2/2016
25 – 48

DSGVO
„One Stop Shop"-Prinzip
G. Leissler, V. Wolfbauer

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Cybercrime

Praxisfall Cyberangriff – hätten Sie ihn erkannt?
Lars D. Preußer

Die Täter sind professioneller geworden
Interview mit Leopold Löschl

Cyber-Versicherung
Thomas Hubinger

Datenmissbrauch: Ernstfall und Vorbereitung
Rainer Knyrim, Clemens Foisner, Paul Prihoda

In Cybercrime verfangene Domains „einfangen"
Rainer Knyrim, Boris Treml

Checkliste Datensicherheitsmaßnahmen
Hans-Jürgen Pollirer

Mit Standardvertragsklauseln in die Cloud
Rainer Knyrim

Gesetzesbeschwerde
Ernst M. Weiss

ISSN 2313-5409

dako.manz.at

MANZ

P.b.b. Verlag Manz 1230 Wien, Gutheil Schoder Gasse 17

Rainer Knyrim/Clemens Foisner/Paul Prihoda
Rechtsanwalt und Partner Preslmayr Rechtsanwälte/Geschäftsführer bei der SEC Consult Unternehmensberatung/Geschäftsführer bei corporate identity prihoda

Datenmissbrauch: Ernstfall und Vorbereitung

Typische Missbrauchsfälle, Informationspflichten und Medienkommunikation. Ein Datenmissbrauch nimmt keine Rücksicht auf die internen Planungen eines Unternehmens. Eine schnelle sicherheitstechnische Lageeinschätzung durch Experten ist entscheidend, um weiteren Schaden zu verhindern. Mit einer lösungsorientierten Informationspolitik kann ein Imageschaden verhindert werden. Gegenüber den vom Missbrauch betroffenen Dritten gibt es eine Informationspflicht.

Das Datenschutzgesetz verpflichtet private Unternehmen und öffentliche Stellen, alle Betroffenen darüber zu informieren, wenn ein Datenmissbrauch, das ist eine *„systematische und schwerwiegende unrechtmäßige Verwendung von Daten“,* erfolgt ist und den Betroffenen ein Schaden droht. Die Bestimmung des § 24 Abs 2a DSG richtet sich an den Auftraggeber; setzt dieser einen Dienstleiter ein und tritt der Missbrauch bei diesem ein, muss der Dienstleister den Auftraggeber umgehend darüber informieren.

Wie der Missbrauch bekannt wird, dh, ob durch Dritte, eigene Wahrnehmung oder Anschlagen eines EDV-Sicherheitssystems, ist nicht relevant. Nach dem Gesetzeswortlaut reicht es, wenn ein Schaden droht, dh, es reicht die Gefahr eines Schadenseintritts.

Typische Missbrauchsfälle und Vorbeugung dagegen

In der Praxis führen folgende Fälle oft zu Missbrauch:

- Mitarbeiter mailt irrtümlich falsche Dateianhänge an Dritte, oder schickt Inhalte irrtümlich an den falschen Empfänger und der Empfänger spielt diese E-Mail den Medien oder anderen Dritten zu. Hier sollte überlegt werden, die Möglichkeit zur Generierung etwa von Excel-Dateien oder pdfs aus Datenbeständen zentralisierter Datenbanken, die heikle Kundendaten enthalten, zu unterbinden, damit diese nicht später irrtümlich verschickt werden; Anhänge nur mit Passwort verschlüsselt zu verschicken; sicherere Kommunikationswege als bloß unverschlüsselte E-Mails zu verwenden ua.
- Daten werden an einen Dienstleister und in der Folge allenfalls sogar an eine Kette von Subdienstleistern zur Erbringung von Dienstleistungen ausgelagert. Beim Dienstleister oder seinem Subdienstleister werden diese Daten gehackt. Der Auftraggeber ist nach § 10 Abs 1 DSG verpflichtet, einen Dienstleister auszuwählen, der ausreichende Gewähr für eine rechtmäßige und sichere Datenverarbeitung bietet, und die Subdienstleisterkette unter Kontrolle zu haben.
- In jüngster Zeit häufen sich Cyberangriffe, bei denen Daten gestohlen werden, insb Daten mit denen ein finanzieller Vorteil erlangt werden kann (zB Konto- oder Kreditkartendaten) oder Daten, die es den Tätern ermöglichen, fremde Identitäten anzunehmen (zB Briefköpfe und eingescannte Unterschriften), um in der Folge weitere Verbrechen auszuführen.

