Lookout

WHITEPAPER

DSGVO-Verstöße in einem Mobile-First Umfeld verhindern

Wie Sie mobile Bedrohungen und Risiken erkennen, durch die Bußgelder drohen

> „Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‚Integrität und Vertraulichkeit').“
>
> DSGVO, Artikel 5, §1(f)

Die DSGVO kommt sicher – und bestimmt den Umgang mit personenbezogenen Daten in Ihrem Unternehmen

Die Sicherheits- und IT-Teams, aber auch die Führungs- und Vorstandsetagen vieler weltweit agierender Unternehmen erwarten das Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) mit Spannung – und das ist gut so. Die vom Parlament, dem Rat und der Kommission der Europäischen Union ausgearbeitete Verordnung tritt am 25. Mai 2018 in Kraft. Sie hat das Ziel, den Datenschutz und das Recht auf Privatsphäre von natürlichen Personen innerhalb der EU zu stärken. Die DSGVO regelt auch den Export „personenbezogener Daten“ aus der EU, also allen Informationen im Zusammenhang mit bestimmten und bestimmbaren Personen.

Begriffsdefinitionen	
Personenbezogene Daten	Alle Informationen im Zusammenhang mit bestimmten und bestimmbaren natürlichen Personen („Datensubjekt“).
Natürliche Person	Ein lebendiger Mensch
Datensubjekt	Jede Person, deren personenbezogene Daten im Besitz eines Unternehmens sind

Jede Organisation, die Daten im Zusammenhang mit Einzelpersonen in Europa verarbeitet, muss sich jetzt schon auf die Einhaltung dieser Verordnung vorbereiten. Das betrifft viele, auch Unternehmen mit Hauptsitz in den USA, die in Europa geschäftlich tätig sind oder dort Dienstleistungen anbieten.

Gleichzeitig nimmt die Nutzung von Mobilgeräten immer weiter zu. Durch die digitale und mobile Transformation sind Mobilgeräte in nahezu jedem Unternehmen ein essenzieller Bestandteil des Arbeitsalltags. Diese tiefgreifende Umwälzung setzt personenbezogene Daten auf Mobilgeräten aber auch einem Risiko aus. Allen Abteilungen und Mitarbeitern, die auf personenbezogene Kunden-, Partner- oder Angestelltendaten zugreifen können, drohen Datenmanipulationen über das jeweilige Mobilgerät – und damit Verstöße gegen die DSGVO.

Das Marktforschungsunternehmen Gartner Inc. berichtete in Revisit Your Enterprise Mobility Management Practices to Prepare for EU GDPR: „Bis 2019 werden 30 % der Organisationen die DSGVO-Vorschriften zum Schutz personenbezogener Daten auf Mobilgeräten nicht einhalten können und deshalb unter starkem finanziellen Druck seitens der Aufsichtsbehörden stehen."

Um dies zu vermeiden und vollständig DSGVO-compliant zu sein, müssen Unternehmen ihr mobiles Risikospektrum kennen und personenbezogene Daten beim mobilen Arbeiten vor Compliance-Risiken schützen.

Eine Druckversion der Matrix für mobile Risiken finden Sie hier.

Warum mobiles Arbeiten für die DSGVO-Compliance ein Problem ist

Besonders durch die digitale Transformation wird immer häufiger über Mobilgeräte auf vertrauliche personenbezogene Daten zugegriffen. Da Unternehmen mittlerweile viele Daten in die Cloud verlagern und gleichzeitig auf Mobilgeräten bereitstellen, setzen sie sie auch breitgefächerten Risiken durch Malware, der Ausnutzung von Schwachstellen sowie versehentliche Datenlecks aus.

Mitarbeiter sind heute so flexibel in ihrer Arbeitsgestaltung wie nie. Sie haben die Wahl zwischen unterschiedlichen Arbeitsgeräten und -orten, Apps und Netzwerken, über die sie auf Unternehmensdaten und -anwendungen zugreifen können. Dazu zählen auch Privatgeräte mit selbstgewählten Apps sowie unternehmenseigene und -kontrollierte Geräte. Die mobile Arbeitsweise versetzt Mitarbeiter in die Lage, standortunabhängig auf arbeitsrelevante Daten und Netzwerke zuzugreifen.

