UIMCommunic@tion
praxisnah.gut.informiert.

05/2022

Ausgabe für Deutschland

Betriebliches Eingliederungsmanagement transparent gestalten

Datenschutz beim BEM umsetzen schützt vor juristischen Pleiten

Das Betriebliche Eingliederungsmanagement (BEM) soll Arbeitnehmern nach einer längeren Arbeitsunfähigkeitsperiode eine geordnete Rückkehr in ihren Betrieb ermöglichen. Im Idealfall profitieren von diesem Instrument beide: Arbeitnehmer und Arbeitgeber. Ziel ist es, mit gesunden, motivierten und gut qualifizierten Beschäftigten überdurchschnittliche Arbeitsergebnisse zu erzielen. Soweit der Idealzustand. „Das BEM hält einige datenschutzrechtliche Fallstricke für Arbeitgeber bereit, die zweifelsohne herausfordernd, aber in jedem Fall zu meistern sind", erklärt Datenschutzexperte Dr. Jörn Voßbein. Was bei einem BEM verlangt wird und wie die Regeln des Datenschutzes erfolgreich umgesetzt werden können, sind die Fragen, die beantwortet werden sollen. Ein Fall aus Baden-Württemberg dient dabei als Beispiel.

Ein BEM kann nur mit Einwilligung des Beschäftigten durchgeführt werden. Gegen seinen Willen funktioniert ein BEM nicht. Mit der Verarbeitung seiner Gesundheitsdaten muss der Arbeitnehmer einverstanden sein. Dabei ist darauf zu achten, dass mögliche Einwilligungserklärungen nicht zu weit gehen und freiwillig erfolgen. Sensible Gesundheitsdaten müssen in keinem Fall Dritten im Betrieb offengelegt werden.

Eine beschäftigte Arbeitnehmerin fehlte häufig wegen Kurzerkrankungen. Der Arbeitgeber startete mit einem Einladungsschreiben ein BEM. Dem Brief war eine „Datenschutzerklärung" beigefügt, mit der die Mitarbeiterin aufgefordert wurde, in die Nutzung ihrer Gesundheitsdaten im Zusammenhang mit dem BEM einzuwilligen. Die datenschutzrechtliche Einwilligung des Beschäftigten ist in Art 9 Abs. 2a DSGVO verankert. Es wäre alles rechtmäßig verlaufen, wenn der Arbeitgeber in der Einwilligungserklärung nicht über das Ziel hinausgeschossen wäre. Er forderte nämlich nicht nur das Einverständnis für die „Erhebung" und „Nutzung" ihrer Gesundheitsdaten im Rahmen des BEM, sondern auch noch das Einverständnis für die „Bekanntmachung" gegenüber ihrem Vorgesetzten und der Standortleitung. Die Arbeitnehmerin reagierte nicht auf die BEM-Einladung.

Stattdessen reagierte der Arbeitgeber: Er kündigte die Mitarbeiterin. Diese reichte eine Kündigungsschutzklage ein, die in 2 arbeitsgerichtlichen Instanzen bestätigt wurde. „Die Kündigung ist nicht sozial begründet" heißt es im Urteilsspruch. Die Unverhältnismäßigkeit der Kündigung hatte sich der Arbeitgeber mit einer unausgegorenen datenschutzrechtlichen Einwilligungserklärung zuzuschreiben. Sie war zu weit gefasst und wurde vom Landesarbeitsgericht verworfen. Es bestehen, laut den Arbeitsrichtern, die berechtigten Interessen des Beschäftigten gegen eine umfassende Informationssammlung, um es dann auf den Punkt zu formulieren: „Die Beachtung des Datenschutzes ist in § 167 Abs. 2 SGB IX zwar verklausuliert, aber dennoch ausdrücklich vorgeschrieben." Gerade die Einwilligung zur angestrebten „Bekanntmachung" der Gesundheitsdaten sei nicht von der Arbeitnehmerin hinzunehmen.

„Es kommt auf die Einwilligungserklärung an. Sie muss sauber, präzise, datenschutzkonform sowie rechtssicher formuliert werden. Dann können solche arbeitsrechtlichen Streitfälle zwar nicht verhindert werden, aber sie nehmen einen anderen Ausgang", unterstreicht UIMC-Geschäftsführer Dr. Jörn Voßbein.

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Wir freuen uns über Ihren Anruf!
+49 202 946 7726 200

UIMCommunication
praxisnah.gut.informiert.

