Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 01/2021

Der IT-Ticker 01/2021 informiert Sie über folgende Themen:

Alarmstufe Rot bei Microsoft Exchange Servern – Akuter Handlungsbedarf

Wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) zum dritten Mal überhaupt erst die Alarmstufe Rot ausruft und vor der Gefährdung tausender von Unternehmen warnt und gleichzeitig Datenschutzaufsichtsbehörden auf eigene Initiative automatisierte Systemanalysen bei einer Vielzahl von IT-Systemen durchführen, ist klar, dass ein Ereignis eingetreten sein muss, das unmittelbaren Handlungsbedarf hervorruft.

Was ist passiert?
Ende vergangenen Jahres entdecken Sicherheitsforscher mehrere Sicherheitslücken in der weitverbreiteten Standardsoftware Microsoft Exchange Server, die es unberechtigten Dritten mit verhältnismäßig wenig Aufwand erlauben, weitgehende Admin-Zugriffe auf die Systeme zu nehmen, ohne die dafür eigentlich notwendigen Admin Passwörter zu kennen. Anfang des Jahres informierten die Forscher Microsoft. Das Unternehmen veröffentliche in der Nacht zum 3.3.2021 außerplanmäßig Patches als Gegenmittel und machte den Fall öffentlich (https://news.microsoft.com/de-de/hafnium-sicherheitsupdate-zum-schutz-vor-neuem-nationalstaatlichem-angreifer-verfuegbar/). Der Fall ist deshalb von hoher Brisanz, da zum einen mit dem Microsoft Exchange Server eines der am weitesten verbreiteten Softwaresysteme zum Austausch von E-Mails, Kontakten und Kalendereinträgen in Unternehmen betroffen ist, zum anderen aber nur solche Installationen von den Schwachstellen betroffen sind, die sich nicht in den Microsoft Cloudsystemen, sondern auf unternehmenseigenen IT-Systemen befinden. Unter diesen „nicht Cloudsystemen“ sind besonders häufig mittelständische Unternehmen anzutreffen, die bisher die Verlagerung ihrer Systeme in die Cloud gescheut haben.

Was ist zu tun? Patchen, prüfen, melden!
Das bayerische Landesaufsichtsamt für den Datenschutz (BayLDA) hat die aus dem Vorfall folgenden Handlungspflichten für Unternehmen so zutreffend wie plakativ zusammengefasst: patchen, prüfen, melden!

Erste Handlungspflicht für alle Unternehmen, die den Microsoft Exchange Server außerhalb einer Cloud Lösung einsetzen, besteht darin alle von Microsoft angebotenen Updates und Patches einzuspielen um den weiteren unberechtigten Zugang für Dritte abzuriegeln. Das BSI geht davon aus, dass allein in Deutschland von dieser Situation ca. 57.000 IT-Systeme betroffen sind. Da es sich hierbei insbesondere um Systeme handelt, die personenbezogene Daten wie Kontakte und E-Mails verwalten, folgt die Pflicht der Unternehmen zur Handlung auch aus Art. 32 DSGVO und den persönlichen Pflichten des Unternehmers sein Unternehmen vor abwendbaren Risiken zu bewahren (§ 43 GmbHG, § 93 AktG).

Allein die Verriegelung der Systeme reicht jedoch nicht aus. Es ist auch sicherzustellen, dass die Angreifer nicht längst auf den Systemen unterwegs waren. Nachdem die Schwachstellen zunächst von einer vermutlich chinesischen Hacker Gruppe mit dem Namen „Hafnium“ genutzt wurden, mehren sich nun die Anzeichen, dass zahlreiche weitere Angreifergruppen sowohl mit dem Hintergrund von Industriespionage als auch mit dem kommerziellen Ziel der Erpressung betroffener Unternehmen aktiv sind. Das BSI berichtet z.B. über die verbreitete Ausnutzung durch die Ransomware Software DearCry. Aus diesen Angriffsszenarien folgen unmittelbare Risiken für die möglicherweise betroffenen personenbezogenen Daten. Die Unternehmen, die solche Systeme betreiben, sind daher zum einen sowohl aus Art. 32 DSGVO als auch aus speziellen IT- Sicherheitsvorgaben z.B. für Unternehmen der kritischen Infrastruktur (KRITIS) (Stadtwerke etc.) zum einen verpflichtet, ihre Systeme auf unberechtigte Zugriffe zu untersuchen zum andere aber auch gegebenenfalls solche Zugriffe gegenüber den zuständigen Aufsichtsbehörden und den Betroffenen zu melden. Hilfestellungen bieten zum einen das BSI mit konkreten Unterstützungen zum Auffinden von Schadsoftware (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf?__blob=publicationFile&v=3) als auch die Datenschutzaufsichtsbehörden mit entsprechenden Hilfestellungen (z.B. https://www.lda.bayern.de/de/thema_exchange_sicherheitsluecke.html). Allein die bayerische Datenschutzaufsicht hat bereits stichprobenartig ca. 16.000 Systeme automatisiert überprüft und weitere anlasslose Kontrollen und die Verhängung von empfindlichen Geldbußen bei Nichtstun und fehlenden Absicherungen angedroht.

Darüber hinaus empfiehlt sich die Hinzuziehung professioneller Unterstützung durch IT Sicherheitsexperten, da insbesondere mit Folgeangriffen und Erpressungsversuchen zu rechnen ist. Teilweise ist eine aktive Bereinigung der Systeme erforderlich, um weiteren Schaden zu vermeiden.

