PRAXISFRAGE

DATENSCHUTZ & CYBERSICHERHEIT

Cyberangriff im Schweizer Konzern mit deutscher Tochter: Welche Meldepflichten bestehen?

Ein Schweizer Unternehmen mit einer Tochtergesellschaft in Deutschland wird Opfer eines Cyberangriffs. Unbekannte verschaffen sich Zugang zu den zentral verwalteten IT-Systemen. Neben internen Geschäftsinformationen sind möglicherweise auch Kunden- und Mitarbeiterdaten der deutschen Gesellschaft betroffen. Noch ist unklar, ob Daten tatsächlich abgeflossen sind und welchen Umfang der Angriff hat.

Welche Meldepflichten bestehen in Deutschland und in der Schweiz? Wer ist innerhalb der Unternehmensgruppe verantwortlich und welche Fristen müssen eingehalten werden?

KURZANTWORT

Ein Cyberangriff kann sowohl in Deutschland als auch in der Schweiz unterschiedliche Meldepflichten auslösen. Entscheidend sind die Art des Vorfalls, die betroffenen Daten und die gesetzlichen Pflichten der jeweiligen Gesellschaft. Auch bei zentral verwalteter IT muss jede Konzerngesellschaft prüfen, welche Meldepflichten sie selbst treffen.

1. DEUTSCHLAND: MELDEPFLICHTEN NACH DER DSGVO

Wann muss ein Cyberangriff gemeldet werden?

Nach Art. 33 DSGVO muss der Verantwortliche, also die Person, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, eine Datenschutzverletzung der zuständigen Aufsichtsbehörde melden, sofern diese voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Eine Datenschutzverletzung ist nicht nur gegeben, wenn personenbezogene Daten gestohlen werden. Auch deren unbefugte Veränderung, Löschung oder der Verlust ihrer Verfügbarkeit können eine Datenschutzverletzung darstellen.

Allerdings ist nicht jeder Cyberangriff automatisch meldepflichtig. Entscheidend ist, ob personenbezogene Daten betroffen sind und die Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Sind ausschliesslich technische Systeme oder Geschäftsgeheimnisse betroffen, ohne dass personenbezogene Daten beeinträchtigt werden, besteht keine Meldepflicht nach Art. 33 DSGVO.

Welche Frist gilt?

Die Meldung muss unverzüglich und möglichst innerhalb von 72 Stunden erfolgen, nachdem der Verantwortliche Kenntnis von der Datenschutzverletzung erlangt hat. Dafür müssen hinreichende Anhaltspunkte vorliegen, dass eine Verletzung des Schutzes personenbezogener Daten eingetreten ist. Der Abschluss der technischen Untersuchungen muss hingegen nicht abgewartet werden. Liegen noch nicht alle erforderlichen Informationen vor, können diese schrittweise nachgereicht werden. Erfolgt die Meldung erst nach Ablauf der 72 Stunden, ist die Verzögerung gegenüber der Aufsichtsbehörde zu begründen.

Müssen auch Kunden und Mitarbeitende informiert werden?

Nach Art. 34 DSGVO müssen betroffene Personen grundsätzlich unverzüglich benachrichtigt werden, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für sie mit sich bringt, etwa durch Identitätsdiebstahl, finanzielle Schäden oder die Offenlegung sensibler persönlicher Informationen.

Ein solches hohes Risiko kann beispielsweise entstehen, wenn sensible Mitarbeiterdaten, Identitätsdokumente oder umfangreiche Kundendaten in unbefugte Hände gelangen.

Eine Benachrichtigung der betroffenen Personen ist jedoch nicht in jedem Fall erforderlich. Sie kann insbesondere entfallen, wenn die Daten durch geeignete technische Massnahmen, etwa eine wirksame Verschlüsselung, geschützt waren oder nachträgliche Massnahmen sicherstellen, dass das hohe Risiko voraussichtlich nicht mehr besteht.

2. DEUTSCHLAND: ZUSÄTZLICHE PFLICHTEN NACH NIS-2

Welche Unternehmen sind betroffen?

Seit Inkrafttreten des deutschen NIS-2-Umsetzungsgesetzes gelten für zahlreiche Unternehmen erweiterte Anforderungen an die Cybersicherheit und zusätzliche Meldepflichten nach dem BSI-Gesetz.

Ob ein Unternehmen betroffen ist, hängt zunächst von seiner Geschäftstätigkeit ab. Erfasst werden bestimmte Unternehmen aus gesetzlich definierten Sektoren, darunter Energie, Verkehr, Gesundheitswesen, digitale Infrastruktur, Maschinenbau und chemische Industrie.

