Es ist 5 vor 12 für die Umsetzung der GDPR-Vorgaben

Die GDPR (DSGVO/Datenschutz-Grundverordnung) tritt am 25. Mai 2018 europaweit in Kraft. Sie regelt EU-weit die einheitliche Verarbeitung von personenbezogenen Daten. Was dies für Schweizer Unternehmen bedeutet und wie man bei der Umsetzung vorgehen soll, erfahren Sie in diesem Artikel.

In der heutigen vernetzten Zeit werden personenbezogene Daten mit einer unglaublichen Geschwindigkeit gesammelt, verarbeitet und genutzt. Diese gilt es zu schützen – und dies regelt die GDPR. Im Vordergrund stehen dabei der Schutz der Personen in der EU bei der bei der Sammlung und Verarbeitung persönlicher Daten. Obwohl die Schweiz nicht in der EU ist, haben die neuen Richtlinien auch einen grossen Einfluss auf Schweizer Unternehmen – aufgrund der extraterritorialen Wirkung. Denn die GDPR gilt für alle Unternehmen in der EU – nicht nur jene, die innerhalb der EU wirtschaften, sondern auch solche mit Angestellten aus der EU oder solche, die Daten aus oder in der EU verarbeiten.

Aber wie findet man diese Daten? Typischerweise sind sie in zahlreichen unstrukturierten Office-Dokumenten auf Servern, in Cloud Services und strukturiert in ERP/CRM-Systemen abgelegt. Hier den Überblick zu behalten, ist eine schwierige Herausforderung. Trotzdem ist es unerlässlich, alle personenbezogenen Daten zu identifizieren und anschliessend auf dieser Basis Schutzmassnahmen abzuleiten.

4 wichtige Aspekte für die GDPR-readiness:

- **Datenklassifizierung:** Unternehmen müssen wissen, wo in ihren Systemen welche Arten von Daten gespeichert sind – insbesondere in strukturierter und unstrukturierter Form, die in Dokumenten und Tabellen vorkommen. Das ist wichtig, um die Daten angemessen zu schützen, aber auch, um Anträgen zur Berichtigung und Löschung von personenbezogenen Daten nachzukommen.

- **Metadaten:** Es gilt, die Datenaufbewahrung zu beschränken. Daher braucht man grundlegende Informationen, wann und für welchen Zweck die Daten erhoben und bearbeitet wurden. Personenbezogene Daten, die auf IT-Systemen liegen, müssen regelmässig überprüft und über ihre weitere Speicherung, Aufbewahrung oder Löschung entschieden werden.

- **Governance:** Da Datenschutz («Privacy by Design» und «Privacy by Default») von der GDPR gefordert ist, sollten sich Unternehmen auf die Grundlagen der Data Governance konzentrieren. Bei unstrukturierten Daten beziehen sich diese auf Kenntnisse darüber, wer innerhalb von Systemen und Anwendungen auf personenbezogene Daten zugreifen kann und wer eine Zugriffsberechtigung haben sollte («Need-to-Know»-Prinzip); Zugriffsberechtigungen sind auf die tatsächlich erforderlichen Rollen der Mitarbeitenden einzuschränken; am effizientesten über rollenbasierte Zugriffskontrollen.

- **Überwachung:** Die Anforderung, Verstösse innerhalb von 72 Stunden zu melden, ist eine weitere Belastung für die Datenverantwortlichen. Sie müssen ungewöhnliche Zugriffsmuster auf klassifizierte und personenbezogene Daten erkennen und bei missbräuchlicher Preisgabe an Unberechtigte diese umgehend der zuständigen Aufsichtsbehörde melden. Die Meldung von Verstössen umfasst aber mehr als nur die reine Meldung des Vorfalls. Es gilt auch die Datenkategorien, die davon betroffenen Daten und die ungefähre Anzahl der betroffenen Personen etc. zu melden. Das bedeutet, dass Unternehmen detaillierte Kenntnisse darüber benötigen, was Hacker oder Insider angerichtet haben.

Weniger ist mehr ...

Unser Tipp zur Sicherheit von personenbezogenen Daten lässt sich in einem Wort zusammenfassen: Minimierung! Dies bezieht sich auf die Minimierung beim Sammeln, Erfassen und Verarbeiten von personenbezogenen Daten. Aber auch die Minimierung der Parteien, mit denen Sie Daten teilen oder welche Daten verarbeiten, sowie die Minimierung der Aufbewahrungsdauer sind relevant. Getreu dem Motto: Weniger ist mehr ...

Autor:
Markus Limacher
ist Head of Security Consulting, InfoGuard AG

InfoGuard
SWISS CYBER SECURITY

InfoGuard AG
Lindenstrasse 10
6340 Baar
www.infoguard.ch