In vielen Fällen ist damit zu rechnen, dass Angreifer jedenfalls in der Zeit zwischen der Veröffentlichung der Patches und dem Einspielen der Patches unberechtigt Zugriff auf den Exchange-Server genommen haben. In diesen Fällen wird häufig ein meldepflichtiger Datenschutzvorfall vorliegen, da Kriminelle mit Schädigungsabsicht Zugriff auf E-Mails und Kontakte hatten. Eine verspätete Meldung solcher Datenschutzvorfälle kann selbst als Datenschutzverstoß geahndet werden. Daher sollten Prüfung und ggf. Meldung schnell erfolgen.

Wie kann man sich schützen? Unser Praxistip
Der Vorfall hat erneut besonders deutlich gemacht, wie richtig die regelmäßig wiederholten Empfehlungen zur IT Sicherheit in den Unternehmen sind. Gerade kleine und mittelständische Unternehmen in Deutschland sind leider immer noch viel zu oft zu sorglos im Umgang mit der IT Sicherheit, obwohl aus den immer häufiger vorkommenden Angriffen sowohl enorme Schadensrisiken für die Unternehmen als auch ganz persönliche Haftungsrisiken für die Unternehmer folgen. Viele Unternehmen prüfen auch, ob die Verlagerung von IT-Systemen zu den professionellen Cloudanbietern eine Lösung für das Problem sein kann. Zumindest in diesem konkreten Fall ist das offensichtlich so, da die Cloudinstallationen des Microsoft Exchange Servers offensichtlich von den Schwachstellen nicht betroffen sind. Gegenüber den immer wieder geäußerten datenschutzrechtlichen Bedenken gegen die Cloudsysteme drängt sich daher die Frage auf, wo die größeren Risiken für personenbezogene Daten und die Unternehmen zu sehen sind: Im abstrakten Risiko, dass gesetzlich geregelte Zugriffe durch demokratisch kontrollierte Behörden auf Systeme denkbar aber nicht bewiesen sind oder darin dass private oder staatlich organisierte Hackergruppen Angriffspunkte haben, um diese zunehmend auch als globale „Hack-as-a-Service“ Geschäftsmodelle zu betreiben.

Schließlich empfiehlt sich immer auch eine Prüfung der zahlreichen Angebote von Cyberversicherungen, um zumindest die finanziellen Risiken aus einer solchen Situation bestmöglich abzufedern.

Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de
Dr. Matthias Orthwein, München
m.orthwein@skwschwarz.de

EuGH stärkt Rechte der Contentprovider

Der EuGH hat am 09.03.2021 entschieden, dass ein Urheberrechtsinhaber (bzw. ein entsprechender Rechteverwerter) technische Schutzmaßnahmen gegen Framing ergreifen bzw. veranlassen kann, um die öffentliche Zugänglichmachung eines Werkes zu begrenzen (Az. C-392/19 - VG Bild-Kunst / Stiftung Preußischer Kulturbesitz). Die Einbettung eines derartig geschützten Werks in die Website eines Dritten durch Framing stellt eine Zugänglichmachung dieses Werks für ein neues Publikum dar (§ 19a UrhG) und ist von der Zustimmung des Rechteinhabers abhängig, wenn sie unter Umgehung technischer Maßnahmen gegen Framing erfolgt ist.

Der EuGH stärkt damit die Rechte der Urheber und Rechteverwerter im Internet (im Folgenden: Contentprovider).

Bisherige Rechtsprechung – BestWater und Svensson
Um diese Entscheidung einordnen zu können, lohnt ein kurzer Rückblick auf das Jahr 2014.

Damals hat der EuGH entschieden, dass die Einbettung eines auf einer Website öffentlich zugänglichen geschützten Werkes („Content“) in die Website eines Dritten unter Verwendung der Framing-Technik und ohne die Umgehung von technischen Schutzmaßnahmen keine neue Veröffentlichung ist.

Wenn der betreffende Content weder für ein neues Publikum noch nach einem speziellen technischen Verfahren wiedergegeben wird, ändere sich das Publikum der ursprünglichen Wiedergabe nicht. Ein Video, das einmal auf YouTube veröffentlicht wurde, werde daher nicht erneut auf der Website eines Dritten im Sinne des § 19a UrhG veröffentlicht, wenn dieser Dritte das entsprechende YouTube-Video per Framing einbindet. Hintergrund ist, dass YouTube keine technischen Schutzmaßnahmen gegen Framing anwendet, so der EuGH im Beschluss vom 21.10.2014 (Az. C-348/13 - BestWater International GmbH/Michael Mebes ua).

Entsprechend hatte der EuGH bereits auch in der Entscheidung vom 13.02.2014 entschieden, dass das Framing eines Textes, ebenfalls ohne Umgehung von technischen Schutzmaßnahmen, keine öffentlichen Wiedergabe im Sinne des § 19a UrhG darstellt (Az. C-466/12 - Nils Svensson, Sten Sjörgren, Madelaine Sahlman, Pia Gadd/Retriever Sverige AB).

Diese EuGH-Entscheidungen sorgten damals für Aufsehen, denn Contentprovider mussten und müssen mit einer Art Erschöpfung ihres Rechts der Wiedergabe leben. Dies gilt nach der aktuellen Entscheidung insbesondere dann, wenn sie sich nicht wirksam gegen Framing schützen.

