Cyberangriffe – Datenschutzrechtliche Pflichten und wie vorbeugen

Cyberangriffe gehören mittlerweile unabhängig von Branche oder Unternehmensgrösse zum Unternehmensalltag. Organisationen müssen daher nicht nur technische und organisatorische Massnahmen (TOM) gewährleisten (Art. 8 DSG), sondern auch im Ernstfall schnell und rechtskonform reagieren. Der folgende Beitrag zeigt die zentralen datenschutzrechtlichen Pflichten bei Cyberangriffen und skizziert wirksame Präventionsansätze.

Von Lukas Lezzi, Alexandra Egger

Meldepflichten bei Verletzungen der Datensicherheit

Für Datensicherheitsverletzungen (gemäss Art. 24 DSG) besteht eine Meldepflicht, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen. Die Eintrittswahrscheinlichkeit, die Sensibilität und die Schwere der befürchteten Folgen sind beispielhafte Beurteilungskriterien.

Meldepflicht an den EDÖB

Der Verantwortliche muss den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) so rasch wie möglich über die Verletzung informieren. Besteht nach erster Einschätzung ein hohes Risiko für die betroffenen Person, wird die Meldung umso dringlicher. Insbesondere bei einer hohen Anzahl von betroffenen Personen soll mit der Meldung nicht weiter zugewartet werden.

Die Meldung muss folgende Informationen enthalten:

- Art der Verletzung
- wahrscheinliche Folgen
- ergriffene oder geplante Massnahmen
- Kontaktstelle für Rückfragen

Auftragsbearbeiter, also z.B. externe Buchhaltungsfirmen, welche im Auftrag des Verantwortlichen Personendaten bearbeiten, müssen den Verantwortlichen bei einer Verletzung der Datensicherheit so rasch als möglich informieren.

Die folgende Risikomatrix gibt Aufschluss darüber, ob die Verletzung der Datensicherheit an den EDÖB gemeldet werden muss und ob die betroffenen Personen benachrichtigt werden müssen (siehe unten stehende Tabelle).

Informationspflicht gegenüber betroffenen Personen

Ist der Schutz der betroffenen Person erforderlich, muss diese ebenfalls informiertdwerden. Die Information muss klar, verständlich und zeitnah erfolgen, damit sie geeignete Schutzmassnahmen treffen kann (z.B. Passwortänderungen, Sperren von Konten). Die Betroffenen sollen achtsam sein und Unregelmässigkeiten bei einer zuständigen Kontaktperson intern melden. In dringenden Fällen (z.B. unmittelbarer Schaden oder akute Bedrohung) können sich Betroffene auch direkt an die Polizei oder das Nationales Zentrum für Cybersicherheit (NCSC) wenden (www.ncsc.admin.ch).

Eine Ausnahme der Information gegenüber den betroffenen Personen besteht, wenn durch eine Information die laufende Untersuchung gefährdet würde, wenn diese nur mit unverhältnismässigem Aufwand möglich wäre (z.B. betroffene Person ist nicht auffindbar) oder wenn die Information durch eine öffentliche Bekanntgabe sichergestellt werden kann.

Schweregrad/ Wahrscheinlichkeit	Selten	Unwahrscheinlich	Möglicherweise	Wahrscheinlich	Fast Sicher
Unbedeutend	Niedrig	Niedrig	Niedrig	Niedrig	Mittel
Kleinere	Niedrig	Niedrig	Niedrig	Mittel	Mittel
Mässig	Niedrig	Niedrig	Mittel	Mittel	Mittel
Bedeutend	Mittel	Mittel	Hoch	Hoch	Hoch
Extrem	Hoch	Hoch	Hoch	Hoch	Hoch

Niedriges Risiko = Keine Melde- oder Anzeigepflicht
Mittleres Risiko = In der Regel Meldepflicht an den EDÖB.
Hohes Risiko = Meldung an den EDÖB und Information der betroffenen Personen

Weitere Meldepflichten

Abhängig von allfälligen Bewilligungen oder Geschäftsfeldern des Verantwortlichen können noch weitere Meldepflichten bei einem Cyberangriff vorliegen. Insbesondere sind hier zu erwähnen:

- Meldung beim Bundesamt für Cybersicherheit (BACS) innerhalb von 24 h bei Angriffen auf kritische Infrastrukturen gemäss Art. 74a ff. Informationssicherheitsgesetz
- Meldung innerhalb von 24 h bei der FINMA bei Angriffen auf Personen, welche eine Bewilligung nach dem Finanzmarktaufsichtsgesetz haben **(ACHTUNG:** Frist läuft hier ab dem Beginn des Angriffs und nicht erst ab Kenntnisnahme des Bewilligungsträgers)

Vorgehen im Ernstfall: Incident Response nach DSG

Eine gut geübte Reaktionsstrategie ist entscheidend, um Schäden zu begrenzen und gesetzliche Vorgaben einzuhalten. Bei einem Datenschutzvorfall sind folgende Schritte zu befolgen:

