DR. RUDEL SCHÄFER & PARTNER
WIRTSCHAFTSPRÜFER RECHTSANWÄLTE STEUERBERATER

PFLICHTEN, HAFTUNG UND SANKTIONEN BEI CYBERANGRIFFEN

KREISSPARKASSE MELLE

26. Oktober 2023

CYBERANGRIFF
SOFORTHILFE

SOFORTHILFE

Was bei einem
IT-Sicherheitsnotfall zu tun ist

1

RUHE BEWAHREN

Bevor Sie etwas tun: Die Umsetzung von Maßnahmen muss gut überlegt sein, da sie sich auf die spätere Spurensicherung auswirkt.
Machen Sie sich also zunächst einen Plan, holen Sie sich Unterstützung und leiten erst dann gezielte Maßnahmen ein.
Klären Sie als erstes, ob es sich um einen Cyber-Angriff oder einen technischen Defekt handelt.

DIGITAL SICHER NRW

INHALT

1. Pflichten nach Datenschutzrecht, Haftung und Sanktionen
2. Pflichten gegenüber Geschäftspartnern, Haftung und Sanktionen
3. Pflichten gegenüber sich selbst
4. Maßnahmen nach einem Cyberangriff
5. Maßnahmen vor einem Cyberangriff

PFLICHTEN NACH DATENSCHUTZRECHT

MELDEPFLICHT GEGENÜBER DER AUFSICHTSBEHÖRDE

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst **binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde.

Ausnahme von der Meldepflicht: **kein Risiko für die Rechte und Freiheiten natürlicher Personen** (Verantwortlicher trägt Risiko der Fehleinschätzung).

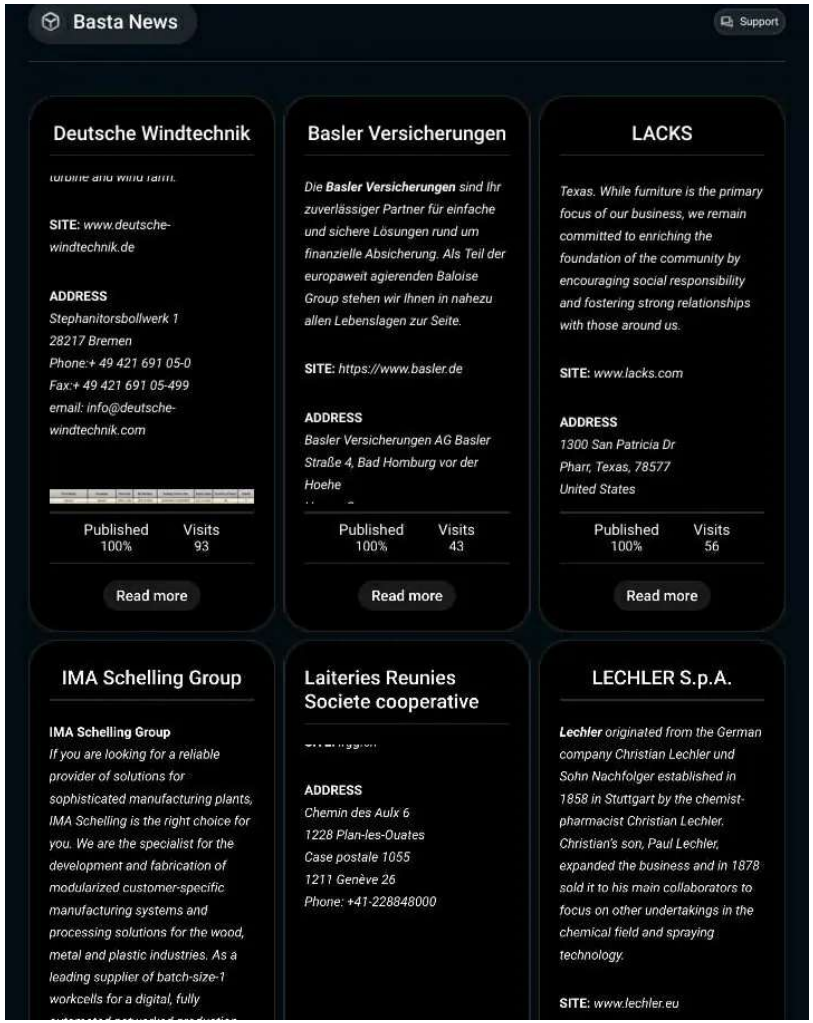
Durch die Meldepflicht wird die Behörde frühzeitig involviert; die Behörde kann auch Maßnahmen gegen den Verantwortlichen geltend machen.

