Alert

Breaking News
von Blum & Grob

Zürich, Februar 2023

Der Einfluss des revidierten Datenschutzgesetzes auf die Cybersecurity – Guidelines für Sie.

Ransomware, Distributed Denial of Service, Datenabfluss, Social Engineering, Phishing, etc. - die Anzahl von Cyberangriffen wächst in der Schweiz kontinuierlich. Innerhalb des letzten Jahres wurden 35'000 Cyberangriffe gemeldet. Das Nationale Zentrum für Cybersicherheit (NCSC) zählte 2021 noch 21'000 Meldungen, dabei waren es schon doppelt so viele Vorfälle wie im Jahr davor.

Diese Zahlen stellen nur die Spitze des Eisbergs dar. Die Dunkelziffer dürfte viel höher sein. Die Cyberangriffe richten sich nicht mehr nur gegen die grossen Konzerne. Im Gegenteil, die Hacker setzen auf Quantität, werfen ihre Netze breit aus und peilen gezielt die KMUs an.

Die neue Masche der Hacker ist die Dreifach-Erpressung: Erstens Daten stehlen und/oder verschlüsseln und so das Unternehmen komplett blockieren; zweitens damit drohen, die gestohlenen, sensiblen Daten zu veröffentlichen; und drittens die gestohlenen Daten analysieren, um damit Personen zu erpressen, die darin vorkommen. Mit dem revidierten Datenschutzgesetz werden Unternehmen auch diesbezüglich noch mehr in die Pflicht genommen. Wir zeigen Ihnen, was Sie beachten müssen.

Was bedeutet ein Cyberangriff für mein Unternehmen?

- Produktionsausfall / Umsatzeinbussen bzw. -ausfall
- Imageschaden, Vertrauensverlust (Kunden / Mitarbeiter)
- Zugang zu Geschäftsgeheimnissen
- Haftung für Schäden gegenüber den Kunden / Mitarbeitenden / Lieferanten
- Strafrechtliche Verantwortung

Kann ich mich als Opfer einer Cyberattacke strafbar machen?

Gemäss dem revidiertem Datenschutzrecht ab dem 1. September 2023 kann die verantwortliche **natürliche Person im Unternehmen** mit einer **Busse bis zu CHF 250'000** bestraft werden, wenn sie vorsätzlich die Mindestanforderungen an die Datensicherheit nicht einhält. Zusätzlich besteht ein Haftungsrisiko insbesondere gegenüber Kunden.

Es gibt aber noch weitere Strafbestimmungen, die zum Tragen kommen können, wie beispielsweise:

- Verletzung einer beruflichen Schweigepflicht
- Unzulässige Auftragsdatenbearbeitung (Übertragung der Personendatenbearbeitung an einen Auftragsbearbeiter ohne Einhaltung der Vorschriften)
- Unzulässige Personendatenübermittlung ins Ausland.

Mit dem neuen Datenschutzrecht gibt es für Unternehmen also Handlungsbedarf. Bis am 1. September 2023 müssen die nötigen Massnahmen umgesetzt sein.

Was nun? Was kann ich vorkehren? Ein paar Beispiele:

1. **Datensicherheit durch technische und organisatorische Massnahmen**

Die Unternehmen müssen das eigene Risiko bestimmen und angemessene technische und organisatorische Massnahmen festlegen und einführen, z.B. Implementierung des «need-to-know» Prinzips, Zugangsbeschränkungen, Firewalls, Virenprüfung, Backups, Weisungen, Schulungen der Mitarbeitenden (häufigste Methode der Cyberkriminellen ist das Social Engineering über Angestellte).

2. **Übersicht über die Datenbearbeitungen im Unternehmen erstellen und pflegen**

Zwar ist ein sog. Bearbeitungsverzeichnis erst für Unternehmen Pflicht, die 250 und mehr Mitarbeitende beschäftigen sowie für Unternehmen, die besonders schützenswerte Personendaten in grossem Umfang bearbeiten oder ein Profiling mit hohem Risiko durchführen. Ein Bearbeitungsverzeichnis oder eine Übersicht, welche Personendaten wo bearbeitet werden, ist für jedes Unternehmen empfehlenswert, denn es ermöglicht **Kontrolle** über die datenschutzrelevanten Prozesse im Unternehmen **(*Data Governance*)**.