Interessenlage
Da durch das Framing der jeweilige Content von der Website eines Dritten in die eigene Website eingebunden werden kann, können die Interessenslagen offenkundig völlig gegenläufig sein. Die ursprüngliche Website muss gerade nicht direkt aufgerufen werden, um den Content auf der Website eines Dritten wahrnehmen zu können. Dies kann Einfluss auf etwaige Werbeeinnahmen und Reichweitenmessungen haben.

Einordnung der aktuellen EuGH Entscheidung
Der EuGH bestätigt in seiner aktuellen Entscheidung zunächst den Grundsatz, wonach das Framing eine öffentliche Wiedergabe darstellt.

Er stellt dann fest, dass der o.g. Rechtsprechung aus dem Jahr 2014 ein anderer Sachverhalt zugrunde lag. Dort wurde der Zugang zu dem Content auf der ursprünglichen Website von keiner beschränkenden (Schutz-)Maßnahme abhängig gemacht. Da technische Maßnahmen fehlten, sei der EuGH davon ausgegangen, dass der Contentprovider sein Werk der Öffentlichkeit frei zugänglich gemacht bzw. eine solche Zugänglichmachung erlaubt habe und er von Anfang an alle Internetnutzer als Publikum angesehen habe. Damit habe der Contentprovider der Wiedergabe durch Dritte auch zugestimmt.

Wenn z. B. ein Content auf einer Website, auf der die ursprüngliche Wiedergabe erfolgte, nicht mehr öffentlich zugänglich ist oder wenn der Content nunmehr auf dieser Website nur einem begrenzten Publikum zugänglich sei, sei der Content der Öffentlichkeit nicht (mehr) frei zugänglich.

Diese Rechtsprechung präzisiert der EuGH in der aktuellen Entscheidung. Er stellt fest, dass aus den früheren Entscheidungen nicht automatisch folgt, dass das Setzen von Hyperlinks zu geschützten Werken auf einer Website, die auf einer anderen Website ohne die Erlaubnis des Urheberrechtsinhabers frei zugänglich gemacht wurden, grundsätzlich nicht unter den Begriff „öffentliche Wiedergabe“ fällt.

Die frühere Rechtsprechung bestätige vielmehr, dass grundsätzlich jede öffentliche Wiedergabe eines Werks von dem Urheberrechtsinhaber erlaubt werden muss. Das gelte auch dann, wenn ein Dritter geschützte Werke, die mit Erlaubnis des Urheberrechtsinhabers auf bestimmten Websites frei zugänglich sind, öffentlich wiedergibt, obwohl der Rechteinhaber technische Maßnahmen zur Beschränkung des Zugangs zu seinen Werken von anderen Websites im Wege der Framing-Technik veranlasst hat. Gleiches gelte, wenn der Rechteinhaber seinen Lizenznehmern technische Schutzmaßnahmen aufgegeben hat, um das Publikum für seine Werke allein auf die Nutzer der ursprünglichen Website zu beschränken.

Der EuGH präzisiert gleichzeitig, dass es dem Urheberrechtsinhaber nicht gestattet ist, seine Erlaubnis auf andere Weise als durch wirksame technische Maßnahmen zu beschränken. Diese Einschränkung sei notwendig, um die Rechtssicherheit und das ordnungsgemäße Funktionieren des Internets zu gewährleisten.

Der EuGH stellt schließlich klar, dass sich die Erlaubnis des Rechteinhabers, der beschränkende Maßnahmen gegen Framing seiner Werke eingeführt hat, nicht auf „sämtliche Internetnutzer“ beziehen kann. Dies würde zu einer Erschöpfung seines Rechts führen und dem Rechteinhaber insbesondere auch die Möglichkeit nehmen, eine angemessene Lizenz für die Nutzung des Werkes zu verlangen.

Praxistipp
Der EuGH verwendet eine klare Sprache, um seine Entscheidung zu begründen. Contentprovider sollten technische Schutzmaßnahmen unbedingt einführen (auch nachträglich), wenn Nutzer Content auf der eigenen Webseite nutzen können. Ein Schutz durch irgendwie geartete organisatorische Schutzmaßnahmen wie bspw. der Hinweis, dass Framing nicht zulässig sei, reichen in keinem Fall, um den Vorgaben des EuGH zum Schutz gegen Framing zu genügen.

Der EuGH formuliert nicht, wie sich diese Ausführungen zum Urheberrecht auf entsprechende wettbewerbsrechtliche Fragen zur Leistungsübernahme (§ 4 Nr. 3 UWG) auswirken. Allerdings wird man eine wettbewerbswidrige Leistungsübernahme wohl annehmen können, wenn technische Schutzmaßnahmen rechtswidrig überwunden werden.

Esther Noske, Frankfurt / Main
e.noske@skwschwarz.de
Dr. Stefan Peintinger, München
s.peintinger@skwschwarz.de

Das Hinweisgeberschutzgesetz kommt - Referentenentwurf für das Hinweisgeberschutzgesetz zur Umsetzung der Whistleblower-Richtlinie liegt vor

Wir berichteten bereits über die Whistleblower-Richtlinie (RL (EU) 2019/1937). Den nationalen Gesetzgebern wurde aufgegeben, diese Richtlinie bis zum 17. Dezember 2021 in nationales Recht umzusetzen. Für Unternehmen mit der Regel bis zu 249 Beschäftigten soll diese Pflicht erst ab dem 17. Dezember 2023 gelten. Für ein entsprechendes Umsetzungsgesetz liegt nun ein Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vor. Mit dem neuen Gesetz zum Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG) soll der bislang lückenhafte und unzureichende Schutz hinweisgebender Personen ausgebaut werden.