Behörden stellen i.d.R. ein Online-Formular für die Meldung zur Verfügung.

Nachmeldungen zulässig. Das Fehlen genauer Informationen (z. B. die genaue Zahl der betroffenen Personen) sollte kein Hindernis für die frühzeitige Meldung einer Datenschutzverletzung sein. Nach der DSGVO dürfen ungefähre Zahlen der betroffenen Personen und der betroffenen personenbezogenen Datensätze angegeben werden.

PFLICHTEN NACH DATENSCHUTZRECHT

MELDEPFLICHT GEGENÜBER DER AUFSICHTSBEHÖRDE



DR. RUDEL SCHÄFER & PARTNER

PFLICHTEN NACH DATENSCHUTZRECHT

MELDEPFLICHT GEGENÜBER DER AUFSICHTSBEHÖRDE

Reaktionen der Aufsichtsbehörden auf Meldung sehr unterschiedlich:

… hiermit bestätige ich den Eingang Ihrer Meldungen gem. Art. 33 Datenschutzgrundverordnung (DS-GVO). Die Meldungen erfolgten fristgerecht im Sinne des Art. 33 DS-GVO. Sollten sich bezüglich des vorgetragenen Sachverhalts offene Fragen ergeben, werde ich unaufgefordert auf Sie zukommen...

Oder:

Zur technischen Beurteilung der Datenpanne bitte ich um Vorlage des forensischen Abschlussberichts. Die Verpflichtung zur Vorlage der Dokumentation über den Datenschutzvorfall ergibt sich aus Art. 33 Abs. 5 DS-GVO.

Aus der Dokumentation soll unter anderem die Beantwortung der folgenden Fragen hervorgehen:

- Auf welche Weise gelang es den Angreifern in Ihr Netz einzudringen? Was war der hierfür genutzte Angriffsvektor?
- Welche technischen und organisatorischen Maßnahmen (toM) gab es, um diesen Angriffsvektor zu verhindern?
- Warum haben die toM in diesem Fall den Angriff nicht verhindern können?
- Welche toM wurden / werden umgesetzt, damit ein solcher Angriff zukünftig besser verhindert werden kann?
- Auf welche Weise gelang es den Angreifern sich durch das Netz zu bewegen?
- Welche toM gab es, um diese Bewegung zu verhindern?
- Warum haben die toM in diesem Fall die Bewegung nicht verhindern können?
- Aussagen zur Schadenshöhe / zum Schadenspotential für die Betroffenen auf Grundlage der abgeflossenen Daten.
- Sind zudem Daten nach Artikel 9 DS-GVO oder besonders schützenswerte Informationen von Betroffenen abgeflossen?

PFLICHTEN NACH DATENSCHUTZRECHT

DOKUMENTATIONSPFLICHT GEGENÜBER DER AUFSICHTSBEHÖRDE

Der Verantwortliche muss die Verletzungen des Schutzes personenbezogener Daten dokumentieren.

Die Dokumentation dient der Überprüfung der Richtigkeit und Vollständigkeit der Meldung, der möglichen Folgen für die Betroffenen und der Notwendigkeit ergänzender Maßnahmen der Schadensbegrenzung.

Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der gesetzlichen Bestimmungen ermöglichen.

