EU-DSGVO und IT-Administrations-kontrolle – was gilt es zu beachten?

Am 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung (EU-DSGVO) in vollem Umfang. Insbesondere für den Bereich der technisch-organisatorischen Datensicherheit gelten dann verschärfte Bedingungen. Ein ganz spezifisches Instrument kann datenverarbeitende Unternehmen in Deutschland darin unterstützen, ihre datenschutzrechtliche Pflicht zur Gewährleistung der „Sicherheit der Verarbeitung" gemäß Artikel 32 DSGVO zu erfüllen: die sogenannte „Administrationskontrolle" bzw. das „Privileged Access Management". Gegenwärtig bietet der Markt unter diesen Bezeichnungen diverse IT-Lösungen an, die eine wirksame Kontrolle von Benutzern mit erweiterten Berechtigungen ermöglichen sollen. Tilman Dralle von TÜV Rheinland beschreibt den Nutzen einer solchen Administrationskontrolle aus Sicht der technisch-organisatorischen Datensicherheit und erläutert mögliche datenschutzrechtliche Bedenken im Zusammenhang mit dem Einsatz entsprechender IT-Lösungen.

IT-Administrationskontrolle: Zweck und Funktionsweise

Die Administrationskontrolle bzw. das „Privileged Access Management" verfolgt ein zentrales Ziel: die Aktivitäten von Nutzern mit privilegierten Berechtigungen zu analysieren und zu protokollieren. Applikations-, System- und Netzwerkadministratoren unterliegen aufgrund ihrer herausgehobenen Stellung keinen nennenswerten Zugriffsbeschränkungen. Deshalb haben sie in der Regel Zugang zu einer Vielzahl personenbezogener Daten. Dazu können besondere Kategorien personenbezogener Daten zählen, wie z.B. Gesundheitsdaten. Zu der Gruppe mit umfassenden Berechtigungen gehören neben internen Mitarbeitern regelmäßig auch Mitarbeiter von externen Dienstleistern, die im Rahmen ihrer Dienstleistungserbringung – z.B. Prüf- oder Wartungsdienstleistungen – auf die IT-Infrastruktur des Auftraggebers zugreifen müssen und dabei zumindest potenziell Zugriff auf große Mengen personenbezogener Daten haben. Schließlich ist es auch möglich, dass sich ein Hacker eines Administratoraccounts bemächtigt.

Um zu verhindern, dass privilegierte Nutzer unbefugt auf personenbezogene Daten zugreifen, diese unbefugt verändern, übermitteln oder auf sonstige Weise verändern, lassen sich die Aktivitäten eines solchen Accounts im Rahmen einer Administrationskontrolle überwachen. Zu diesem Zweck wird der gesamte „User-Traffic" mitgeschnitten und in Form von sogenannten „Audit-Trails", d.h. Videosequenzen, aufgezeichnet. So lässt sich beispielsweise nachvollziehen, welcher Administrator zu welchem Zeitpunkt auf welche Datenbank bzw. welchen Server zugreift, welche Befehle er dort ausführt, und welche Dateien er aufruft, herunterlädt oder modifiziert. Die Audit-Trails können später wiedergegeben und für forensische Untersuchungen durchsucht und analysiert werden. Neben der manipulationssicheren Aufzeichnung von Remotezugriffen bieten die entsprechenden IT-Lösungen auch Schutz vor bestimmten schädlichen Aktionen.

Angemessenes Schutzniveau gewährleisten

IT-Lösungen zur Administrationskontrolle leisten einen klaren Beitrag zur Umsetzung der datenschutzrechtlichen Verpflichtungen aus der EU-DSGVO. Nach Artikel 32 Abs. 1 EU-DSGVO müssen alle datenverarbeitenden Unternehmen in Deutschland geeignete technische und organisatorische Maßnahmen (TOMs) treffen, um ein Schutzniveau zu gewährleisten, das dem mit der Datenverarbeitung verbundenen Risiko angemessen ist. Bei der Auswahl der TOMs sind u.a. der Stand der Technik, die Implementierungskosten sowie die Eintrittswahrscheinlichkeit und das Schadenspotenzial möglicher Risikoszenarien zu berücksichtigen. Die von der EU-DSGVO vorgegebenen Schutzziele sind Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit.