Schutzbereich
Das HinSchG regelt den Schutz von natürlichen Personen, die im Zusammenhang mit ihrer beruflichen oder dienstlichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen (hinweisgebende Personen). Darüber hinaus werden auch natürliche Personen geschützt, die Gegenstand einer

Meldung oder Offenlegung sind, sowie sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind.

Pflicht zur Einrichtung interner Meldestellen
Entsprechend der Vorgaben der Whistleblower-Richtlinie werden Unternehmen ab einer Größe von 50 Beschäftigten, Kommunen ab einer Größe von 10.000 Einwohnern, sowie Behörden zur Errichtung von Meldesystemen für Hinweisgeber verpflichtet. Für bestimmte Unternehmen gilt die Pflicht zur Einrichtung interner Meldestellen unabhängig von der Zahl der Beschäftigten, z.B. für Wertpapierdienstleistungsunternehmer im Sinne des § 2 Absatz 10 des Wertpapierhandelsgesetzes.

Die Whistleblower-Richtlinie stellt es den EU-Mitgliedsstaaten frei, ob nur Meldungen über Verstöße gegen EU-Recht oder auch Verstöße gegen nationales Recht von den nationalen Umsetzungsgesetzen erfasst sein sollen. Der deutsche Gesetzgeber hat sich dazu entschieden, dass auch straf- und bußgeldbewährte Vorschriften in den Anwendungsbereich des deutschen Hinweisgeberschutzgesetzes fallen sollen. Begründet wird dies mit der Vermeidung von Wertungswidersprüchen, weil bei einfacher Umsetzung der Whistleblower-Richtlinie künftig zwar Verstöße gegen Europäisches Vergaberecht in den Anwendungsbereich des Hinweisgeberschutzgesetzes fallen würden, schwere Wirtschaftsstraftaten hingegen nicht.

Aufgaben der Meldestellen und sonstige Vorgaben
Bei internen Meldungen bestätigt die interne Meldestelle der hinweisgebenden Person den Eingang einer Meldung spätestens nach sieben Tagen, hält mit dieser Kontakt, prüft die Stichhaltigkeit der eingegangenen Meldung, ersucht die hinweisgebende Person erforderlichenfalls um weitere Informationen und ergreift angemessene Folgemaßnahmen.

Interne Meldekanäle müssen Meldungen in mündlicher oder in Textform ermöglichen. Auf Ersuchen der hinweisgebenden Person ist für eine Meldung innerhalb einer angemessenen Zeit eine persönliche Zusammenkunft mit den für die Entgegennahme einer Meldung zuständigen Personen der internen Meldestelle zu ermöglichen.

Hervorzuheben ist weiterhin, dass die Hinweisgeberstellen nicht verpflichtet werden sollen, anonymen Hinweisen nachzugehen. Die Identität sowohl der Hinweisgeber als auch der durch die Meldung sonst betroffenen Personen sind von der Meldestelle vertraulich zu behandeln.

Der Gesetzesentwurf sieht ferner konkrete Regelungen zu den einzuhaltenden Verfahrensabläufen nach Eingang einer Meldung vor. Dies betrifft insbesondere die Dokumentationspflichten, Fristen für Rückmeldungen an den Hinweisgeber und Folgemaßnahmen wie z. B. Internal Investigations.

Weiterhin sieht der Gesetzesentwurf vor, dass die internen Meldestellen Unabhängigkeit wahren müssen und frei von Interessenkonflikten sind. Eine interne Meldestelle kann zum einen durch eine im Unternehmen beschäftigte Person und zum anderen durch eine interne Organisationseinheit betrieben werden. In Betracht kommen z. B. der Compliance-Beauftragte, eine beschäftigte Person aus der Rechtsabteilung oder der Datenschutzbeauftragte des Unternehmens.

Der Gesetzesentwurf sieht aber auch ausdrücklich vor, dass externe Dritte, wie z. B. Rechtsanwälte als sog. Ombudsperson eingesetzt werden können. Hier besteht also ein Wahlrecht für die betroffenen Unternehmen um ein Hinweisgeber-System auf die konkreten Bedürfnisse des Unternehmens anpassen zu können.

Zudem soll es für Unternehmen in einer Größenordnung zwischen 50 bis 249 Beschäftigten aus Kosten- und Organisationsgründen möglich sein, mit anderen Unternehmen eine gemeinsame Meldestelle zu betreiben.

Wahlrecht zwischen interner und externer Meldung
Der Gesetzesentwurf sieht neben unternehmensinternen Meldestellen auch die Errichtung von externen Meldestellen durch Bund und Länder vor. Personen, die beabsichtigen, Informationen über einen Verstoß zu melden, können wählen, ob sie sich an eine interne Meldestelle oder eine externe Meldestelle wenden. Hierdurch sollen Unternehmen dazu animiert werden, ihre internen Meldestellen möglichst attraktiv auszugestalten.

