CYBER EU-Datenschutz

Neue Pflichten durch EU-Datenschutz (DSGVO)

Seit dem 25. Mai 2018 ist die neue Europäische Datenschutz-Grundverordnung in Kraft. Diese Richtlinien können auch Schweizer Unternehmen betreffen.
Die Europäische Datenschutz-Grundverordnung (DSGVO) verschärft die Gesetzgebung im Bereich des Datenschutzes in der ganzen EU. Sie enthält zahlreiche neue Pflichten. Betroffen sind nicht nur EU-Unternehmen, sondern auch solche in der Schweiz.

Betroffene Schweizer Unternehmen

Betroffen ist eine Firma dann, wenn sie Waren oder Dienstleistungen an Personen in der EU anbietet, oder wenn das Verhalten von Personen innerhalb der EU beobachtet wird. Deshalb können sich aus diesen Richtlinien auch für Unternehmen mit Sitz in der Schweiz rechtliche Konsequenzen ergeben.

Verschärfte Sanktionen

Die Verordnung sieht zahlreiche neue Dokumentations- und Nachweispflichten vor. Ausserdem können Unternehmen neu dazu verpflichtet sein, einen Datenschutzbeauftragten einzusetzen. Die Rechte der betroffenen Privatpersonen werden ausgebaut und zusätzlich verschiedene organisatorische, technische oder administrative Pflichten neu eingeführt. Werden die Datenschutzvorschriften verletzt, kommen verschärfte Sanktionen zum Zug. Schlimmstenfalls droht einem Unternehmen eine Busse in Höhe von EUR 40 Mio. oder 4% des globalen Jahresumsatzes.

Meldepflicht und Meldefrist

Unternehmen müssen im Fall einer Verletzung der Datensicherheit, insbesondere bei einem Hackerangriff innerhalb von 72 Stunden eine Meldung an die zuständige Datenschutzbehörde machen. Je nach Umständen müssen betroffene Personen, deren Daten gestohlenen wurden, direkt informierten.

Bussen

Bussen werden nur verhängt, wenn ein Cyberangriff nicht innerhalb von 72 Stunden bei der Datenschutzbehörde gemeldet wird.

CYBER Attacken

Betroffen sind alle Unternehmen

Unabhängig von Datenschutzverletzungen mit der EU, sind sämtliche Unternehmen Cyberattacken ausgesetzt. Alle Unternehmen sollten sich vor Angriffen schützen und Massnahmen treffen.

Viren

Dies sind selbst verbreitende Programme und stellen eine hohe Gefahr dar. Sie können Hardware, Betriebssysteme und andere Software beeinflussen.

Spam-E-Mails

Unerwünschte E-Mails und werden sehr oft für kriminelle Zwecke verwendet, wie zum Beispiel für die Verbreitung von Viren.

Phishing-E-Mails

Solche Mails werden von Absendenden mit falscher Identität verschickt, die sich vertrauliche Daten beschaffen wollen.

Trojaner

Schadprogramme und richten oft unerkannt im Hintergrund Schaden an oder sammeln heimlich Daten.

DDOS (Distributed Denial of Service-Attacken)

Service-Attacken setzen auf Quantität. Bei diesem Vorgehen werden Angriffe in hoher Zahl auf ein IT-System, in Form von sehr vielen Anfragen zur gleichen Zeit gestartet, um einen Service oder eine Webseite lahmzulegen.

Social Engineering

Hier handelt es sich um eine Telefonmasche, bei der persönliche Angaben wie eine Telefonnummer genutzt werden, um an vertrauliche Daten zu gelangen und diese zur persönlichen (meist finanziellen) Bereicherung zu verwenden. Ein Anruf, bei dem Ihnen ein Computerservice angeboten wird, der die Herausgabe Ihrer Zugangsdaten verlangt, kann ein solcher betrügerischer Anruf sein.

Hacking

Das Hacking ist ein nicht autorisierter Zugriff auf Rechner oder auf ein ganzes Netzwerk, um an Informationen, respektive Daten zu gelangen. Die Daten können anschliessend zur Erpressung genutzt werden.

CYBER Virenbefall

Wichtige Sofortmassnahmen nach einem Virenbefall

Nachdem ein Antivirenprogramm Schadsoftware auf dem PC gefunden hat, ist es ratsam, den Rechner neu aufzusetzen, da niemand zweifelsfrei nachvollziehen kann, welche Auswirkungen das Schadprogramm auf den PC hat und ob es restlos durch das Antivirenprogramm gelöscht werden konnte.

Ruhe bewahren und Überblick verschaffen

Nach einen Cyberangriff müssen Sie Ruhe bewahren und zuerst einen Überblick verschaffen!
Informieren Sie dann die IT-Abteilung oder Ihr IT-Anbieter.