Eine wirksame Administrationskontrolle sorgt in erster Linie dafür, dass Nutzer mit erweiterten Berechtigungen nur dann auf personenbezogenen Daten zugreifen (können), wenn dies für ihre Aufgabenerfüllung unbedingt erforderlich ist. Insofern steht hier das Schutzziel der Vertraulichkeit im Vordergrund. Darüber hinaus zahlt ein „Privileged Access Management" aber auch auf das Schutzziel Integrität ein. Denn es ermöglicht eine nachträgliche Überprüfung und Feststellung, ob und ggf. von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder gelöscht wur-

den. Auch wenn Artikel 32 Abs. 1 EU-DSGVO eine risikoorientierte Auswahl von Datensicherheitsmaßnahmen vorschreibt und pauschale Aussagen folglich nicht möglich sind, ist als Ergebnis festzuhalten, dass die Administrationskontrolle für viele Unternehmen ein wichtiger Baustein für die Wahrung von Vertraulichkeit und Integrität ihrer personenbezogenen Daten ist. Wenn darüber hinaus bestimmte Risikofaktoren vorliegen (z.B. Datenverarbeitung in großem Umfang, Verarbeitung von vertraulichen oder höchst sensiblen Daten), steigt tendenziell der Rechtfertigungsdruck für das jeweilige Unternehmen im Rahmen der von Artikel 32 EU-DSGVO geforderten Abwägungsentscheidung.
Ist die „Verletzung des Schutzes personenbezogener Daten" im Sinne von Artikel 4 Nr. 12 EU-DSGVO bereits eingetreten, können die Audit-Trails auch dazu genutzt werden, der Aufsichtsbehörde bzw. den von der Datenschutzpanne betroffenen Personen die gemäß Artikel 33-34 EU-DSGVO erforderlichen Informationen zur Verfügung zu stellen.

Datenschutzrechtliche Anforderungen beachten

Eine professionelle Administrationskontrolle soll u.a. helfen, datenschutzrechtliche Anforderungen umzusetzen. Selbstverständlich müssen aber auch die entsprechenden IT-Lösungen selbst den datenschutzrechtlichen Anforderungen gerecht werden, denn auch Nutzer mit erweiterten Berechtigungen genießen den Schutz der EU-DSGVO. Vor diesem Hintergrund ist es durchaus verständlich, dass Betriebsräte vereinzelt Bedenken hinsichtlich der datenschutzrechtlichen Kompatibilität von „Privileged Access Management"-Lösungen geäußert haben. Diese Bedenken lassen sich jedoch ausräumen.