PFLICHTEN NACH DATENSCHUTZRECHT

EMPFEHLUNGEN

Mit den Datenschutzbehörden Kontakt halten und Fristen einhalten.

Betrieblichen Datenschutzbeauftragten schulen und vorbereiten.

PFLICHTEN NACH DATENSCHUTZRECHT

PFLICHT ZUR BENACHRICHTIGUNG DER BETROFFENEN

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen** zur Folge, so benachrichtigt der Verantwortliche die betroffenen Personen **unverzüglich** von der Verletzung. Bsp.: hohe Wahrscheinlichkeit für einen Schaden beim Betroffenen und/oder hoher Schaden

Soll dem Betroffenen Maßnahmen zum Selbstschutz und zur Schadensminderung ermöglichen.

VERSTOß GEGEN DATENSCHUTZPFLICHTEN

HAFTUNG UND SANKTIONEN

Die Betroffenen haben Schadensersatzansprüche.

Die Betroffenen haben Auskunftsansprüche.

Bußgelder der Behörden

Problem von Meldungen: Verwendung von Informationen aus der Meldung im Bußgeldverfahren (Art. 83 DSGVO)

Prüfungsverfahren der Datenschutzbehörden können kostenpflichtig sein.

VERSTOß GEGEN DATENSCHUTZPFLICHTEN

HAFTUNG UND SANKTIONEN

Durchsetzung von Ansprüchen wird den Betroffenen leicht gemacht durch z.B. Europäische Gesellschaft für Datenschutz

EuGD in der Presse

Bild 07.10.2023
Hacker-Angriff auf „Motel One" Was Betroffene jetzt tun sollten

Allianz für Cyber-Sicherheit
Teilnehmer

tagesschau.de 25.09.2023
Klagewelle gegen Schufa?

DER SPIEGEL 04.01.2023
Außergerichtlicher Vergleich [...] zahlt Kunden wegen Datenleck 300 Euro

DR. RUDEL SCHÄFER & PARTNER

PFLICHTEN GEGENÜBER GESCHÄFTSPARTNERN

GESETZLICHE & VERTRAGLICHE VERPFLICHTUNGEN

Dem betroffenen Unternehmen sind Informationen und Daten „anvertraut“.

Hacker erlangen z.B. Zugriff auf geheime Konstruktionspläne, Know-How, das dem betroffenen Unternehmen von dessen Kunden zur Verfügung gestellt werden.

Pflichten aus Vertraulichkeitsvereinbarung (NDA), soweit abgeschlossen.

Pflichten aus Sicherheitsrichtlinie, soweit Vertragsbestandteil,

Pflichten aus dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), auch Pflicht Geschäftsgeheimnisse nicht offen zu legen.

PFLICHTEN GEGENÜBER GESCHÄFTSPARTNERN

PFLICHT VIREN UND SCHADSOFTWARE NICHT WEITERZUGEBEN

Geschäftspartner wird über Cyberangriff beim eigenen Unternehmen nicht rechtzeitig informiert, Angreifer können z.B. auch Kunden angreifen.

Weitergabe eines Computervirus (z.B. E-Mail mit Schadprogramm).

Systeme des Unternehmens werden für eine Cyberattacke gegen ein anderes Unternehmen genutzt (z.B. DDoS-Attack).

PFLICHTEN GEGENÜBER GESCHÄFTSPARTNERN

EMPFEHLUNGEN

Geschäftspartner informieren und informiert halten, möglicherweise ergeben sich für diese Pflichten (z.B. Meldepflichten).

Veröffentlichung auf Website?

PFLICHTEN GEGENÜBER GESCHÄFTSPARTNERN

HAFTUNG UND SANKTIONEN

Schadenersatz für z.B. Verzugsschäden oder Nichterfüllung aus dem Vertrag

Unterlassung und Auskunft

Vertragsstrafen

Beendigung der Geschäftsbeziehung / Kündigung von Lieferverträgen

Bei Abschluss einer Vertraulichkeitsvereinbarung (NDA) hängen Folgen von den vertraglichen Regelungen ab.