Viele aktuelle Anbieter für hard- und softwareorientierte Sicherheit blenden das mobile Risikospektrum jedoch aus. Vor Jahren entwickelte Produkte berücksichtigten schon damals nicht die Sicherheit mobiler Endgeräte und selbst Tools für das Mobilgerätemanagement schützen nicht vor allen mobilen Bedrohungen, Schwachstellen oder riskanten Verhalten.

Angesichts dieser Mobile-Security-Lücke riskieren Unternehmen erhebliche Sicherheitsverstöße, die oft in exponierten Daten, finanziellen Verlusten, Rechtsstreitigkeiten und Ansehensverlusten für Organisation und Marke enden. Doch das ist noch nicht alles: Mobilgeräte stellen für Unternehmen mittlerweile ein großes Compliance-Risiko dar. Dieselben Richtlinien, die für fest installierte Endgeräte gelten, müssen jetzt auch auf mobile Endgeräte angewendet werden.

Unternehmen müssen sich der Tatsache stellen, dass es zu Datenmanipulationen auf Mobilgeräten kommen kann. Und dass sowohl Hackerangriffe als auch unbeabsichtigte Datenlecks von Apps Compliance-Probleme schaffen können, die in empfindlichen Bußgeldern und anderen negativen Folgen resultieren.

Die Frage ist nun: Wie kann meine Organisation die Sicherheit der über unsere Mobilgeräteflotte abgefragten Daten sicherstellen? Die jeweils gewählte Lösung wird sich jedenfalls auf die Fähigkeit der Organisation auswirken, wertvolles geistiges Eigentum zu schützen und compliant zu sein.

84%

der IT-Führungskräfte in den USA befürchten, dass der Zugriff auf personenbezogene Daten über die Mobilgeräte der Mitarbeiter eine Verletzung der DSGVO darstellen könnte.*

64%

der Angestellten in den USA geben an, über ihr Mobilgerät auf die Kunden-, Partner- und Mitarbeiterdaten ihres Unternehmens zuzugreifen.*

73%

verwenden für Privates und Berufliches dasselbe Telefon.*

* Ergebnisse einer Online-Umfrage unter US-amerikanischen und britischen Teilnehmern. Die Umfrage wurde vom 5. bis 15. September 2017 durchgeführt. Insgesamt beantworteten 2.062 Personen die Umfrage (exklusive Abbrüchen und Zeitüberschreitungen). Alle Befragten waren volljährig sowie Vollzeitangestellte eines Unternehmens mit mindestens 1.000 Mitarbeitern sowie Mitarbeitern und/oder Kunden/Partnern in der Europäischen Union (Großbritannien ausgenommen; wenn es sich nur um „Kunden/Partner" handelt, muss das Unternehmen deren personenbezogene Daten speichern). 1.000 Teilnehmer waren Entscheidungsträger oder an Entscheidungen zum Thema IT-Sicherheit beteiligt und hatten eine Position inne, die über der eines Praktikanten, Einsteigers oder Analysten/Associate liegt. Bei den anderen Teilnehmern handelte es sich um Unternehmensangestellte, für welche dieselben Kriterien galten. Die Stichprobe wurde vom Marktforschungsunternehmen Market Cube bereitgestellt. Alle potenziellen Teilnehmer erhielten die Einladung zur Umfrage per E-Mail. Die Fehlertoleranz beträgt 2,2 %.

Welche mobilen Bedrohungen und Risiken die DSGVO-Compliance gefährden

Zahlreiche Unternehmen stellen sich bereits der Herausforderung DSGVO-Compliance – viele davon befinden sich aber noch in der Evaluierungsphase.

