IT-Sicherheit und Datenschutz

Wie müssen Unternehmen auf die neue Datenschutz-Grundverordnung reagieren?

Dipl.-Ing. Ulrich Lieske, Senftenberg

IT-Sicherheit, Datenschutz und IT-Service-Management: Mit dieser Kombination wird jedes Klein- und Mittelstands-Unternehmen konfrontiert, insbesondere Betreiber kritischer Infrastrukturen im Personen- und Güterverkehr. Nachdem die Schlagwörter rund um IT-Sicherheit und Datenschutz durch die Medien getrieben wurden (Abb. 1), versuchen Verantwortliche in Verkehrs-, Transport- und Logistik-Betrieben zu deuten, wie weit diese Themen konkret in ihre Verantwortung reichen.

Der Gesetzgeber hat mit der Datenschutz-Grundverordnung (DSGVO) und dem IT-Sicherheitsgesetz nachdrücklich die Frage gestellt, wie es Unternehmen mit IT-Sicherheit und Datenschutz halten. Die Unternehmen sind in der Pflicht, Antworten zu geben. Eine Vogel-Strauß-Taktik wird zu empfindlichen Schäden führen. Unwissenheit erwies sich schon immer als teuer.

Langsam dämmert die Erkenntnis, dass Digitalisierung zur Effizienzsteigerung und Kostensenkung einher geht mit der Notwendigkeit, bisher unbekannte Prozesse, Technologien und Gefahren zu beherrschen. Die Gesetze und Verordnungen erzeugen lediglich den Druck auf etwas, was eigentlich selbstverständlich sein müsste – der Schutz und verantwortungsvolle Umgang mit Eigentum: eigenem und fremdem. Der Gedanke an digitales Eigentum scheint gewöhnungsbedürftig, ist in der Realität jedoch längst angekommen.

Wer also personenbezogene Daten speichert und verarbeitet, wer digitale Prozesse in seinem Unternehmen einführt, hat eine Management-Aufgabe: die Balance zwischen IT-Nutzen und -Sicherheit herzustellen. Was ist zu tun, um dieser Aufgabe gerecht zu werden?

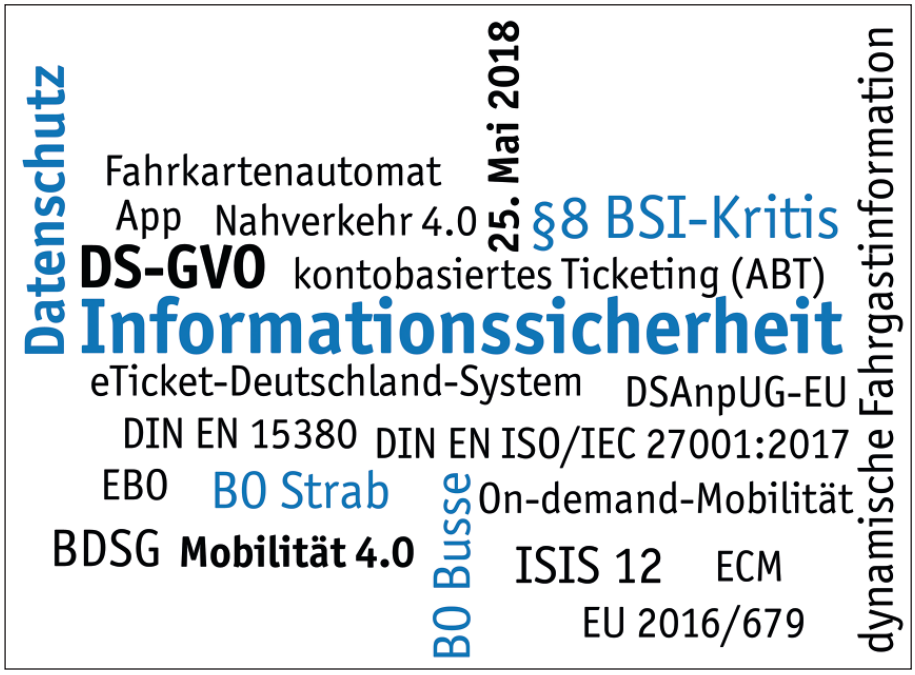

Abb. 1: Was bewegt Nahverkehrsbetreiber bei der anstehenden Digitalisierung?

Zunächst muss die Verantwortung für diese Aufgabe eindeutig und klar zugewiesen sein. Ob Datenschutz- oder IT-Sicherheitsbeauftragter, Chief Security Officer oder Administrator, diese Person wird scheitern, wenn ihr nicht auch Budget, fachliche Ressourcen sowie Unterstützung und Kontrolle der Geschäftsführung sicher sind.