Was im Ernstfall als Erstes zu tun ist

Ein Datenmissbrauch ist wie ein Brand, der weder Rücksicht auf die interne Planungen eines Unternehmens (Urlaube, Wochenenden etc) nimmt, noch Nachlässigkeit im Brandschutz verzeiht. Eine schnelle sicherheitstechnische Lageeinschätzung durch Experten ist entscheidend. Innerhalb von 24 Stunden müssen die ersten IT-Forensik-Maßnahmen eingeleitet sein, um einerseits wertvolle Spuren nicht zu verwischen, und andererseits um durch technische Sofortmaßnahmen weiterführenden Datenabfluss einzudämmen.

PRAXISTIPP

Es empfiehlt sich einen Bereitschaftsvertrag mit auf Cyber Incident Res-

ponse und Cyber Forensik spezialisierten Firmen mit 24 h Hotline abzuschließen oder ein eigenes internes IT-Forensik-Team aufzubauen.

Die beste Feuerwehr ist auf gute Baupläne angewiesen. Daher ist auch beim Cyber-Ernstfall eine gute Vorbereitung unabdingbar; dazu gehört die Umsetzung eines unternehmensweiten Konzeptes für Identifikation und Sammlung von Cyber-Alarmen. Zusätzlich helfen spezielle Fallen für Cyber-Angreifer (zB CyberTrap), einen Datenmissbrauch zu entdecken und rechtliche Schritte einzuleiten.

Am schnellsten kommt eine Organisation mit den technischen Vorbereitungen gegen Datenmissbrauch voran, wenn Sicherheitstests mit genau dieser Zielsetzung durchgeführt werden.

Ein Reality-Check durch einen Sicherheitstest überzeugt in der Regel alle Zweifler von der Sinnhaftigkeit solcher Vorbereitungen.

Pflicht zur Verständigung

Kommt der Auftraggeber – allenfalls mit Unterstützung eines externen, auf Datenschutzrecht spezialisierten Rechtsbeistandes – bei der Prüfung eines Missbrauchsfalls zum Ergebnis, dass eine Informationspflicht vorliegt, dann ist im Einzelfall zu überlegen, wie die Betroffenen zu verständigen sind; typischerweise per Brief, E-Mail oder Anruf.[1] Wenn dies nicht möglich ist oder einen unverhältnismäßigen Aufwand bedeutet, kann auch per Inserat in der Zeitung verständigt werden. Es empfiehlt sich, in allen Fällen die interne PR-Abteilung oder einen externen PR-Berater hinzuzuziehen, der die Formulierungen des Rechtsberaters bestmöglich in die Medien transportiert.

Mediendesaster verhindern

„Die richtige Information in der richtigen Qualität, zur richtigen Zeit am richtigen Ort". Diesen Leitsatz gilt es im Falle eines Krisenprozesses ständig mitzudenken. Ein strategisches Krisenmanagement kann als Schutzschild gegen Mediendesaster verstanden werden. Wirtschaftliche und das Image betreffende Schäden sind maßgeblich von der wohlüberlegten Umsetzung abhängig. Diese Strategien müssen vor, während und nach einer Krise berücksichtigt werden:

- **Vor der Krise ist nach der Krise**

Krisen können unvorhersehbar sein. Das bedeutet aber nicht, dass man Krisen auch unvorbereitet begegnen sollte. Eine unprofessionelle Krisenkommunikation lässt sich schnell an folgenden Merkmalen ausmachen: Sie ist zu spät, zu kompliziert, zu unpersönlich und zu technisch. In diesem Fall ist die Kommunikation meist fremdbestimmt und die Medienberichterstattung geprägt von Spekulationen. Ab diesem Zeitpunkt ist es für Unternehmen nur mehr schwer, ohne langfristige Imageschäden aus der Krise zu kommen. Entscheidend ist daher eine frühzeitige Auseinandersetzung mit dem Thema. Im Rahmen eines Krisenkommunikationsplanes werden bspw Verantwortlichkeiten definiert sowie Planentscheidungen und Sprachregelungen vorbereitet.

- **Während der Krise: Lösungen, nicht Probleme artikulieren**

Ein sorgfältig ausgearbeiteter Krisenkommunikationsplan ermöglicht ein professionelles Agieren während der Krise selbst. Dazu zählt va die zielgruppenadäquate Ansprache der eigenen Mitarbeiter, Partner, Kunden sowie Medienvertreter. Dabei sollte die Kommunikation va von Fakten geprägt sein. Spekulationen und Gerüchten wird damit wirksam vorgebeugt. Das Einhalten der W-Regel (wer, wo, was, wann, wie) dient als Orientierungshilfe in puncto Kommunikationsinhalte.

- **Nach der Krise ist vor der Krise**

Eine offene Informations- und Kommunikationspolitik stärkt die Glaubwürdigkeit und das Vertrauen in die handelnden Personen. Es ist förderlich, die Bewältigung der Krise zu protokollieren und eine anschließende Evaluation vorzunehmen. Mit den gewonnenen Erfahrungen können Schwachstellen entdeckt und der Krisenkommunikationsplan verbessert werden.

Ein Krisenmanagement kann die Dauer sowie die Kosten bei Missbrauchsfällen verringern und unterstreicht eine verantwortungsbewusste Arbeitsweise.

Ausnahmen von der Informationspflicht

Von der Informationspflicht gibt es in § 24 Abs 2a Satz 2 DSG zwei (alternative) Ausnahmen, nämlich wenn diese

- *„angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits*
- *oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert".*

Da vom Gesetzgeber ausdrücklich das Wort „oder" verwendet wird, genügt das Vorliegen einer der beiden Bedingungen, um von der Informationspflicht befreit zu sein.[2] Der Anwendungsbereich der beiden Ausnahmen ist unklar. Im ersten Fall ist unsicher, wie hoch ein Schaden sein kann, um gerade noch als „geringfügig" zu gelten.[3] Im zweiten Fall ist fraglich, ab wann die Informationskosten unverhältnismäßig wären. Das Unternehmen muss beide Ausnahmefälle im eingetretenen Missbrauchsfall anhand der konkreten Umstände (Betroffenenkreis, Anzahl der Betroffenen, Arten der drohenden Schäden,[4] Schadenshöhen usw) beurteilen.

Keine Pflicht zur Meldung an die Behörde

Die österr Datenschutzbehörde ist nach derzeitiger Rechtslage über einen Missbrauchsfall weder zu informieren noch sonst einzubinden.[5] Dies scheint für betroffene Unternehmen im ersten Moment zwar ein Vorteil zu sein, bedeutet aber letztlich, dass Unternehmen völlig alleine beurteilen müssen, in welcher Form Betroffene über einen Missbrauchsfall geeignet zu informieren sind. Auch im Hinblick auf mögliche zivilrechtliche Haftungen wegen eines Verstoßes gegen Schadensminderungspflichten und Haftungsfreizeichnungen von Risikoversicherungen der betroffenen Unternehmen bei Ignorieren der Informationspflicht (Schutzgesetzverletzung)[6] wird den Unternehmen eine erhebliche Selbstverantwortung auferlegt.[7]