So erhalten Unternehmen eine Übersicht über ihre Datenbearbeitungen und können beispielsweise klären, ob Dritte Zugang zu Personendaten haben (z.B. IT-Provider), oder Personendaten extern, allenfalls im Ausland, gespeichert

werden (Cloud-basierte Programme). Beides gilt als Auftragsbearbeitung und setzt eine besondere Vereinbarung voraus. Der Beizug von Auftragsbearbeitern oder die Übermittlung ins Ausland muss sodann in Datenschutzerklärungen offengelegt werden.

3. Schriftliche Vereinbarungen über die Auftragsdatenbearbeitung

Um das Risiko einer oben erwähnten Busse zu minimieren, lohnt es sich, die Vereinbarungen mit den Dienstleistern schriftlich festzuhalten und die respektiven Pflichten der Auftragsbearbeiter, Kontroll- und Weisungsrechte des verantwortlichen Unternehmens sowie Rechte der allfälligen natürlichen betroffenen Personen festzulegen.

4. Bewertung der Übermittlungen der Personendaten ins Ausland

Übermittlungen der Personendaten ins Ausland setzen einen angemessenen Schutz im Empfängerstaat voraus. Gewähren das die Gesetze im betreffenden Land nicht, bedarf es zusätzlicher Schutzmassnahmen, beispielsweise besondere Datenschutzklauseln in einem Vertrag. Gegenwärtig existiert gemäss dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in folgenden Staaten ein angemessenes Datenschutzniveau: EU, EWR, UK, Kanada, Argentinien, Israel und Neuseeland. Ein Personendatentransfer aus der Schweiz in andere Staaten, wie z.B. USA, China, Indien, etc., erfordert demnach weitere Schutzmassnahmen. Das können z.B. vom EDÖB anerkannte Datenschutzklauseln in Verträgen sein. Je nach Land bedarf es aber auch zusätzlicher technischer Massnahmen, z.B. Verschlüsselung, damit die Personendaten im Ausland nicht gelesen werden können.

5. Implementierung von *Privacy by Design and by Default*

Personendaten dürfen nur für den Zweck bearbeitet werden, zu dem sie beschafft worden sind. Weiter ist zu prüfen, wer in einem Unternehmen überhaupt Zugang zu Personendaten benötigt (z.B. Arbeitnehmerdaten aber auch Kundendaten). Zu welchen Zwecken Personendaten bearbeitet werden dürfen und von wem, ist daher im Unternehmen zu regeln. Diese Grundsätze sind bei der Gestaltung der Prozesse im Unternehmen und bei der Entwicklung und/oder Implementierung der IT-Produkte und -Systeme zwingend zu berücksichtigen.

6. Erstellen und Implementieren eines Prozesses bei Datenschutzverletzungen (*Data Breach*) inkl. Meldungen an den EDÖB

Gelangen Personendaten in falsche Hände, besteht eine Meldepflicht an den EDÖB und betroffene Personen. Nur in Ausnahmefällen kann auf eine Meldung verzichtet werden. Die Meldung an den EDÖB hat so rasch als möglich zu erfolgen. Wie man auf einen Cyberangriff reagiert, muss nur schon aus diesem Grund vorbereitet sein.

7. Datenschutzberaterin oder -berater

Die Ernennung eines unabhängigen Datenschutzberaters ist keine Pflicht, aber empfehlenswert, denn klare Zuständigkeiten bedeuten effiziente Entscheidungswege. Die Funktion kann intern oder extern besetzt sein.

Setzen Sie die Anforderungen des revidierten Datenschutzgesetzes zeitgerecht um und steigern Sie damit gleichzeitig Ihre IT-Sicherheit im Unternehmen.

Gerne erläutern wir Ihnen die Details dazu und machen Sie auf weitere neue Pflichten gemäss dem revidierten Schweizer Datenschutzrecht aufmerksam. Wir zeigen Ihnen auf, wie Sie rasch und mit möglichst wenig Aufwand compliant werden.

Ihr Blum&Grob Datenschutz-Team

David Schwaninger, d.schwaninger@blumgrob.ch
André Wahrenberger, a.wahrenberger@blumgrob.ch
Giedre Neverauskas, g.neverauskas@blumgrob.ch