Innerhalb dieser Sektoren unterscheidet das Gesetz zwischen «wichtigen» und «besonders wichtigen Einrichtungen». Massgeblich sind grundsätzlich folgende Grössenschwellen:

- **Wichtige Einrichtungen:** mindestens 50 Mitarbeitende oder ein Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Mio. Euro.
- **Besonders wichtige Einrichtungen:** in bestimmten besonders kritischen Sektoren mindestens 250 Mitarbeitende oder ein Jahresumsatz von über 50 Mio. Euro und eine Jahresbilanzsumme von über 43 Mio. Euro.

Für bestimmte Einrichtungen, etwa Betreiber kritischer Anlagen, gelten Sonderregelungen unabhängig von diesen allgemeinen Grössenschwellen. Die Unterscheidung zwischen wichtigen und besonders wichtigen Einrichtungen wirkt sich insbesondere auf die behördliche Aufsicht und mögliche Sanktionen aus. Die nachfolgend beschriebenen Meldepflichten gelten grundsätzlich für beide Kategorien.

Für Schweizer Unternehmensgruppen besonders relevant: Bei der Berechnung der Grössenschwellen können auch Mitarbeitende und Finanzkennzahlen verbundener Unternehmen einzubeziehen sein. Eine deutsche Tochtergesellschaft kann daher unter die Vorschriften fallen, obwohl sie die Schwellenwerte allein nicht erreicht.

Wann muss ein Sicherheitsvorfall gemeldet werden?

Nicht jeder Cyberangriff löst eine Meldepflicht nach dem BSI-Gesetz aus. Erforderlich ist grundsätzlich ein erheblicher Sicherheitsvorfall. Ein solcher liegt insbesondere vor, wenn der Vorfall schwerwiegende Betriebsstörungen oder erhebliche finanzielle Verluste verursacht oder verursachen kann. Auch wenn andere Personen oder Unternehmen erheblich geschädigt werden können, kann eine Meldepflicht bestehen.

Beispielsweise kann ein Ransomware-Angriff, der die Produktion einer betroffenen Einrichtung für mehrere Tage lahmlegt, einen erheblichen Sicherheitsvorfall darstellen. Ein erfolgloser Angriffsversuch ohne entsprechende Auswirkungen ist dagegen nicht allein deshalb meldepflichtig.

Welche Meldefristen gelten?

Bei einem erheblichen Sicherheitsvorfall sieht § 32 BSI-Gesetz ein gestuftes Meldeverfahren vor:

- **Innerhalb von 24 Stunden nach Kenntniserlangung:** frühe Erstmeldung.
- **Innerhalb von 72 Stunden nach Kenntniserlangung:** ergänzende Meldung mit einer ersten Bewertung des Vorfalls und seiner Auswirkungen.
- **Spätestens einen Monat nach der 72-Stunden-Meldung:** Abschlussmeldung. Dauert der Vorfall noch an, ist zunächst eine Fortschrittsmeldung erforderlich.

Die Meldungen erfolgen an die gemeinsame Meldestelle des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK).

Diese Meldepflichten bestehen unabhängig von den datenschutzrechtlichen Anforderungen der DSGVO. Auch ein erheblicher Sicherheitsvorfall, bei dem keine personenbezogenen Daten betroffen sind, kann daher meldepflichtig sein.

3. SCHWEIZ: WELCHE MELDEPFLICHTEN BESTEHEN?

Meldung nach dem Datenschutzgesetz

Nach Art. 24 des Schweizer Datenschutzgesetzes (DSG) muss der Verantwortliche dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eine Verletzung der Datensicherheit so rasch als möglich melden, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt.

Anders als die DSGVO sieht das Schweizer DSG keine starre 72-Stunden-Frist vor. Massgebend ist die unverzügliche Reaktion unter Berücksichtigung der konkreten Umstände.

Die betroffenen Personen müssen informiert werden, wenn dies zu ihrem Schutz erforderlich ist, beispielsweise damit sie kompromittierte Passwörter ändern oder Kreditkarten sperren können. Der EDÖB kann eine solche Information ebenfalls verlangen, wenn er sie zum Schutz der Betroffenen für notwendig hält.

Zusätzliche Meldepflicht für kritische Infrastrukturen

Seit dem 1. April 2025 besteht in der Schweiz eine gesetzliche Meldepflicht für bestimmte Cyberangriffe auf kritische Infrastrukturen.

Erfasste Betreiber müssen meldepflichtige Cyberangriffe innerhalb von 24 Stunden nach ihrer Entdeckung dem Bundesamt für Cybersicherheit (BACS) melden.

