hinsichtlich Cyber Security)

Ja, Mitarbeiter des OT-Bereiches werden regelmäßig zu Sicherheitsbedrohungen geschult. Die OT-Verantwortlichen werden regelmäßig vom ICS-ISB zur Bedrohungslage und möglichen Handlungsbedarf geschult.

Wurde eine TARA (Threat and Risk Analysis) für die Produkte/Komponenten durchgeführt nach ISO 21434 und werden die erkannten Risiken entsprechend behandelt?

Ja, für die Produkte/Komponenten wurde eine TARA (Bedrohungs- und Risikoanalyse) nach ISO 21434 durchgeführt und die identifizierten Risiken werden entsprechend behandelt.

Wird vor Auftragsvergabe an Fremdfirmen die Cyber Security der Auftragnehmer geprüft und sichergestellt?

Ja, die Cyber Security der Auftragnehmer wird vor Auftragsvergabe geprüft und sichergestellt.

Wie wird die Geheimhaltung bei der Zusammenarbeit mit Fremdfirmen

sichergestellt?

Die Geheimhaltung bei der Zusammenarbeit mit Fremdfirmen wird sichergestellt, indem die Clients der Geschäftsführung nicht zusammengefasst werden und ein Schutzzonenkonzept umgesetzt wird. Darüber hinaus erfolgt eine regelmäßige Überprüfung durch den Sicherheitsdienst.

Werden interne Audits zur Überprüfung der Cyber Security durchgeführt?

Ja, werden interne Audits zur Überprüfung der Cyber Security durchgeführt. Das Schwerpunkt des internen ISMS-Audits ist der IT-Grundschutz-Check.

Existiert eine Zutrittssteuerung in Ihrem Unternehmen?

Ja, es gibt eine Zutrittssteuerung in Ihrem Unternehmen. Die Auslandsreisen müssen von dem Vorgesetzten und der Personalabteilung genehmigt werden. Darüber hinaus sind die Mitarbeiter verpflichtet sich über die klimatischen sowie die notwendigen Schutzmaßnahmen (Impfungen etc.) zu informieren und bei Besonderheiten immaterielle Folgen in Form von Imageschäden für das Unternehmen zu verhindern.

Existiert eine Sicherheitszonenkonzept in Ihrem Unternehmen und wenn ja, wie ist dieses Aufgebaut?

Ja, es gibt ein Schutzzonenkonzept in Ihrem Unternehmen. Das Konzept beinhaltet Maßgaben hinsichtlich der Gebäudenutzung und regelt den Zutritt zu den Büros. Es gibt keinen Publikumsverkehr.

Wie ist das Unternehmen gegen umgebungsbezogene Bedrohungen geschützt?

Das Unternehmen ist gegen umgebungsbezogene Bedrohungen geschützt, indem es Maßnahmen wie die Verwendung von Geräten und Systemen durch berechtigte Administratoren oder Mitarbeiter setzt, eine Zwei-Faktor-Authentisierung verwendet und das Restrisiko als vertretbar ansieht.

Wie werden Backups erstellt und die erfolgreiche Durchführung kontrolliert?

Backups werden im Raum erstellt und sicher gespeichert. Die erfolgreiche Durchführung von Backups wird durch regelmäßige Integritätsprüfungen kontrolliert, sodass bei einem Ausfall die Daten schnell wiederhergestellt werden können.

Werden regelmäßige Restore -Tests durchgeführt? (Wiederherstellung der Backups)

Ja, regelmäßige Restore -Tests werden durchgeführt.

Wie werden Back -End -Server geschützt?

Die Back-End-Server werden durch die aktive Verwaltung der Wurzelzertifikate geschützt.

Gibt es segmentierte Netzwerke im Unternehmen? (z.B. Gästenetzwerk und Produktivnetzwerk)

Ja, es gibt segmentierte Netzwerke im Unternehmen. Im Sicherheitskonzept sind verschiedene Segmentierungskonzepte definiert, wie z.B. DMZ-Segmentierung und spezifische Richtlinien für das Netzwerk der RECPLAST GmbH. Die Segmentierung ist netztechnisch realisiert worden.

Gibt es ein Konzept wie Software -Stände und Software -Update der E/E -Produkte über den Produkt -Lebenszyklus gemanaged werden?

Ja, es gibt ein Konzept wie Software-Stände und Software-Update über den Produkt-Lebenszyklus gemanaged werden. Die RECPLAST GmbH verfolgt hierbei eine standardisierte Vorgehensweise bei der Einführung neuer Office-Produkte, die von Anforderungskatalog erstellt wird, getestet wird und schließlich installiert wird. Zudem gibt es regelmäßige Updates, die über den Produkt-Lebenszyklus gemanaged werden.

Wie wird der Zugriff durch Dritte auf das Unternehmensnetz geregelt (z.B. Dienstleister)?

Der Zugriff durch Dritte auf das Unternehmensnetz wird geregelt, indem die Verbindungen zu öffentlichen Netzen (Telefonnetz, Internet) oder über ein öffentliches Gelände reichen, sorgfältig kontrolliert werden. Darüber hinaus sind alle Clients geschützt durch eine Firewall und einen Switch mit Paketfilter abgesichert. Ferner wird der Zugriff auf das Archivsystem nur angemeldeten Usern möglich.

