GDPR und die neue Rolle des Data Protection Officer (DPO)

Wiesbaden, 17. August 2017 – Die Uhr tickt: Mai nächsten Jahres beginnt eine neue Ära der europäischen Datenschutzgesetze. Die EU-Datenschutz-Grundverordnung (GDPR) gilt für alle Mitgliedsstaaten der Europäischen Union (einschließlich des Vereinigten Königreichs, vor und voraussichtlich auch nach dem Brexit). Bis heute wurde viel über Strafen und Sanktionen bei Verstößen diskutiert, darunter bis zu 20 Mio. Euro oder 4 Prozent des jährlichen weltweiten Umsatzes eines Unternehmens. Dennoch scheint die Anforderung an die Rolle des Data Protection Officer (DPO) in Unternehmen bisher noch eine untergeordnete Rolle zu spielen. „In der Vergangenheit war die Rolle des DPO weitgehend undefiniert, denn das aktuell noch bestehende europäische Datenschutzgesetz stammt aus einer EU-Richtlinie von 1995, welche derartige Rollen und Aufgaben noch nicht in dem Maße berücksichtigt, wie in der GDPR“, erklärt Michael Veit, IT-Security Experte bei Sophos.

In jenen Tagen wurden Daten fast ausschließlich im „Computing-Kontext“ gesehen und die ersten Personen, die den informellen Titel des DPO erhielten, hatten meist einen IT-Hintergrund. Sie waren diejenigen, die den Fluss von computergesteuerten Daten verstehen, identifizieren und „schützen“ konnten. Heute, in einer Zeit in der Technik unser Leben so sehr bestimmt, haben sich Rolle und Aufgabe eines DPO maßgeblich verändert. Heute ist der DPO die Instanz für Datenschutz innerhalb einer Organisation. Der DPO muss einem Unternehmen oder einer Organisation helfen, den gesetzlichen Verpflichtungen nachzukommen - auch hinsichtlich der Achtung der Privatsphäre von Privatpersonen.

Es geht generell um Sicherheit und diese beinhaltet nicht nur die Sicht auf die IT, sondern auch die Kompetenz in den Bereichen Recht, Compliance oder Kundenservice und viele mehr. Um die Richtlinien einzuhalten, formuliert die GDPR die Rolle eines DPO und verpflichtet auch deren Einsatz in Unternehmen und Organisationen. Zum Beispiel werden alle öffentlichen Einrichtungen einen DPO zwingend benötigen, um die Informationsfreiheit oder Menschenrechte zu garantieren. Dies bedeutet auch, dass unter Umständen auch sehr kleine Organisationen oder Unternehmen in der gesetzlichen Pflicht stehen, einen DPO zu haben - zum Beispiel Gemeinden oder staatlichen Schulen. Aber die Rolle ist auch für diejenigen Organisationen zwingend, deren Kerntätigkeiten eine „regelmäßige und systematische Überwachung von Daten in großem Maßstab“ beinhalten oder wenn die Kernaktivitäten die Verarbeitung von besonders sensiblen Daten beinhalten (z. B. Daten, die sich auf die ethnische Herkunft, religiöse Überzeugungen, Gesundheit, Sexualleben oder strafrechtliche Verurteilungen beziehen).

Gewisse und teilweise hilfreiche Leitlinien wurden von der Artikel-29-Arbeitsgruppe, einer Gruppe von Vertretern von Datenschutzbehörden der gesamten EU, erstellt. Diese Leitlinien erklären beispielsweise, dass kritische „Kernaktivitäten“ nicht die Verarbeitung von Personalinformationen innerhalb einer Personalabteilung betreffen - jegliche gegenteilige Ansicht hätte dazu geführt, dass jeder Arbeitgeber einen DPO benötigen würde.

Die GDPR beschreibt Strukturen und definiert einige der erforderlichen Qualitäten und Pflichten eines DPO. Folgende Qualifikationen sind erforderlich:
- Möglichkeit von „unabhängigem“ Handeln
- Unabhängig von Anweisungen des Arbeitgebers
- Kenntnis des Datenschutzrechts
- Ausreichende Ressourcen zur Erfüllung der Aufgaben
- Bericht direkt an die höchste Management-Ebene

Dabei muss ein DPO nicht unbedingt im eigenen Haus bestellt werden. Die GDPR macht deutlich, dass die Rolle auch von einem externen Spezialisten erfüllt werden kann. Dies ist zweifellos für die kleineren Organisationen hilfreich. Diese würden es schwer haben einen qualifizierten internen Mitarbeiter für die Aufgaben eines DPO zu finden. Denn laut Artikel 29 der Leitlinien, darf zusätzlich zur Qualifikation auch kein Interessenkonflikt stattfinden. Einige Rollen im Unternehmen sind mit dem DPO nicht vereinbar, darunter beispielsweise der CEO, CFO, Marketingleiter, HR oder IT.

Was passiert aber, wenn eine Organisation einen DPO nach GDPR ernennen muss, dies aber unterlässt? In der Theorie könnte eine solche Verletzung eine „niedrigere" Geldbuße von bis zu 10 Mio. Euro oder 2 Prozent des jährlichen weltweiten Umsatzes zur Folge haben. Soweit zur Theorie, denn es ist vermutlich nicht zu erwarten, dass ein Datenschutzkontrolleur jemals eine solche Geldbuße nur für das Versäumnis, einen DPO zu ernennen, erheben wird. Tragisch wird die Situation, wenn neben der Nicht-Ernennung eines DPO substanzielle Verstöße gegen die GDPR begangen werden.
„Generell sollte jedes Unternehmen oder jede Organisation einen DPO ernennen, auch solche, die es laut Vorgaben nicht müssen. Denn Compliance und organisatorische Verbesserungen müssen für die kommende Jahre angestoßen und justiert werden", sagt Michael Veit, IT-Security Experte bei Sophos.

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de