Dokumentation ist die Basis

Die Basis jeglicher Umsetzung von IT-Sicherheit und Datenschutz im Unternehmen bildet die Dokumentation der IT-Umgebung und der IT-gestützten Prozesse. So ungeliebt und vernachlässigt diese Aufgabe ist, so essentiell ist sie. Eine pauschale Definition, was und wie zu dokumentieren ist, gibt es nicht. Eine pragmatische Vorgehensweise ist es, zunächst eine allgemein abstrahierende Struktur der IT-Dokumentation top-down zu entwickeln. Ausgehend von den Überschriften Organisation, Technik, Prozesse/Software/Daten und Betriebsführung (Tab. 1) ermöglicht dieser Ansatz die weiterführende Anpassung an die Spezifika des jeweiligen Unternehmens.

Wichtig ist es, die Dokumentationsablage unternehmensweit zentral zu etablieren. Inhaltlich sollte sie so kompakt wie möglich und so umfangreich wie nötig sein. Wer sich vorher Gedanken um die Dokumentationsinhalte macht, diese in unternehmensweite Vorlagen „gießt“ und dazu einheitliche Konventionen zur Dokumentenlenkung definiert, spart sich eine Menge Arbeit im Nachgang, unterschiedliche Sichten Einzelner mühsam zusammenzuführen.

Bei IT-Projekten im Unternehmen ist eine adäquate Dokumentation von (internen oder externen) Dienstleistern einzufor-

Zum Autor

Dipl.-Ing. Ulrich Lieske ist einer der Gründer der Senftenberger Zedas GmbH und Leiter des Geschäftsbereichs Systemintegration. Er ist Ansprechpartner für die Planung und Umsetzung komplexer IT-Infrastrukturlösungen. Seine Spezialgebiete sind die Architektur sicherer Produktionsnetzwerke und Data Analytics Lösungen. Lieske studierte an der Hochschule für Verkehrswesen Dresden Informationstechnik mit den Schwerpunkten Automatisierungstechnik, Eisenbahnsicherungstechnik, Fernmeldetechnik/Rechnernetze und war mehrere Jahre als Dozent an der FH Lausitz tätig.

Tab. 1: Ansatzpunkte zur Entwicklung einer IT-Dokumentation.

Organisation	Organigramm, Verträge, Vereinbarungen, Richtlinien, Anordnungen, Verzeichnis der Verarbeitungstätigkeiten, technisch-organisatorische Maßnahmen, …
Technik	Inventarisierung, Topologie- und Systemstruktur, Regelwerke, Konfigurationen, …
Prozesse/Software/Daten	Kritische Unternehmensprozesse, Software-Versionen, Lizenzen, Anwender, Rollen, Berechtigungen, Daten-Klassifizierung, …
Betriebsführung	Änderungs-Management, Monitoring, Helpdesk & Entstörung, Security-Management, Datensicherung und -wiederherstellung, Schnittstellendokumentation, …

Tab. 2: Allgemeine Grundsätze für IT-Sicherheit und Datenschutz.

Security by Design	Berücksichtigung von IT-Sicherheit/Datenschutz in jeder Planung
Security by Obscurity	Beschränkung auf notwendige Informationen und Berechtigungen
Security by Default	Es wird/ist per Standard alles gesperrt, was nicht explizit erlaubt ist
Security by Himself	Jeder Mitarbeiter ist verantwortlich

dern. Die Informationen sind zum Projektabschluss in die zentrale IT-Dokumentation zu integrieren. Dieser Meilenstein darf in keinem Projektplan fehlen. „80 Prozent dokumentiert, ist immer besser als keine Dokumentation“ – jedes Sicherheitsaudit wird dieses Prinzip bestätigen.

Vergleich mit dem Stand der Technik

Dokumentieren führt fast immer zu Fragen und – richtig gemacht – zum Hinterfragen des Ist-Standes. Die Beschäftigung mit der Materie ist eine gute Gelegenheit, den Vergleich mit dem Stand der Technik und den Vorgaben der Sicherheitsrichtlinien zu führen.

Letztere sind im Unternehmen zu definieren und schriftlich festzuhalten. Auch sie sind einfach und praktikabel zu gestalten. Man beginnt mit den grundsätzlichen, naheliegenden Richtlinien, wie: Umgang mit Passwörtern, Datenträgern, Mailanhängen, Beginn und Beendigung eines Beschäftigungsverhältnisses, Meldung von Auffälligkeiten.