Die Aufzeichnung der Administratoraktivitäten und das Fertigen entsprechender Audit-Trails stellen fraglos Datenverarbeitungen dar, die eines Zulässigkeitstatbestandes bedürfen. Auch wenn durch die Überwachungsmechanismen u.a. auch Straftaten aufgedeckt werden können, so sollte die hierfür einschlägige Rechtsgrundlage nicht in § 26 Abs. 1 S. 2 BDSG n. F. (Verarbeitung von Beschäftigtendaten zur Aufdeckung von Straftaten), sondern in § 26 Abs. 1 S. 1 BDSG n. F. gesucht werden. Danach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses u.a. dann verarbeitet werden, wenn dies für dessen Durchführung erforderlich ist.
Die Erforderlichkeit einer Administrationskontrolle und der damit verbundenen Datenverarbeitung für die Durchführung des Beschäftigungsverhältnisses ist bei IT-Verantwortlichen mit umfangreichen Zugriffsrechten grundsätzlich klar gegeben. Ein milderes Mittel mit gleicher Effektivität ist auf den ersten Blick nicht ersichtlich. Wenn Administratoren eines externen Auftragsverarbeiters beim Remotezugriff überwacht werden, ist der Rückgriff auf die Rechtsgrundlage in § 26 Abs. 1 S. 1 BDSG n. F. nicht möglich, da es sich hier nicht um Beschäftigte im Sinne von § 26 Abs. 8 BDSG n. F. handelt. In diesem Fall bietet sich die Interessenabwägung nach Artikel 6 Abs. 1 Buchst. f der EU-DSGVO an. Da die Datenverarbeitung ausschließlich im Zusammenhang mit dem Zugriff auf kritische IT-Systeme erfolgt, ist mit guten Gründen davon auszugehen, dass hier die berechtigten Interessen des Verantwortlichen grundsätzlich gegenüber den Interessen bzw. Grundrechten und Grundfreiheiten der betroffenen Person überwiegen.
Dieser Befund der grundsätzlichen Rechtmäßigkeit einer IT-basierten Administrationskontrolle wird auch nicht durch ein kürzlich ergangenes Urteil des Bundesarbeitsgerichts (BAG) erschüttert (Urteil vom 27.7.2017, 2 AZR 681/16). In diesem Fall hatte das BAG entschieden, dass der Einsatz eines Software-Keyloggers, mit dem alle Tastatureingaben an einem dienstlichen Computer für eine verdeckte Überwachung und Kontrolle des Arbeitnehmers aufgezeichnet werden, nach § 32 Abs. 1 BDSG a. F. (entspricht § 26 Abs. 1 BDSG n. F.) unzulässig ist, wenn kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung besteht. Das BAG-Urteil kann nicht gegen eine Administrationskontrolle in Stellung gebracht werden, da beim „Privileged Access Management" kein pauschales Monitoring von Mitarbeiter-Aktivitäten auf den jeweiligen Clients erfolgt, sondern nur die Zugriffe privilegierter Nutzer auf bestimmte kritische Systeme der insofern zeitlich und sachlich klar begrenzten Aufzeichnung unterliegen. Aus diesem Grund wird auch kein „umfassendes und lückenloses Profil" weder von der dienstlichen noch der privaten Nutzung durch die betroffene Person erstellt.
Es bleibt folglich dabei, dass die der Administrationskontrolle immanente Datenverarbeitung im Grundsatz über § 26 Abs. 1 S. 1 BDSG n. F. bzw. Artikel 6 Abs. 1 Buchst. f EU-DSGVO gerechtfertigt werden kann. Allerdings müssen – wie bei jedem IT-System – auch bei „Privileged Access Management"-Lösungen systeminterne und -externe Maßnahmen ergriffen werden, um den Dienst EU-DSGVO-konform auszugestalten.

Konkrete Maßnahmen zur Sicherstellung der EU-DSGVO-Kompatibilität

Zunächst ist die Zweckbindung der entsprechenden personenbezogenen Daten zu berücksichtigen (siehe Artikel 5 Abs. 1 Buchst. b EU-DSGVO). Danach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden (hier die Administrationskontrolle) und dürfen nicht zu inkompatiblen Zwecken weiterverarbeitet werden. Folglich dürfen die Audit-Trails nicht für eine Leistungskontrolle der externen oder internen Mitarbeiter genutzt werden. Auch der Grundsatz der Speicherbegrenzung muss beachtet werden (siehe Artikel 5 Abs. 1 Buchst. e und Artikel 17 DS-GVO). Die aufgezeichneten Audit-Trails dürfen nicht „auf Vorrat" gespeichert werden, sondern müssen nach einer entsprechenden Vorhaltefrist gelöscht werden. Die Speicherdauer ist dabei strikt an der Zweckbestimmung der Datenverarbeitung auszurichten.