Gibt es Richtlinien im Unternehmen für den Umgang mit mobilen Datenträgern?

Ja, es gibt Richtlinien im Unternehmen für den Umgang mit mobilen Datenträgern. Die [Richtlinie Mobile Datenträger] regelt u.a. die Telefonfunktion des Smartphones, die Nutzung der "Luftschnittstelle", die Sicherstellung der Energieversorgung und die sichere Datenübertragung über Mobiltelefone.

Gibt es im Unternehmen einen Prozess zur sicheren Entsorgung von Datenträgern?

Ja, das Unternehmen hat einen Prozess zur sicheren Entsorgung von Datenträgern. Die RECPLAST GmbH setzt für das Löschen bzw. Vernichten von Datenträgern eine Freeware, mit der die Datenträger mehrfach mit Zufallszahlen überschrieben werden. Darüber hinaus müssen alle schutzbedürftigen Datenträger und Informationen bis zur Rückkehr vernichtet oder entsorgt werden lassen. Die Mitarbeiter werden im Rahmen der Informationssicherheitsschulungen auf den Prozess der Vernichtung von Datenträgern hingewiesen.

Gibt es eine Leitlinie zur Anwendung von Verschlüsselung und kryptografischen Maßnahmen?

Ja, es gibt eine Leitlinie zur Anwendung von Verschlüsselung und kryptografischen Maßnahmen im Kryptokonzept. Die RECPLAST GmbH orientiert sich bei der Auswahl von kryptografischen Verfahren an der "BSI TR-02102-1".

Inwiefern sind Maßnahmen für das Cyber Security Monitoring und das Schwachstellenmanagement etabliert?

Maßnahmen für das Cyber Security Monitoring und das Schwachstellenmanagement sind etabliert, indem Störungen oder Sicherheitsvorfälle über das internet Ticket-System gemeldet werden können. Zusätzlich besteht die Möglichkeit über die Notfallnummer der IT-Abteilung eine Störung oder einen Sicherheitsvorfall zu melden. Die Kommunikationswege und die Ansprechpartner sind in der Security Policy definiert.

Inwieweit ist das Arbeiten mit mobilen Geräten geregelt?

Das Arbeiten mit mobilen Geräten wird in der Richtlinie "Mobiles Arbeiten" geregelt. Die Richtlinie untersagt grundsätzlich die Nutzung von mobilen Endgeräten in unsicheren Umgebungen und enthält Vorgaben für den Schutz von Informationen, wie z.B. die Verwendung von Bildschirmschutzfolien und die Sicherstellung einer dauerhaften Stromversorgung.

Gibt es eine Anordnung zur Einhaltung der Ordnung? (z.B. clean desk policy)

Ja, es gibt eine Anordnung zur Einhaltung der Ordnung namens Clear Desk Policy. Sie verpflichtet jeden Mitarbeiter dazu seinen Arbeitsplatz aufgeräumt zu hinterlassen, um Unbefugten keinen Zugang zu IT-Anwendungen und/oder zu schützenden Informationen zu ermöglichen.

Existiert eine Richtlinie zum Patch -Management?

Ja, es gibt eine Richtlinie zum Patchmanagement. Es wird in der Systemdokumentation definiert und zwei Updateverwaltungstools eingesetzt, die das Einspielen von Updates aus der Ferne ermöglichen.

Wie werden Unternehmensnetzwerke vor Schadsoftware geschützt?

Unternehmensnetzwerke werden vor Schadsoftware geschützt, indem Verbindungen zwischen dem Unternehmen und öffentlichen Netzen begrenzt werden, Virenschutzsoftware eingesetzt wird und die Systeme über geeignete Schutzmechanismen verfügen. Zusätzlich soll eine Cyber- Versicherung abgeschlossen werden, um monetäre Schäden zu vermeiden oder zu verringern.

Werden Informationen im Unternehmen klassifiziert? (z.B. öffentlich, intern, vertraulich & streng vertraulich)

Ja, Informationen im Unternehmen werden klassifiziert. Es gibt ein Klassifizierungsschema mit den Stufen S1 (öffentlich), S2 (intern) und S3 (geheim). Dokumente werden gemäß diesem Schema klassifiziert.

Gibt es Definitionen zum Umgang mit Informationen entsprechend einer Klassifizierung? (z.B. Handhabung, Transport, Speicherung und Löschung)

Ja, es gibt Definitionen zum Umgang mit Informationen entsprechend einer Klassifizierung. Im Kontext der RECPLAST GmbH werden Dokumente gemäß des folgenden Klassifizierungschemas klassifiziert (S1 öffentlich, S2 intern und S3 geheim). Darüber hinaus gibt es Richtlinien für den Umgang mit Informationen, wie z.B. die Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen (CON.6 Löschen und Vernichten).

Gibt es Sicherheitseinrichtungen für Notfälle? (z.B. Brandschutzzonen, redundante Systeme o.ä.)

Ja, es gibt Sicherheitseinrichtungen für Notfälle wie Brandschutzzonen und redundante Systeme.