Die Regelung betrifft insbesondere gesetzlich erfasste Organisationen und Betreiber kritischer Infrastrukturen. Sie gilt nicht pauschal für jedes Schweizer Unternehmen.

Können bei der Erstmeldung noch nicht alle erforderlichen Angaben gemacht werden, besteht grundsätzlich eine Frist von 14 Tagen zur Vervollständigung.

4. WER IST INNERHALB DER UNTERNEHMENSGRUPPE VERANTWORTLICH?

Bei grenzüberschreitenden Unternehmensgruppen ist zwischen der technischen Betreuung der IT-Systeme und der rechtlichen Verantwortung zu unterscheiden. Betreibt die Schweizer Muttergesellschaft die IT-Systeme für ihre deutsche Tochtergesellschaft, kommt es insbesondere darauf an, welche Gesellschaft über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

Ist die deutsche Tochtergesellschaft datenschutzrechtlich Verantwortliche, bleibt sie grundsätzlich für die Erfüllung ihrer DSGVO-Pflichten zuständig. Die Schweizer Muttergesellschaft kann daneben eigene Pflichten haben, etwa als eigenständig oder gemeinsam Verantwortliche oder aufgrund des Schweizer Datenschutzrechts.

Ist die Muttergesellschaft lediglich als Auftragsbearbeiterin tätig, muss sie die verantwortliche Gesellschaft über die Datenschutzverletzung informieren. Welche konkreten Pflichten bestehen, richtet sich nach dem jeweils anwendbaren Recht.

Auch die Pflichten nach dem deutschen BSI-Gesetz knüpfen an die jeweils erfasste Einrichtung an. Die konzernweite Organisation der IT führt daher nicht automatisch dazu, dass Meldepflichten auf die Muttergesellschaft übergehen.

Wichtig: Eine Meldung an eine deutsche Datenschutzaufsichtsbehörde ersetzt weder eine gegebenenfalls erforderliche Meldung an das BSI noch eine Meldung an schweizerische Behörden.

PRAXISTIPP FÜR SCHWEIZER UNTERNEHMEN

Unternehmen mit Gesellschaften oder Geschäftstätigkeiten in Deutschland sollten bereits vor einem Sicherheitsvorfall festlegen, wer im Ernstfall welche Aufgaben übernimmt.

Dazu gehört insbesondere:

- Prüfen, welche Gesellschaften unter die DSGVO, das Schweizer DSG oder besondere Cybersicherheitsvorschriften fallen.
- Zuständigkeiten zwischen Konzernleitung, IT, Datenschutz und Geschäftsführung eindeutig festlegen.
- Interne Meldewege und Eskalationsverfahren definieren.
- Sicherstellen, dass auch ausserhalb der üblichen Geschäftszeiten eine fristgerechte Reaktion möglich ist.
- Sicherheitsvorfälle, Risikoabwägungen und getroffene Massnahmen nachvollziehbar dokumentieren.
- Vertragliche Informations- und Meldepflichten gegenüber Kunden, Geschäftspartnern, Dienstleistern und Versicherern identifizieren und in die Incident-Response-Prozesse einbeziehen.



Meldepflichten im Überblick

Rechtsgrundlage	Meldefrist
EU-DSGVO	Möglichst innerhalb von 72 Stunden
Deutsches BSI-Gesetz (NIS-2)	Erstmeldung 24 Std., Folgemeldung 72 Std., Abschlussmeldung grundsätzlich nach einem Monat
Schweizer DSG	So rasch als möglich
Schweizer Informationssicherheitsgesetz	Innerhalb von 24 Stunden

Typische Stolperfallen

- Zu lange abgewartet: Die Meldung wird erst vorbereitet, wenn die technische Untersuchung abgeschlossen ist.
- Nur Datenschutz geprüft: Zusätzliche Meldepflichten nach dem BSI-Gesetz oder Schweizer Informationssicherheitsrecht werden übersehen.
- Zuständigkeiten ungeklärt: Mutter- und Tochtergesellschaft gehen jeweils davon aus, dass die andere Gesellschaft die Meldung übernimmt.
- Datenabfluss als Voraussetzung angesehen: Auch die Verschlüsselung oder der Verlust der Verfügbarkeit personenbezogener Daten kann eine meldepflichtige Datenschutzverletzung darstellen.
- Betroffene Personen vergessen: Die Meldung an eine Behörde ersetzt nicht eine gegebenenfalls erforderliche Benachrichtigung von Kunden oder Mitarbeitenden.



NOCH FRAGEN?
info@vsud.ch
+41 61 375 9500

VSUD-COMMUNITY

Wenden Sie sich an die VSUD – Community
und profitieren Sie vom Erfahrungsaustausch

www.vsud.ch/community