Darüber hinaus gilt selbstverständlich auch für die in den Audit-Trails verkörperten personenbezogenen Daten der Grundsatz der Vertraulichkeit (siehe Artikel 5 Abs. 1 Buchst. f und Artikel 32 EU-DSGVO). Da beispielsweise Passwörter in den Audit-Trails sichtbar sind, soweit sie in den administrativen Verbindungen im Klartext eingegeben werden, muss der Zugriff auf diese Sitzungsprotokolle sinnvoll eingeschränkt werden. Dies kann insbesondere durch eine entsprechende Verschlüsselung (zumindest des „Upstream-Trails", in dem die Tastatureingaben wie Passwörter enthalten sind) erfolgen. Durch eine Verschlüsselung mit zwei Zertifikaten kann sichergestellt werden, dass nur ein fest definierter Personen-Kreis im Rahmen des Vier-Augen-Prinzips auf die Protokolle zugreifen kann. Der private Schlüssel zu einem dieser Zertifikate sollte im Besitz des Betriebsrates sein. Ein Kritikpunkt aus Datenschutzsicht ist allerdings, dass die Verschlüsselung in der Regel manuell aktiviert werden muss. Um den „Privacy-by-Design"-Anforderungen der EU-DSGVO zu genügen, sollte ein entsprechender Druck auf die Hersteller ausgeübt werden, damit diese Anforderungen bereits in der Entwicklung berücksichtigt werden.

Betriebsrat und Mitarbeiter frühzeitig ins Boot holen

Generell gilt: Für die Umsetzung einer Administrationskontrolle bedarf es der frühzeitigen Einbindung des Betriebsrats sowie der betroffenen Mitarbeiter. Denn nur so ist eine entsprechende Akzeptanz erreicht werden. Der Betriebsrat ist nach den Vorschriften des BetrVG ohnehin mitbestimmungspflichtig, da es sich bei den in Rede stehenden IT-Lösungen um technische Einrichtungen handelt, die dazu geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, auch wenn dieser Zweck tatsächlich nicht verfolgt wird (vgl. § 87 Abs. 1 Nr. 6 BetrVG). Auch den betroffenen Mitarbeitern, d.h. den IT-Verantwortlichen, sollte der Mehrwert einer wirksamen Administrationskontrolle klar vor Augen geführt werden: Schutz von Geschäftsgeheimnissen und anderen vertraulichen Informationen durch erhöhte Informationssicherheit sowie Umsetzung von regulatorischen Anforderungen im Bereich Datenschutz und damit Reduzierung entsprechender Reputations- und Bußgeldrisiken (siehe Artikel 83 EU-DSVO). Darüber bietet ein „Privileged Access Management" für IT-Administratoren im Fall einer Störung oder einer Datenschutzpanne die Möglichkeit, anschaulich nachzuweisen, dass sie gute und fehlerfreie Arbeit geleistet haben.Schlussendlich ist ein hohes Maß an Transparenz auch für die Erfüllung der Informationspflichten nach Artikel 13 und 14 EU-DSGVO erforderlich. So müssen die internen bzw. externen Mitarbeiter insbesondere über den Zweck der mit der Administrationskontrolle verbundenen Datenverarbeitung und deren Rechtsgrundlage informiert werden.

Fazit

Eine wirksame Administrationskontrolle mithilfe entsprechender IT-Lösungen ist ein effektives Instrument, um den Missbrauch von erweiterten Berechtigungen zu verhindern, und leistet somit einen nicht zu unterschätzenden Beitrag zur Gewährleistung der Vertraulichkeit und Integrität personenbezogener Daten gemäß Artikel 32 EU-DSGVO. Gleichzeitig kann eine Administrationskontrolle auch ein wichtiger Bestandteil eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001:2013 bzw. eines Konzepts zur Umsetzung der „Bankaufsichtlichen Anforderungen an die IT" (BAIT) der Bundesanstalt für Finanzdienstleistungsaufsicht sein, um hier nur zwei Beispiele zu nennen. Grundsätzlich ist eine IT-basierte Administrationskontrolle datenschutzrechtlich zulässig. Bei der Implementierung entsprechender Lösungskonzepte sind allerdings eine Reihe von Datenschutzaspekten (Zweckbindung der Daten; Zugriffsbeschränkung auf die Sitzungsprotokolle; Löschpflichten) zu beachten und der Betriebsrat sowie die entsprechenden IT-Verantwortlichen frühzeitig eingebunden werden.

Autor: Tilman M. Dralle, LL.M. (Nottingham), Heidelberg, TÜV Rheinland, Security Consultant mit Schwerpunkt im Bereich Informationssicherheit und Datenschutz