Zu den zentralen Elementen der DSGVO gehört das Konzept „Datenschutz von Anfang an", also die proaktive Einbindung und Anwendung datenschutzrechtlicher Aspekte in IT-Systemen, Netzwerktechnik und Geschäftspraktiken.

Dieser „eingebaute" Datenschutz ist in der DSGVO eine rechtliche Anforderung für Unternehmen und Organisationen und erklärt im Grundsatzparagrafen des Textes in sechs Absätzen, wie mit EU-basierten personenbezogenen Daten umzugehen ist.

Acht Datenschutzprinzipien

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität
- Vertraulichkeit

Zum sechsten Datenschutzgrundsatz heißt es darin: „Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen."

Viele Unternehmen – auch solche, die bei der DSGVO-Compliance schon weiter sind – erkennen möglicherweise nicht die Auswirkungen von Mobiltechnologie auf ihren Konformitätsstatus.

Wie wirkt sich die DSGVO auf das mobile Arbeiten aus?

Umgang mit Daten

Unternehmen müssen wissen, welche Daten von wem mobil genutzt werden, wie der Zugriff geregelt ist und wohin die Daten gelangen.

Benachrichtigung bei Datenpannen

Unternehmen müssen jederzeit wissen, wie mobile Bedrohungen bei ihnen erkannt, gemeldet und zeitnah beseitigt werden.

„Datenschutz von Grund auf“

Unternehmen müssen die richtige Mischung aus Governance und Endanwenderdatenschutz finden und wissen, ob sie unwissentlich weitere personenbezogene Daten erfassen.

Vielfältige mobile Risiken bedrohen das 6. Datenschutzprinzip der DSGVO

- Bösartige Apps, die Daten aus- oder einschleusen, Geräte beschädigen, weil sie sich so tief darin einbetten, dass diese selbst durch das Zurücksetzen auf die Werkseinstellungen nicht entfernt werden können, und Unbefugten Remote-Zugriff verschaffen
- Gerätebedrohungen, die Angreifern zusätzliche Berechtigungen verschaffen, mit denen sie die gesamte Datenübertragung auf dem Gerät überwachen und Daten in verheerendem Ausmaß abziehen können
- Apps, die auf Kontaktdaten zugreifen und sie an Server außerhalb der EU senden
- Mobilgeräte in einem Netzwerk, das einem Man-in-the-Middle-Angriff ausgesetzt ist, bei dem Daten aus den Geräten abgezogen werden

Aufgrund der wachsenden Menge an Kundendaten und dem weitverbreiteten Einsatz von Mobilgeräten ist das Risiko eines Datenverlusts oder -lecks erheblich. Dabei spielt es keine Rolle, ob die fraglichen Geräte Eigentum des Unternehmens oder der Mitarbeiter sind. Gerade die Tendenz zum BYOD („Bring your own device“) verschärft die Komplexität der Sicherheitsanforderungen noch. In manchen Ländern nutzen weiterhin viele Menschen ihre privaten Smartphones und Tablets für Arbeitsaufgaben und riskieren dadurch Datenverlust, unzureichende Sicherheit durch veraltete Patches und andere Probleme, die sich aus der Nutzung nicht unternehmenseigener Mobilgeräte ergeben.