PFLICHTEN GEGENÜBER SICH SELBST

Eigene Dokumente und Informationen des Unternehmens sind durch Cyberangriff gelöscht.

Pflichtverstöße:

- Verstoß gegen Aufbewahrungspflichten nach AO und HGB
- Beweisschwierigkeiten in einem etwaigen Rechtstreit

Folgen:

- Steuerschätzung
- verlorener Rechtstreit
- Betriebsunterbrechung
- Kosten für Datenwiederherstellung
- IT-Forensik, Anwalt
- Reputationsschäden

MAßNAHMEN NACH CYBERANGRIFF
MELDUNGEN AN BEHÖRDEN

1. Polizei
2. Verfassungsschutz (bei Wirtschaftsspionage)
3. Zentrale Ansprechstelle Cybercrime für die nds. Wirtschaft
4. Landeskriminalamt
5. Landesbeauftragte für Datenschutz

MAßNAHMEN NACH CYBERANGRIFF

VERSICHERUNGEN

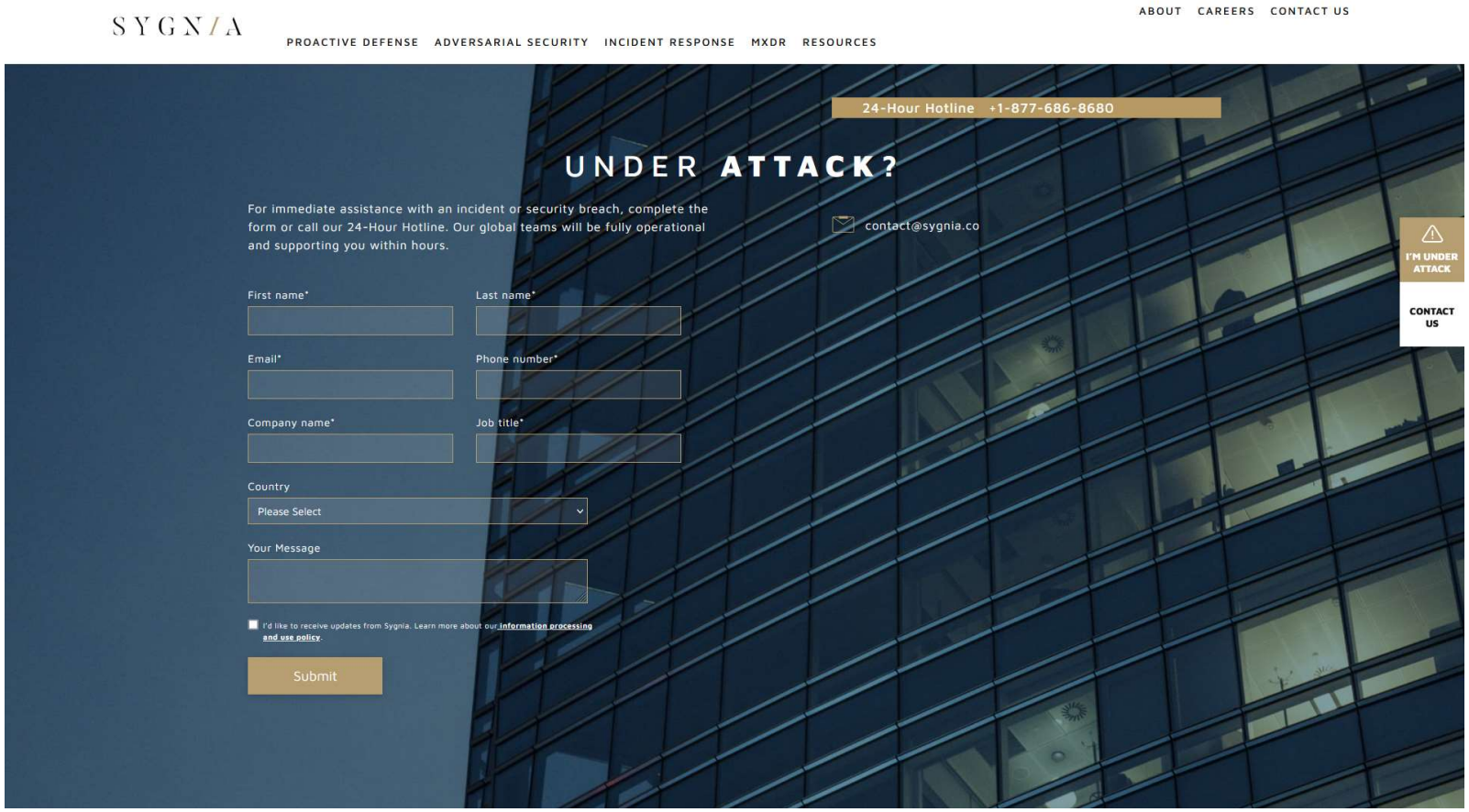
(Schadens-) Meldung an Versicherer, insbesondere bei Cyber-Versicherung