Netzwerk- und WLAN-Verbindung trennen

Trennen Sie als das Netzwerkkabel zu Ihrem PC oder Server. Falls vorhanden deaktivieren Sie das WLAN. Sofern Sie alleine Ihr WLAN nutzen, schalten Sie den WLAN-Router komplett aus.

Passwörter löschen

Nicht selten sind Viren und Trojaner auch dazu bestimmt, fremde Passwörter und Zugänge zu anderen Systemen wie E-Mail zu erschleichen. Ändern Sie nach Möglichkeit kurzfristig Ihre wichtigen Passwörter.

Datensicherung (Rettung Ihrer persönlichen Dateien)

Das Rettungssystem ermöglicht meist eine Datensicherung von wichtigen persönlichen Daten. Diese speichern Sie zunächst auf einen USB-Stick oder ein anderes externes Medium. Um eine Infektion dieser Sicherung auszuschliessen, sollten Sie sie mit zwei verschiedenen Virenscannern untersuchen.

Festplatte komplett löschen

Nun geht es darum, Ihren PC für die weitere Nutzung komplett von der Schadsoftware zu befreien. Trotz der Entfernung des Computervirus und Negativmeldung des Virenschutzprogramms können Reste auf Ihrer Festplatte verblieben. Um die Malware komplett zu entfernen, muss die Festplatte vollständig gelöscht werden.

Neuinstallation des Betriebssystems

Nun können Sie das Betriebssystem von einem Installationsmedium, meist der Original-CD des Herstellers, auf die leere Festplatte installieren. Ein selbst erstelltes Installationsmedium, auf dem schon Updates des Betriebssystems eingebunden sind, erfüllt diese Zwecke ebenfalls. Nach dem Start der CD läuft die Installation meist selbstständig ab.

CYBER Prävention

Unternehmen und Mitarbeitende schützen?

Cyberkriminalität wie Hacking, Malware oder auch menschliches Versagen kann jedes Unternehmen treffen.

Schulungen

Unternehmen müssen die Mitarbeitenden schulen, um die IT-Sicherheit zu erhöhen. Das Ziel ist die Aufmerksamkeit zu schärfen und Anwendungsfehler zu vermeiden, um Cyber-Angriffe zu verhindern oder zumindest zu reduzieren.

IT-Kommunikation

Mit einer skeptischen Grundeinstellung gegenüber der Herkunft vom Mitteilungen aus dem Internet, E-Mails und anderen elektronischen Kommunikationskanälen.

IT-Infrastruktur

Für das Unternehmen ist die Grundlage eine angemessene IT-Sicherheitsinfrastruktur, die kontinuierlich zu überprüfen ist und gegebenenfalls zu aktualisieren.

Software-Updates

Halten Sie das Betriebssystem und Software immer auf dem neusten Stand.

Antivirusprogramm

Ein Antivirenprogramm hat zwei Hauptaufgaben: Es scannen zunächst den PC auf schädliche Programme und versucht bei einem Befall den PC zu säubern. Die zweite Aufgabe besteht darin, den PC permanent gegen Gefahren durch Schadprogramme zu schützen.

IT Room Security

Der Zugang zu spezifischen IT-Räumlichkeiten und Endgeräten ist mit einer Authentifizierung, wie beispielsweise einem Passwort, Zertifikat oder einem Fingerabdruck ausgestattet sein.

CYBER Versicherung

Cyber-Versicherung schützt Sie vor:

Drittschäden

Die Haftpflicht deckt Drittschäden für Vermögensschäden infolge Informationssicherheitsverletzung.

- → Datenverlust
- → Unerlaubter Eingriff in IT-Systeme (Hacking)
- → Verletzung von Schutzrechten
- → Verletzung des Datenschutzes oder der Geheimhaltungspflicht
- → Verletzungen von PCI-Datensicherheitsstandards

Eigenschäden

Deckt Eigenschäden des Versicherungsnehmers.

- → Entfernung von Schadsoftware sowie Wiederherstellung und Wiederbeschaffung von elektronischen Daten und Programmen (Software)
- → Mehrkosten wie Überstunden Ihrer Mitarbeitenden
- → Elektronischer Zahlungsverkehr
- → Versand von Waren
- → Ertragsausfall infolge Betriebsunterbruch Haftzeit während 2 Jahren
- → Cyber-Erpressung

Assistance

Sie werden im Schadenfall begleitet und erhalten Unterstützung bis der Schaden ausgestanden ist.

- → Kosten zur Ermittlung der Ursache
- → Kosten im Zusammenhang mit der Verletzung von Datenschutz und der Geheimhaltungspflicht
- → Reputationsmassnahmen und Krisenmanagement
- → Rechtsschutz bei behördlichen Verfahren