Leitlinie zur Informationssicherheit

Die Geschäftsführung verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil ihrer Strategie:

Stellenwert der Informationsverarbeitung

Informationsverarbeitung spielt eine Schlüsselrolle für unseren Geschäftsbetrieb. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informations- und Kommunikationstechnik (Information and Communication Technology ‚ICT') maßgeblich unterstützt. Ein Ausfall von ICT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf unser Geschäft nicht zusammenbrechen. Da unsere Kernkompetenz in der partnerschaftlichen Entwicklung innovativer Produkte im Zusammenspiel mit Kunden und Lieferanten liegt, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung.

Übergreifende Ziele

Unsere Daten und unsere ICT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer *Verfügbarkeit* so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und ICT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (*Integrität*). Die Anforderungen an *Vertraulichkeit* haben ein normales, an Gesetzeskonformität orientiertes Niveau. Für Konstruktionsdaten unserer Kunden und der Entwicklungsabteilung gelten maximale Anforderungen an die Vertraulichkeit.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und den ICT-Systemen stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze (z. B. Gesetze und Regelungen zum Datenschutz), interne Verfahrens- und Arbeitsanweisungen und getroffene vertragliche Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße und Vertragsverletzungen sind zu vermeiden.

Alle Mitarbeiter und die Unternehmensführung sind sich ihrer Verantwortung beim Umgang mit ICT-Systemen bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

Detailziele

Verspätete oder fehlerhafte Managemententscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen der Zugriff auf aktuelle

Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicherzustellen.

Die Datenschutzgesetze und die Interessen unserer Mitarbeiter verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die ICT-Anwendungen der Personalabteilung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Geschäftspartner.

Anfrage- und Angebotsdaten von und zu unseren Kunden sowie Konstruktionsdaten unserer Kunden und unserer Entwicklungsabteilung haben sehr hohe Vertraulichkeitsanforderungen. Durch deren Verlust oder Diebstahl können Wettbewerbsnachteile oder gegen uns gerichtete Schadensersatzforderungen entstehen. Durch technische Maßnahmen und hohe Aufmerksamkeit der Mitarbeiter wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt.

Für die Logistikbereiche und die Produktionswerke werden die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt. Stillstandzeiten sind nur in einem sehr geringen Maße akzeptabel, da diese direkt, aber auch indirekt zu Erlösminderungen führen können und sich negativ auf die Kundenzufriedenheit auswirken.

Die Nutzung des Internets und von Portalanwendungen zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Nutzung möglichst gering bleiben.

Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet. Es ist ein Beauftragter für Informationssicherheit benannt worden. Der Beauftragte für Informationssicherheit berichtet in seiner Funktion direkt an die Geschäftsführung.

Dem Beauftragten für Informationssicherheit werden von der Geschäftsführung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Management festgelegten Informationssicherheitsziele zu erreichen.

Die ICT Sicherheitsadministratoren und der Beauftragte für Informationssicherheit sind durch die ICT-Benutzer in ihrer Arbeit zu unterstützen.

Der Beauftragte für Informationssicherheit ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Die ICT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des Beauftragten für Informationssicherheit zu halten.

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, ICT-Anwendungen und ICT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf ermittelt und die Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass die Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu ICT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computerviren-Schutzprogramme werden auf allen ICT-Systemen eingesetzt. Alle Internetzugänge werden durch geeignete Firewallsysteme gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die ICT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der ICT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrechtzuerhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Sofern ICT-Dienstleistungen an externe Stellen ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Sofern zur Vertragserfüllung Daten mit hohem Schutzbedarf Lieferanten zugänglich gemacht werden müssen, werden diese von uns gesondert und ausdrücklich zur Geheimhaltung verpflichtet. Das Recht auf Kontrolle wird festgelegt.

ICT-Benutzer nehmen an Schulungen zur korrekten Nutzung der ICT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Unternehmensleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Verbesserung der Sicherheit

Das Managementsystem der Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Geschäftsleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der ICT-Sicherheitstechnik zu halten.

Bamberg, 02-05-2018

- Geschäftsführung -

Thomas Mai

Stefan Frey

- Beauftragter für Informationssicherheit –

Ralf Ruf