Wenn einem intern gemeldeten Verstoß nicht abgeholfen wurde, bleibt es der hinweisgebenden Person unbenommen, sich anschließend an eine externe Meldestelle zu wenden.

Schutzmaßnahmen
Hinweisgebende Personen werden bei Vorliegen der entsprechenden Voraussetzungen vor Repressalien, wie z.B. Kündigungen oder Nichtbeförderungen, geschützt. Insoweit gilt eine Beweislastumkehr: Falls eine hinweisgebende Person nach einer Meldung oder Offenlegung eine Benachteiligung im Zusammenhang mit ihrer beruflichen Tätigkeit erleidet, hat die Person, die die hinweisgebende Person benachteiligt hat, zu beweisen, dass die Benachteiligung auf hinreichend gerechtfertigten Gründen basierte oder dass sie nicht auf der Meldung oder Offenlegung beruht.

Praxishinweise
Zwar handelt es sich bisher nur um einen Referentenentwurf. Es ist aber damit zu rechnen, dass das Hinweisgeberschutzgesetz noch im Jahr 2021 verabschiedet werden wird. Mit Inkrafttreten des Gesetzes sind Unternehmen dann zur Einrichtung von internen Meldestellen verpflichtet. Unternehmen sollten sich auf die kommenden Regelungen durch Einrichtung entsprechender Meldekanäle und Schulungen der Mitarbeiter vorbereiten. Ein gutes internes Meldesystem kann auch dazu führen, dass sich Beschäftigte an interne statt externe Meldestellen wenden. Unternehmen, die bereits über ein internes Meldesystem verfügen, müssen prüfen, ob dieses den neuen gesetzlichen Vorgaben an Meldewegen und den einzuhaltenden Verfahrensabläufen entspricht.

Ein gut funktionierendes Hinweisgeber-System stellt zukünftig einen wichtigen Baustein für ein effektiv funktionierendes Compliance Management System dar.

In weiteren Beiträgen wird SKW Schwarz Rechtsanwälte über die konkreten Pflichten, die Unternehmen treffen, im Detail berichten.

Die Experten von SKW Schwarz Rechtsanwälte stehen Ihnen für Fragen zur Whistleblower-Richtlinie jederzeit gerne zur Verfügung.

Dr. Oliver Hornung, Frankfurt / Main
o.hornung@skwschwarz.de
Philipp Sauer, Frankfurt / Main
p.sauer@skwschwarz.de

IT-Sicherheitsgesetz 2.0 im Bundestag – was ist neu?

Größerer Anwendungsbereich des BSIG, Regulierung „kritischer“ Komponenten und das IT-Sicherheitskennzeichen. Die wesentlichen Neuerungen des IT-SiG 2.0 im Überblick.

m Januar 2021 hat die Bundesregierung ihren Entwurf für das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) zur Beratung in den Bundestag eingebracht. Nach heftiger Kritik am Referentenentwurf aus Mai 2020 aus der Wirtschaft und der politischen Diskussion um den Aufbau der 5G-Infrastruktur im Bundesgebiet wurde der Gesetzesentwurf erneut angepasst. Aktuell ist davon auszugehen, dass der Bundestag das IT-Sicherheitsgesetz 2.0 in der eingebrachten Fassung zeitnah beschließen wird. Die Stellungnahme des Bundesrats liegt seit dem 12.02.2021 vor.

Neben rund 1.500 neuen Planstellen in verschiedenen Ministerien der Bundesverwaltung sieht das Gesetz in erster Linie Änderungen des BSIG vor. Insbesondere werden mit der Kategorie der Unternehmen im besonderen öffentlichen Interesse weitere Adressaten des BSIG etabliert. Außerdem reguliert das BSIG künftig auch den Einsatz kritischer Komponenten und räumt dem BSI die Möglichkeit ein, den Einsatz kritischer Kernkomponenten nicht vertrauenswürdiger Hersteller zu untersagen. Ebenfalls neu ist das freiwillige IT-Sicherheitskennzeichen.

Das „need-to-know“ zu diesen drei Stichworten fassen wir im Folgenden knapp zusammen:

Unternehmen im besonderen öffentlichen Interesse
Neben den bereits derzeit regulierten „Kritischen Infrastrukturen“ und „digitalen Diensten“ werden zukünftig auch „Unternehmen im besonderen öffentlichen Interesse“ unmittelbar durch das BSIG verpflichtet. Unternehmen im besonderen öffentlichen Interesse sind:

1. Unternehmen, die Güter im Sinne von § 60 Abs. 1 Nr. 1, 3 AWV herstellen oder entwickeln;
2. Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind. Die maßgeblichen Kennzahlen wird das BSI durch Rechtsverordnung gesondert festlegen; und
3. Unternehmen, die Betreiber eines Betriebsrechts der oberen Klasse der Störfall-Verordnung oder diesen gleichgestellt sind.

Unternehmen im Sinne der Nr. 1 und 2 müssen sich beim BSI registrieren, eine für das BSI erreichbare Stelle benennen und alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit gegenüber dem BSI abgeben. Für Unternehmen im Sinne der Nr. 3 ist dies jeweils optional.

Zudem müssen Unternehmen im besonderen öffentlichen Interesse wesentliche Störungen ihrer Systeme, Komponenten und Prozesse mit Auswirkung auf ihre Wertschöpfung an das BSI melden.