- Identifikation: Erkennen des Vorfalls (z.B. durch Monitoring)
- Eindämmung: Nach der Identifikation eines Angriffs müssen umgehend Massnahmen ergriffen werden, um die Aktivität des Angriffs sofort zu stoppen und die Situation zu stabilisieren, damit keine weiteren Angriffe folgen. Dazu gehören:
  1. kurzfristige Eindämmungsmassnahmen wie die Trennung betroffener Systeme vom Netzwerk, Sperren kompromittierter Benutzerkonten, Blockieren schädlichen Datenverkehrs sowie Unterbinden von Remote-Zugriffen
  2. Stabilisierungsmassnahmen wie Wechsel privilegierter Passwörter, Aktivieren zusätzlicher Monitoring- und Logging-Funktionen sowie Segmentierung oder Isolation betroffener Bereiche
- Weiter muss das Risiko bewertet werden, um einzuschätzen, ob eine meldepflichtige Verletzung im Sinne von Art. 24 DSG vorliegt. Dabei sollten interne oder externe Datenschutzexperten und IT-Sicherheitsverantwortliche involviert werden.
- Falls nötig, muss eine Meldung an EDÖB und die Betroffenen erfolgen (innert angemessener Frist und mit den gesetzlich geforderten Inhalten).
- Alle vorgenommenen Schritte müssen lückenlos dokumentiert werden.
- Wiederherstellung und Analyse: Nach der Eindämmung werden die betroffenen Systeme bereinigt und wiederhergestellt, damit der Betrieb sicher weiterlaufen kann. Anschliessend wird der Vorfall analysiert, um die Ursache zu bestimmen und Sicherheitsmassnahmen gezielt zu verbessern.

Präventionsstrategien: Cybersecurity als dauerhafter Prozess

Der effektivste Schutz vor datenschutzrechtlichen und wirtschaftlichen Schäden liegt in präventiven Massnahmen. Die folgenden Punkte gelten als Best Practices:

- Zero-Trust-Architektur: Es sind starke Authentifizierungsverfahren, fein granulierte Berechtigungen und laufende Überprüfung von Zugriffsrechten vorzunehmen.
- regelmässige Penetrationstests und Schwachstellenanalysen: Wiederkehrende technische Tests helfen, Sicherheitslücken zu erkennen, bevor Angreifer sie ausnutzen können. So können Unternehmen nachweisen, dass sie den «Stand der Technik» berücksichtigen und Risiken aktiv reduzieren.
- kontinuierliches Awareness-Training: Schulungen zu Social Engineering, Phishing und sicherem Umgang mit Daten sind zentrale organisatorische Massnahmen, welche das Risiko von Vorfällen erheblich senken.
- Notfallübungen: Durch realistische Übungen werden Incident-Response-Abläufe, Meldeprozesse und interne Kommunikationswege getestet, damit die Unternehmung im Ernstfall weiss, was zu tun ist.

Fazit

Das Datenschutzgesetz zwingt Unternehmen, Cybersecurity strukturiert und regelmässig zu adressieren. Cyberangriffe lassen sich kaum vollständig verhindern, doch die rechtlich geforderte Kombination aus angemessenen Schutzmassnahmen, klaren Prozessen und schneller Reaktion reduziert Risiken erheblich. Unternehmen, die Prävention ernst nehmen, erfüllen nicht nur ihre gesetzlichen Pflichten, sondern stärken auch das Vertrauen ihrer Kunden und Geschäftspartner.

PRAXISBEISPIELE

Beispiele von Cyberangriffen

Beispiel 1: Angriff über unsichere WLAN-Verbindung

Ein Mitarbeiter verbindet sich unterwegs über ein öffentliches WLAN mit dem Firmennetzwerk. Ein Angreifer hat dort einen «Fake-Hotspot» eingerichtet und liest den Datenverkehr mit. Dadurch erhält er Zugang zu Log-in-Daten und sensiblen Firmeninformationen, ohne dass der Mitarbeiter etwas merkt.

Beispiel 2: Phishing-E-Mail

Ein Mitarbeiter erhält eine scheinbar legitime E-Mail von «Microsoft», die zur Passworterneuerung auffordert. Der Link führt jedoch zu einer gefälschten Log-in-Seite. Nach Eingabe des Passworts erhalten die Angreifer Zugang zum Firmenkonto und können interne Daten stehlen.

Beispiel 3: Website gehackt

Ein Webmaster aktualisiert wie gewohnt die Firmenwebsite, ohne zu wissen, dass sein Computer mit einem Trojaner infiziert ist. Beim FTP-Log-in werden seine Zugangsdaten mitgelesen und an Kriminelle übertragen. Diese übernehmen die Webseite, verändern Inhalte und platzieren schädliche Dateien. Erst durch Warnmeldungen von Kunden wird der Angriff bemerkt.

AUTOREN

Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.

Alexandra Egger arbeitet als Juristin bei LezziLegal. Sie arbeitet hauptsächlich im Bereich des Datenschutzrechts.