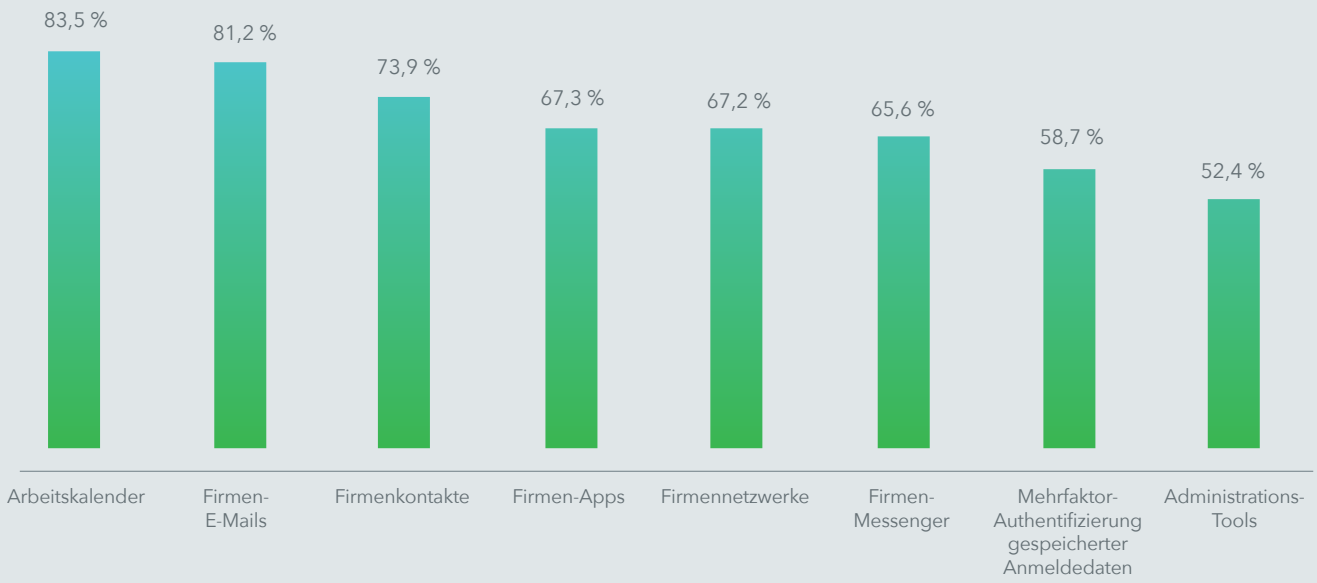
Mobilitätsrichtlinie Nr. 1: BYOD

Im November 2016 wurden erstmalig mehr Mobilgeräte als Desktop-Computer für den Internetzugang genutzt. Ihre Mitarbeiter verbringen wahrscheinlich mehr Zeit mit Ihrem Mobilgerät als mit ihren Computern, und arbeiten dann auch viel eher mit Apps als mit einem Browser. Häufig nutzen sie Mobilgeräte in der Öffentlichkeit, zum Beispiel im Café oder in der Hotellobby. Der Zugriff auf Unternehmensdaten erfolgt dann in der Regel über das öffentliche WLAN dieser Orte. Außerdem geht für viele Unternehmen der Trend weg vom dedizierten Rechenzentrum hin zur Cloud, was das mit dem Datenzugriff verbundene Risiko ebenfalls erhöhen kann.

Das zunehmend mobile Arbeiten in Verbindung mit der wachsenden Anzahl an Cloud Services und Apps hat bei vielen Unternehmen die Produktivität und Zusammenarbeit nachhaltig verbessert. Allerdings haben zentrale IT-Abteilungen und unternehmenseigene Sicherheitsprogramme so auch viel weniger Kontrolle über Daten und Systeme. Führen Sie sich nur einmal vor Augen, welche Daten und IT-Systeme üblicherweise auf einem Smartphone verfügbar sind: Firmen-E-Mails, Anmeldedaten für Firmen- und privat genutzte Portale, Unternehmensnetzwerke und -Apps sowie Funktionen wie Mikrofon und hochauflösende Kamera. Auf modernen Smartphones werden Unmengen an sensiblen Daten genutzt und gespeichert – und ihre Besitzer nehmen sie überall mit hin.

Sowohl Mobilgerätenutzer als auch die von ihnen genutzten Apps können sensible Daten einem Risiko aussetzen. So haben sie eventuell Zugriff auf personenbezogene Daten zu Kunden, können sensible Daten auf externe Server hochladen, Bestimmungen zur Datenhoheit verletzen oder Daten an riskante geografische Standorte übermitteln. Manche Apps greifen auf Cloud-Speicherdienste, Social-Networking-Dienste oder Peer-to-Peer-Netzwerke zu, und wieder andere verschlüsseln Daten, die sie speichern oder übermitteln, nicht ausreichend. Außerdem gibt es Apps mit bekannten Schwachstellen.