Kritische Komponenten
Neu ist außerdem die vor allem im Kontext der 5G-Infrastruktur öffentlich diskutierte Regulierung kritischer Komponenten durch das geänderte BSIG.

Der Begriff „kritische Komponenten“ beschreibt – stark verkürzt – Software und Hardware, die für Kernfunktionen einer kritischen Infrastruktur (KRITIS) eingesetzt wird und welche entweder durch Gesetz als kritische Komponente bestimmt wurde oder eine aufgrund eines Gesetzes als kritisch bestimmte Funktion realisiert.

Die Regulierung kritischer Komponenten betrifft damit primär KRITIS-Betreiber. Kritische Komponenten dürfen künftig nur noch eingesetzt werden, wenn der Hersteller der Komponente eine Garantieerklärung gegenüber dem KRITIS-Betreiber abgegeben hat. Daraus muss auch hervorgehen, ob und wie der Hersteller hinreichend sicherstellt, dass die kritische Komponenten über keine technischen Eigenschaften verfügt, um missbräuchlich auf Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der KRITIS einzuwirken. Die Anforderungen an die Garantieerklärung legt das BMI gesondert fest.

Zudem hat das BSI künftig die Befugnis, den Einsatz kritischer Komponenten und in Einzelfällen sogar den Betrieb der kritischen Infrastruktur an sich zu untersagen, wenn der Hersteller der Komponenten sich als nicht vertrauenswürdig erwiesen hat. Mittelbar hat die Regulierung kritischer Komponenten damit auch substantielle Auswirkungen auf Hersteller kritischer Komponenten.

IT-Sicherheitskennzeichen
Zur Verbesserung der Information von Verbrauchern zur IT-Produktsicherheit führt das IT-Sicherheitsgesetz 2.0 für vom BSI separat festzulegende Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein.

Hersteller oder Anbieter von Produkten dieser Kategorien können beim BSI die Freigabe zur Verwendung des IT-Sicherheitskennzeichens beantragen. Erteilt das BSI die beantragte Freigabe, kann der Hersteller das Kennzeichen für das Produkt verwenden, indem er das Etikett des IT-Sicherheitskennzeichens auf dem Produkt anbringt oder elektronisch veröffentlicht.

Das Kennzeichen besteht aus einer Zusicherung des Herstellers, wonach das Produkt bestimmte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung) und einer Information des BSI über sicherheitsrelevante IT-Eigenschaften des Produkts (Sicherheitsinformation). Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite, auf der Herstellererklärung und Sicherheitsinformation für das Produkt abrufbar sind.

Das IT-Sicherheitskennzeichen ist freiwillig. Weder ist das IT-Sicherheitskennzeichen Voraussetzung für den Vertrieb von Produkten im Bundesgebiet, noch sieht das IT-Sicherheitsgesetz 2.0 ausdrücklich eine rechtliche Wirkung des IT-Sicherheitskennzeichens gegenüber Verbrauchern zu. Mittelbar kann

das Kennzeichen dennoch verbindlich sein, etwa als Bestandteil der vertraglich geschuldeten Beschaffenheit des Produkts.

Dr. Daniel Meßmer, München
d.messmer@skwschwarz.de

Zwei-Faktor-Authentifizierung für Zahlungen im Internet

Was für das Online-Banking bereits seit 2019 gilt und was für Kreditkartenzahlungen von der BaFin zunächst verschoben wurde (wir berichteten bereits), muss ab Januar 2021 auch für Kreditkarten- und sonstige Zahlungen im Online-Handel beachtet werden: Die sog. Zwei-Faktor-Authentifizierung (auch bezeichnet als „Strong Customer Authentication" (SCA)).

Für Verbraucher ist der Einkauf im Internet seit Beginn des Jahres 2021 komplizierter geworden. Sie müssen sich nun bei Zahlungen mit der Kreditkarte ein zweites Mal identifizieren. Durch diese sogenannte Zwei-Faktor-Authentifizierung soll das Shoppen im Internet sicherer werden, um Betrügereien im Onlinehandel zu erschweren. Zugleich soll damit die Öffnung der Zahlungskonten für Dritte ermöglicht werden, etwa für Fintechs.

Diese Art der Identifikation gilt als besonders sicher. Denn eventuelle Angreifer müssten nicht nur die Zugangsdaten ihres Opfers stehlen oder hacken, sie müssten auch etwas Physisches wie das Handy oder die Kreditkarte in ihren Besitz bringen. Außerdem sind die TAN transaktionsgebunden - im Gegensatz zu den früheren meist auf Papier existierenden TAN-Listen der Banken.

Wie wurde die neue Regelung umgesetzt?
Bei Kreditkarten:
Die Neuregelung für Kreditkartenzahlungen von Verbrauchern erfolgt in unterschiedlichen Stufen, wohl um die Verbraucher langsam an die Neuerung zu gewöhnen und die angestrebte Absicherung langsam zu steigern. So erfordern Zahlungen mit einer Kreditkarte im Online-Handel seit dem 15. Januar 2021 ab 250 EUR einen doppelten Identitätsnachweis. Ab 15. Februar 2021 gilt diese Regelung dann bereits ab 150 EUR und ab 15. März 2021 sogar für Zahlungen ab 30 EUR.