Angriffe, Social Engineering & andere Gefahren

„Vor dem Hintergrund der politischen Lage“ sei mit Angriffen auf deutsche Webseiten zu rechnen – so hat das Bundesamt für Verfassungsschutz die Unternehmen und Behörden gewarnt. Konkret wird vor Attacken der prorussischen Hacker-Gruppierung „Killnet“ gewarnt. In den vergangenen Wochen waren die pro-russischen Aktivisten offenbar mit einigen Angriffen gegen die Websites deutscher Behörden erfolgreich. Die Seiten des Bundeskriminalamtes (BKA) und der Bundespolizei waren offenbar bereits Ziele von massenhaften, koordinierten Störversuchen.

Das klingt erstmal bedrohlich. Die offenbar Putin-treuen Hacker führten aktuell „eine Kampagne gegen diverse deutsche Webseiten aus Privatwirtschaft und Forschung“, heißt es im Sicherheitshinweis des deutschen Inlandsgeheimdienstes. Gewarnt wird insbesondere vor sogenannten DDoS-Angriffen, die zum Ziel haben, Websites durch massenhafte künstliche Aufrufe lahmzulegen. Nebenbei warnt das Amt auch vor der Ransomware-Gruppierung „Revil“. Die Gruppe erpresst ihre Opfer, nachdem sie deren Systeme lahmgelegt hat.

Doch neben den o. g. Angriffsszenarien kommt dem Social Engineering eine immer stärkere Bedeutung zu. Hierbei handelt es sich um Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen oder zum Klicken eines (virenbehafteten) Links zu bewegen.

Dass die Warnungen nicht abstrakt, sondern sehr konkret sind, zeigt auch, was „Killnet“ unternimmt. Die „Killnet“-Hacker haben in ihrem Kanal auf dem Messengerdienst Telegram eine Liste mit den Webadressen verschiedener deutscher „Ziele“ gepostet – offenbar als Aufruf an ihre Gefolgschaft.

Die UIMC ist hier ganz konkret unterwegs und rät Personalabteilungen, Beschäftigte mit russischer Staatsangehörigkeit auf Möglichkeiten von Anbahnungsversuchen durch russische Geheimdienste hinzuweisen. Außerdem sollten Meldewege für Verdachtsfälle etabliert werden. Konkrete Bedrohungen und Verdachtsfälle sollten umgehend gemeldet werden.

Grundsätzlich sollten E-Mails misstraut werden, die zu dringenden Handlungen auffordern; dies gilt auch für E-Mails aus dem Familien- oder Bekanntenkreis. Passwörter sollen niemals angegeben werden. Ebenfalls sollen keine Links oder Anhänge verdächtiger E-Mails geöffnet werden. Nach Möglichkeit soll Schutz der Mail- und weiterer besonders sensibler Konten mittels Multi-Faktor-Authentifizierung erfolgen.

Gesamter Artikel unter www.uimc.de/news

web.eCollege
kompakt praxisnah informieren

Sie haben das letzte web.eCollege verpasst, würden aber gerne noch mehr zum den vergangenen Themen erfahren? Dann schauen Sie sich die Unterlagen und/oder die Aufzeichnung an:

http://update.uimcollege.de

Sie können sich als Gast anmelden. Hierzu geben Sie bitte den Code ein, den Sie bei uns erfragen können.
Sofern Sie als Kunde bereits Zugangsdaten für einen anderen Kurs im eCollege haben, können Sie sich auch „selbst einschreiben“. Die Einschreibung bleibt einen Monat bestehen.

Die nächsten Termine [kostenfrei]

08.06.2022: [Basics] Know What, Know How: Die 10 wichtigsten Maßnahmen im Datenschutz

13.07.2022: 7 nützliche Tipps für eine Lieferantenbewertung / Dienstleister-Auditierung

10.08.2022: 5 Anforderungen beim Drittlandtransfer

Anmeldung unter www.uimc.de/webecollege

Aktuelles im Online-Formular-Center

» alle Unterlagen sind aktuell

Um über Neuerungen zeitnah informiert zu werden, können Sie künftig unser News-Forum abonnieren und erhalten daraufhin eine E-Mail (siehe oben).

www.uimcollege.de

Mehr Informationen, Hinweise & Tipps finden Sie hier: https://www.UIMC.de/communication

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.