Möglicherweise Unterstützung von Versicherer

MAßNAHMEN NACH CYBERANGRIFF

SCHUTZ DER DATEN UND INFORMATIONEN AUCH NACH DEM ANGRIFF

Dienstleister beauftragen (Computer Emergency Response Team (CERT))?



MAßNAHMEN NACH CYBERANGRIFF
LÖSEGELD

Lösegeldzahlung an Cyberkriminelle könnte problematisch sein:

- Unterstützung krimineller Vereinigungen und terroristischer Vereinigungen
- Geldwäsche
- Embargoregelungen und Sanktionslisten
- Außenwirtschaftsgesetz
- Terrorismusfinanzierung

MAßNAHMEN VOR EINEM CYBERANGRIFF

IT-SICHERHEITSKONZEPT & TECHNISCHE NOTFALLVORSORGE-MAßNAHMEN

Aus **organisatorischer Sicht** sollte sich ein Unternehmen ein übergeordnetes **IT-Sicherheitskonzept** geben. In diesem sind die grundlegenden Aspekte, Strategien und auch Vorgaben zu Rollen, Zuständigkeiten und Maßnahmen für die Cybersicherheit darzulegen.

Technische und organisatorische Maßnahmen zum Schutz der Daten. Unzulänglichkeiten möglicherweise im Bericht des Forensikers zu lesen.

Hinzu kommen überwiegend **technische Notfallvorsorge-Maßnahmen**, die die Weiterführung des Geschäftsbetriebs ermöglichen, wie Backup- und Archivierungslösungen für die Recovery-Planung.

NIS 2 Richtlinie beobachten!

- Wird bis spätestens Oktober 2024 in nationales Recht überführt
- Betroffen sein können z.B. Unternehmen mit 50 bis 249 Mitarbeitende und einem Jahresumsatz von weniger als 50 Mio. EUR
- Zu den Verpflichtungen in der NIS 2 Richtlinie zählen Maßnahmen zur Erhöhung des Schutzes vor Cyberangriffen
- Ausweitung und Verschärfung der Haftung

DR. RUDEL
SCHÄFER
& PARTNER
WIRTSCHAFTSPRÜFER RECHTSANWÄLTE STEUERBERATER

Osnabrück

Dr. Rudel, Schäfer & Partner mbB
Wirtschaftsprüfer, Rechtsanwälte, Steuerberater

Friedrich-Janssen-Straße 1
49076 Osnabrück

Tel. 05 41/3 58 33 0
Fax 05 41/3 58 33 33

anwaelte@rudel-schaefer-partner.de

Melle

Dr. Rudel, Schäfer & Partner mbB
Wirtschaftsprüfer, Rechtsanwälte, Steuerberater

Bahnhofstraße 12
49324 Melle

Tel. 0 54 22/95 54 0
Fax 0 54 22/95 54 54

melle@rudel-schaefer-partner.de