Die Zwei-Faktor-Authentifizierung erfordert dabei gem. der Zahlungsdiensterichtlinie (PSD2) neben der Angabe der Kreditkartennummer und Prüfziffer zwei weitere Elemente der Identifizierung. Durchgesetzt hat sich ähnlich wie beim Online-Banking die Identifizierung mittels Handy ggf. in Verbindung mit einer besonderen App. Auf diese Weise findet zusätzlich eine Identifizierung über ein Wissenselement (Zugangsdaten) oder Inhärenzelement (z.B. Fingerabdruck) sowie einem Besitzelement (Handy) statt.

Bei sonstigen Zahlungsmöglichkeiten:
Die neuen Anforderungen gelten nicht nur für Kreditkartenzahlungen, sondern auch für Zahlungsarten wie bspw. Paypal. Hier erfolgt die Zwei-Faktor-Authentifizierung mittels der Anmeldung bei dem Paypal-Konto mittels Passwort (Wissenselement) sowie eines Sicherheitscodes per SMS auf das Handy (Besitzelement).

Ausblick
Durch diese Neuerungen wird zwar die Sicherheit deutlich erhöht, Zahlungen werden aber nicht nur für die Kunden, sondern auch für Online-Händler und Zahlungsdienstleister komplizierter. Es bleibt deshalb abzuwarten, auf welche Akzeptanz die neuen Anforderungen stoßen.

Praxistipp
Weiterhin sind von den neuen Regelungen in erster Linie Zahlungsdienstleister betroffen. Andere E-Commerce-Akteure, wie beispielsweise Online-Shops, sollten jedoch unbedingt bei ihren Zahlungsdienstleistern in Erfahrung bringen, ob die Vorgaben eingehalten werden, um rechtskonforme Zahlungsmöglichkeiten anbieten zu können.

Johannes Schäufele, München
j.schaeufele@skwschwarz.de
Dr. Tatjana Schroeder, Frankfurt / Main
t.schroeder@skwschwarz.de

Arbeitsschutz in der Corona-Krise: Was bedeutet die neue SARS-CoV-2-Arbeitsschutzverordnung für Arbeitgeber?

Infolge der Corona Beschlüsse vom 19. Januar 2021 hat das Bundesministerium für Arbeit und Soziales mittlerweile den Entwurf der SARS-CoV-2-Arbeitsschutzverordnung zur Verfügung gestellt – dieser soll fünf Tage nach seiner Verkündung bis zum 15. März 2021 Rechtskraft entfalten.

1. Was ist der Kern der Verordnung?
Neben weiteren Vorgaben zum betrieblichen Gesundheitsschutz, u.a. die Pflicht den Arbeitnehmern medizinische Gesichtsmasken unter bestimmten Umständen zur Verfügung zu stellen, ist Kernelement der Verordnung die Verpflichtung des Arbeitgebers, die Erbringung der Arbeitsleitung im Home Office zu ermöglichen.

2. Was muss der Arbeitgeber tun?
Der Arbeitgeber hat seinen Arbeitnehmern, sofern diese Bürotätigkeiten erbringen, anzubieten, dass diese ihre Aufgaben von zu Hause aus erfüllen. Aus Nachweisgründen sollte dieses Angebot dokumentiert sein, etwa per Email. Der Arbeitgeber wird des Weiteren wieder die technische Grundausstattung (Notebook, Handy etc.) stellen müssen. Allerdings sieht die Verordnung weder vor, dass der Arbeitgeber einen vollwertig ausgestatteten Arbeitsplatz (u.a. Büromöbel) zur Verfügung stellen muss, noch dass die Arbeitnehmer das Angebot annehmen müssen. Ebenso wenig ist der Arbeitgeber auf Basis der Verordnung berechtigt, die Arbeitnehmer in das Home Office zu versetzen.

3. Kann der Arbeitgeber das ablehnen?
Der Arbeitgeber muss seine Angebotspflicht nicht erfüllen, wenn zwingende betriebsbedingte Gründe entgegenstehen. Wann dies der Fall sein soll, regelt weder die Verordnung noch die Gesetzesmaterialien. Unter Berücksichtigung des Wortlauts der Verordnung wird jede Büroarbeit, welche nicht zwingend nur vom Büro aus erbracht werden kann, Home Office-geeignet sein, mit der Folge, dass der Arbeitgeber hier seiner Angebotspflicht nachkommen muss; dies wird vor allem für einfachere Sachbearbeiter- und/oder Telefontätigkeiten gelten.

4. Welche Konsequenzen drohen?
Die Verordnung selbst sieht keine Sanktionen vor. Erst wenn die jeweils zuständige Arbeitsschutzbehörde eines Landes die Einhaltung der Verordnung konkret anordnet, kann bei einem Verstoß ein Bußgeld verhängt werden. Angesichts der Äußerungen von Bundesarbeitsminister Heil erscheint diese Eskalation derzeit fernliegend – dies gilt es aber im Blick zu behalten. Darüber hinaus wird der Arbeitgeber „weiche“ Sanktionen abwägen müssen, etwa in Form atmosphärischer Störungen innerhalb der Belegschaft oder negativer Berichterstattung in den Medien.