Regelung ab 2018 verschärft

Mit der ab Frühjahr 2018 in Kraft tretenden DSGVO werden die Regelungen zum Da-

[1] Für den Inhalt der Verständigung geben die Sonderregelungen der Verordnung (EU) 611/2013 der Kom vom 24. 6. 2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 2013/173 einen Anhaltspunkt; die Formulierung ist aus juristischer Sicht heikel. [2] *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 24 Anm 28. [3] € 50,– können je nach Einkommensverhältnis unbedeutend oder wesentlich sein; *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 24 Anm 27. [4] Die RV zur DSG-Nov 2010 spricht von Vermögensschäden, eine Einschränkung auf solche ergibt sich aus dem Gesetzeswortlaut nicht und wäre auch widersinnig; siehe *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 24 Anm 21. [5] *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 24 Anm 26. Beachte aber die Sonderregelungen in § 85a TKG. [6] Siehe zur zivilrechtlichen Verantwortlichkeit und den Informationspflichten als nebenvertragliche Schutzpflichten *Feiler*, MR 2009, 281 (283 f). [7] *Knyrim/Leissler*, Die Datenschutzgesetznovelle 2010 – ein Überblick, ecolex 2010, 297 (299).

tenmissbrauch deutlich verschärft. Dann ist der Datenschutzbehörde binnen 72 Stunden darüber eine Meldung zu machen, in der bereits die Art der Verletzung, die betroffenen Datenkategorien, die ungefähre Anzahl der betroffenen Personen und die ungefähre Zahl der betroffenen Datensätze sowie eine Beschreibung der wahrscheinlichen Folgen des Vorfalls und eine Beschreibung der bereits ergriffenen oder vorgeschlagenen Maßnahmen enthalten sein müssen. Wenn die Frist nicht eingehalten wird, ist das gegenüber der Behörde zu begründen. Wie bisher sind auch die Betroffenen von dem Vorfall zu verständigen, wenn sich für diese voraussichtlich ein hohes Risiko ergibt und nicht durch technische Sicherheitsmaßnahmen (zB Verschlüsselung) vorgesorgt wurde.

In der DSGVO sind bei Datenmissbrauch Strafen bis zu 10 Mio Euro oder 2% vom globalen Umsatz vorgesehen!

Der Vorfall ist weiters intern so zu dokumentieren, dass er der Datenschutzbehörde die Möglichkeit gibt, zu überprüfen, ob die Vorgaben der DSGVO eingehalten wurden.

Vorbereitung auf den Ernstfall

Unternehmen wie öffentlichen Stellen ist – vor allem in Hinblick auf die Strafverschärfung ab 2018 – zu raten, einen möglichen Ernstfall nicht unvorbereitet auf sich zukommen zu lassen, sondern proaktiv Maßnahmen zu ergreifen. Vorbereitungsmaßnahmen sind nicht nur das Durchspielen unternehmenstypischer Risikoszenarien durch die Rechtsabteilung, auch die gemeinsame Ausarbeitung von Notfallplänen mit betroffenen Abteilungen (PR-Abteilung, externe PR-Berater, Unternehmens-IT, externe IT-Sicherheitsberater, Bereitschaftsteams bei Cyberangriffen, Krisenmanagement, externe Rechtsberater, Geschäftsführung sowie betroffene Fachabteilungen) gehört dazu.[8]

Dako 2016/20

[8] *Knyrim/Leissler*, ecolex 2010, 297 (300).

Zum Thema

Über die Autoren

RA Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte. Kontakt: Tel: +43 0(1) 533 16 95, E-Mail: knyrim@preslmayr.at, Internet: www. preslmayr.at

Mag. Clemens Foisner ist Geschäftsführer bei der SEC Consult Unternehmensberatung GmbH. Kontakt: Tel: +43 (0)1 890 3043-0, E-Mail: C.Foisner@sec-consult.com, Internet: www.sec-consult.com

Paul Prihoda ist Geschäftsführer der corporate identity prihoda gmbh, einer Full-Service-Agentur mit Sitz in Wien. Kontakt: Tel: +43 (0)1 47 96 366-0, E-Mail: paul.prihoda@cip.at, Internet: www.cip.at