Sicherheitsrichtlinien orientieren sich an der Gefährdungs- und Risikoanalyse der Unternehmensprozesse. Welche Szenarien bedrohen die Geschäftsfähigkeit des Unternehmens? Was sind die schwächsten Glieder in den jeweiligen Prozessketten? Die Einbeziehung von Mitarbeitern aus den Prozessen in diese Betrachtungen offenbart, dass gefühlte Sicherheit und Wahrscheinlichkeit von Risiken zwei unterschiedliche Schuhe sind. Stehen Verhaltensregeln dann auf dem Papier, sind sie den Mitarbeitern zu kommunizieren. Bei Richtlinien, die sich technisch durchsetzen lassen, sollte das auch getan werden.

Für den Vergleich mit dem Stand der Technik ist es opportun, sich externe Unterstützung ins Haus zu holen und Expertenwissen gezielt zu nutzen. Im Ergebnis dessen sind die technischen und organisatorischen Lücken in der IT-Sicherheit und dem Datenschutz zu schließen. Höchste Priorität haben die Maßnahmen zur Eindämmung der größten Risiken. Wer dabei aus abstrahierten Grundsätzen wiederholbare, konkrete Lösungen schafft, wird außerdem seine IT-Umgebung konsolidieren, vereinheitlichen und damit einfacher und überschaubarer machen können.

Neben dem Tagesgeschäft führen Szenarien wie die Nicht-Erreichbarkeit der Unternehmens-IT für Stunden oder das Kompromittieren personenbezogener Daten zum Nachdenken über Eskalationsprozeduren und Notfallmanagement. Die entsprechende Notfall-Richtlinie fordert (hoffentlich) eine Kommunikationsstrategie ein, die auf Transparenz, Offenheit und Verantwortung basiert.

Mitarbeiter sensibilisieren

Es klingt banal. Aber neben Dokumentation und technischen Maßnahmen besteht die größte Herausforderung darin, Mitarbeiter zu sensibilisieren, zu schulen und zu Aktivposten zu entwickeln aber auch zum Datengeheimnis zu verpflichten. Mitarbeiter werden wesentlich von der Unternehmenskultur geprägt. Die Etablierung der allgemeinen Grundsätze für IT-Sicherheit und Datenschutz: Security by Design, by Obscurity, by Default und by Himself in die Unternehmens-DNA ist das Gebot zum Bestehen in einer digitalisierten Welt (Tab. 2).

IT-Sicherheit und Datenschutz bedeuten, Ordnung und Struktur für alle Mitarbeiter zu schaffen. Das ist ein fortlaufender Prozess, für den DSGVO und IT-Sicherheitsgesetz spätestens jetzt ein Initial sein sollten. Nur der Fokus auf praktische Schritte wird zur Compliance mit Security-Standards führen. Nicht umgekehrt.

Der Geschäftsbereich Systemintegration der Zedas GmbH unterstützt Unternehmen bei dieser Aufgabe seit vielen Jahren. Langjährige Erfahrungen aus Kundenprojekten und als Software-as-a-Service-Dienstleister sowie der ganzheitliche Ansatz bei IT-Sicherheit und Datenschutz waren und sind Basis für eine erfolgreiche Zusammenarbeit.

Zusammenfassung/Summary

IT-Sicherheit und Datenschutz

Digitalisierung zur Effizienzsteigerung und Kostensenkung geht einher mit der Notwendigkeit, bisher unbekannte Prozesse, Technologien und Gefahren zu beherrschen. Die Gesetze und Verordnungen erzeugen lediglich den Druck auf etwas, was eigentlich selbstverständlich sein müsste – der Schutz und verantwortungsvolle Umgang mit Eigentum. Wer also personenbezogene Daten speichert und verarbeitet, wer digitale Prozesse in seinem Unternehmen einführt, hat eine Management-Aufgabe: die Balance zwischen IT-Nutzen und -Sicherheit herzustellen. IT-Sicherheit und Datenschutz bedeuten, Ordnung und Struktur für alle Mitarbeiter zu schaffen. Das ist ein fortlaufender Prozess, für den DSGVO und IT-Sicherheitsgesetz ein Initial sein sollten. Nur der Fokus auf praktische Schritte wird zur Compliance mit Security-Standards führen, nicht umgekehrt.

IT security and privacy protection

Digitalization to increase efficiency and reduce costs goes hand in hand with the need to master yet unknown processes, technologies and threats. The laws and regulations merely create pressure on something that should be self-evident – the protection and responsible handling of property. Therefore whoever stores and processes personal data, who introduces digital processes in his company, has a management task: to balance between IT benefit and security. IT security and privacy mean creating order and structure for all employees. This is an ongoing process for which DSGVO and IT Security Act should be an initial. Only focus on practical steps will lead to compliance with security standards. Not the other way around!