5. Ist sonst etwas zu beachten?
Die Verordnung befreit die Arbeitgeber nicht von der Einhaltung sonstiger gesetzlicher Vorgaben. Insbesondere muss bei der Tätigkeit im Home Office die Einhaltung des Datenschutzes sowie der IT-Sicherheit gewährleistet sein – hierauf sollten Arbeitnehmer noch einmal gesondert hingewiesen werden. Aus Nachweisgründen empfiehlt sich eine dokumentierte Form des Hinweises, etwa per Email.
Weitere Informationen zur rechtskonformen Gestaltung von Home Office finden Sie in unserem Artikel.
Wir unterstützen Sie bei der Umsetzung der SARS-CoV-2-Arbeitsschutzverordnung

Wenn Sie Interesse an einer Beratung zur Umsetzung der SARS-CoV-2-Arbeitsschutzverordnung haben, schreiben Sie uns an kommunikation@skwschwarz.de. Wir rufen Sie gerne kurzfristig zurück und besprechen mit Ihnen das weitere Vorgehen.

Franziska Ladiges, Frankfurt / Main, f.ladiges@skwschwarz.de
Alexander Möller, Frankfurt / Main, a.moeller@skwschwarz.de
Dr. Oliver Hornung, Frankfurt / Main, o.hornung@skwschwarz.de
Michael Wahl, Frankfurt / Main, m.wahl@skwschwarz.de

Neujahrsgeschenk für Datenübermittlungen in das Vereinigte Königreich

Datenübermittlungen in das Vereinigte Königreich sind auf Basis der Schlussbestimmungen des Handels- und Kooperationsabkommens ("Brexit-Abkommen") vom 31.12.2020 erstmal weiterhin möglich.

Für eine Übergangsfrist von vier Monaten mit Option auf Verlängerung um weitere zwei Monate - bzw. wenn vor Ablauf dieser Frist ein Angemessenheitsbeschluss vorliegt bis zu diesem Zeitpunkt - gilt die Übermittlung personenbezogener Daten aus der EU an das Vereinigte Königreich nicht als Übermittlung an ein Drittland im Sinne des Unionsrechts. Daher sind Standardvertragsklauseln, Binding Corporate Rules oder andere Garantien nach Art. 46 DS-GVO erstmal für Übermittlungen in das Vereinigte Königreich nicht erforderlich. Damit sind auftretende gravierende Erschwernisse – mit allen Schwierigkeiten nach dem EuGH-Urteil Schrems II (https://www.skwschwarz.de/details/empfehlungen-des-edsa-fuer-drittlandstransfers-veroeffentlicht) und allen damit verbundenen Schwierigkeiten hinsichtlich des Einsatzes der Standardvertragsklauseln – erstmal vertagt.

Auf den Seiten 468/469 des Vertrags findet sich dazu folgende Regelung:

„Article FINPROV.10A: Interim provision for transmission of personal data to the United Kingdom

1) For the duration of the specified period, transmission of personal data from the Union to the United Kingdom shall not be considered as transfer to a third country under Union law, provided that the data protection legislation of the United Kingdom on 31 December 2020, as it is saved and incorporated into United Kingdom law by the European Union (Withdrawal) Act 2018 and as modified by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("the applicable data protection regime"), applies and provided that the United Kingdom does not exercise the designated powers without the agreement of the Union within the Partnership Council.

(...)

4) The "specified period" begins on the date of entry into force of this Agreement and, subject to paragraph 5, ends:

(a) on the date on which adequacy decisions in relation to the UK are adopted by the European Commission under Article 36(3) of Directive (EU) 2016/680 and under Article 45(3) of Regulation (EU) 2016/679, or

(b) on the date four months after the specified period begins, which period shall be extended by two further months unless one of the Parties objects;

whichever is earlier."

Praxistipp: Was ist jetzt datenschutzrechtlich zu beachten?

- Bis die genannte Frist abgelaufen ist, können Daten erstmal wie zuvor in das Vereinigte Königreich übermittelt werden (https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Brexit-Uebergangsfrist/Brexit-Uebergangsfrist.html).
- Derzeit ist unklar, wann es einen Angemessenheitsbeschluss für das Vereinigte Königreich geben wird. Wen Unternehmen ganz sichergehen möchten, sollten diese vorsorglich innerhalb der Übergangsfrist entsprechende Garantien, wie z.B. Standardvertragsklauseln, implementieren. Andernfalls sollten die Entwicklungen zumindest genau beobachtet werden.
- Sofern für ein Unternehmen nach Art. 27 DS-GVO ein Vertreter zu bestellen ist und der bestellte Vertreter im Vereinigten Königreich niedergelassen ist, sollte das Unternehmen einen anderen, in der EU niedergelassenen Vertreter bestellen.
- Unternehmen, die Übermittlungen von Daten in Drittländer auf Binding Corporate Rules (BCR) stützen und diese von der britischen Aufsichtsbehörde ICO genehmigt wurden, sollten prüfen, ob die BCR weiterhin herangezogen werden können.
- Die EU-Kommission ist jetzt aufgefordert, tragfähige Angemessenheitsentscheidungen vorzulegen, die die aktuelle Rechtsprechung des EuGHs zu Schrems II berücksichtigen.

Die SKW Taskforce Datenschutz hält Sie selbstverständlich eng über die weiteren Entwicklungen zum Datentransfer in das Vereinigte Königreich unterrichtet.

Dr. Oliver Hornung, Frankfurt / Main
o.hornung@skwschwarz.de
Philipp Sauer, Frankfurt / Main
p.sauer@skwschwarz.de