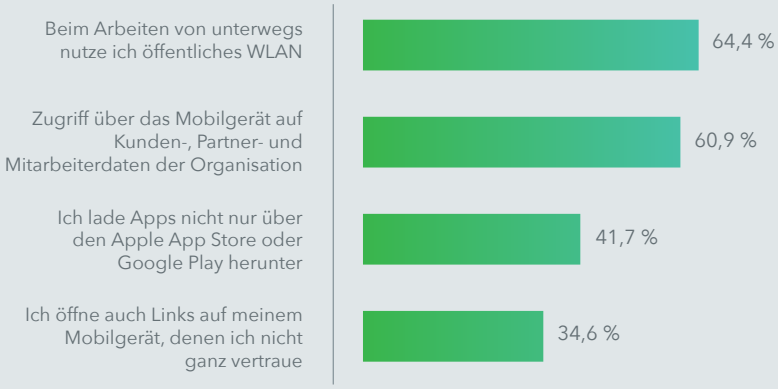
Die meisten Mitarbeiter nutzen Firmen-Apps für Kalender und E-Mails



Können Sie über das Mobiltelefon auf Folgendes zugreifen? J/N

Um DSGVO-Compliance zu erreichen, müssen Unternehmen Technologien bereitstellen, mit denen sie die Funktionen und das auffällige Verhalten der von Mitarbeitern genutzten Apps analysieren. Eine solche Lösung muss vor Angriffen auf Mobilgeräte schützen, also beim unfreiwilligen oder vom Anwender initiierten Jailbreaking und Ausnutzen von Betriebssystemschwachstellen sowie bei verloren gegangenen oder gestohlenen Geräten, Malware, nicht konformen Apps, App-Schwachstellen, Datenlecks und Man-in-the-Middle-Angriffen.

Mitarbeiterverhalten kann personenbezogene Daten auf Mobilgeräten gefährden



Wofür nutzen Sie Ihr Mobilgerät?

Haben Unternehmen Einblick in ihr mobiles Risikospektrum erlangt, geht es als nächstes darum, personenbezogene Daten in und aus der EU durch Richtlinien zu schützen, die Bedrohungen schnell zu beseitigen und das Datenverlustrisiko von Apps umfassend minimieren. Bei all dem muss natürlich die Privatsphäre der Endanwender gewahrt sein. „Umfassend" ist ein wichtiges Stichwort im Zusammenhang mit Richtlinien. Mit einer einzigen Richtlinien-Engine sollte es möglich sein, nicht konforme Verhaltensweisen und andere Risiken zu definieren, damit alle potenziellen Problembereiche in der Mobilgeräteflotte schnell in den Fokus rücken.

Wie Sie mobile Bedrohungen für die DSGVO-Compliance aufspüren und stoppen

Von der DSGVO betroffene Unternehmen und Organisationen brauchen Lösungen zur Abwehr mobiler Bedrohungen, z. B. Lookout Mobile Endpoint Security, die mittels Analysen und Richtlinien personenbezogene Daten in und aus der EU schützen und das Risiko messbar senken. So kann ihnen eine solche Lösung helfen, sich auf die DSGVO vorzubereiten:

- **Schnelle Erkennung von mobilen Risiken für personenbezogene Daten in und aus der EU.** Lookout Mobile Endpoint Security bietet Einblicke in das mobile Risikospektrum zur schnellen Erkennung signifikanter Probleme. Dazu dient ein Dashboard, das in großer Detailtiefe Informationen zur jeweiligen Bedrohung, Software-Schwachstelle oder riskanten Verhaltensweisen bzw. Konfigurationen liefert, die personenbezogene Daten in und aus der EU dem Risiko unbefugter Nutzung oder des Verlusts aussetzen könnten.
- **Implementierung umfassender Richtlinien zur großangelegten Beseitigung mobiler Risiken.** Die Lösung bietet Richtlinien-Kontrollmaßnahmen zum umfassenden Schutz von personenbezogenen Daten in und aus der EU, durch die Unternehmen das Risiko messbar senken können. Sie können Richtlinien erstellen, welche Bedrohungen schnell beseitigen und das Datenverlustrisiko von Apps umfassend minimieren, während Sie gleichzeitig die Privatsphäre der Endanwender nachhaltig schützen.
- **Einrichtung von risikoabhängigen bedingten Zugangsberechtigungen.** Die Integration von Lookout Mobile Endpoint Security in das Mobilgerätemanagement (MDM) erlaubt Unternehmen die Erstellung risikoabhängiger bedingter Zugangsberechtigungen zur Absicherung der unternehmenseigenen Daten. Wenn die Lookout-Lösung beispielsweise feststellt, dass ein Anwender eine mit Malware infizierte „sideloaded" App verwendet, wird das MDM-System sofort über die mangelnde Compliance des Geräts benachrichtigt. Das MDM kann dann angemessen reagieren, z. B. indem es den Zugang des Geräts für alle Unternehmensanwendungen widerruft, bis das Risiko beseitigt ist.
- **Vorbereitung auf die DSGVO-Anforderung, Datenpannen innerhalb von 72 Stunden zu melden.** Lookout Mobile Endpoint Security informiert Administratoren zeitnah, wenn es möglicherweise zu böswillig verursachten oder versehentlichen Datenabflüssen von einem Mobilgerät gekommen ist. Administratoren erhalten in der Lookout-Konsole Detailinformationen über das erkannte Problem und können so „unverzüglich" die Aufsichtsbehörden in Kenntnis setzen.
- **Absicherung des Transfers von Daten aus der EU in andere Länder.** Die Lösung bietet Transparenz über Apps, die bei der Datenspeicherung und -übertragung unsichere Methoden anwenden und zeigt außerdem die Ziele der versendeten Daten an. Anhand dieser Informationen können Unternehmen personenbezogene Daten aus der EU besser schützen. Handelt es sich um eine Inhouse-entwickelte App, kann der Administrator diese in die Konsole hochladen, damit sie auf derartige Schwachstellen und andere riskante Verhaltensweisen geprüft wird.
- **Sicherstellen, dass die Mobile-Security-Lösung den „Datenschutz von Anfang an"-Prinzipien genügt.** Das Konzept „Datenschutz von Anfang an" war für Lookout bei der Lösungsentwicklung maßgeblich. Das Unternehmen schützt bereits Millionen Geräte weltweit mit einer Lösung, die auf den Schutz der Privatsphäre seiner Endanwender ausgelegt ist. Dazu verfügt sie über robuste Datenschutzkontrollen, einschließlich der Möglichkeit, die Erfassung von personenbezogenen Daten zu Anwendern oder verwalteten Geräten einzuschränken.

Das riesige globale Sensorennetzwerk sowie die leistungsstarken Bedrohungsanalysen machen die Lösung von Lookout einzigartig - und zudem außerordentlich effektiv, wenn es etwa um DSGVO-Compliance geht. Der Erfolg seiner von Privatanwendern und in Unternehmen eingesetzten Produkte für Endgeräte bietet Lookout Erkenntnisse auf Basis von über 150 Millionen Mobilgeräten in der ganzen Welt.

Jeden Monat senden Millionen von Geräten in über 150 Ländern Sicherheits-Telemetriedaten an die Lookout Security Cloud. Damit hat Lookout neue Akteure, die eine Bedrohung darstellen, immer im Blick – und bleibt branchenführend bei der Erkennung neuartiger Bedrohungen, wie der mobilen Pegasus-Spyware. Eine in dieser Form einzigartige Datenbank mit Informationen zum Thema Mobilität bietet Kunden den Vorteil von Präzision und Kontextrelation: Unternehmen können erkennen, ob ein Signal oder eine entsprechende Eigenschaft, die potenziell eine mobile Bedrohung darstellen könnten, im weltweiten Rahmen normal, selten oder tatsächlich anormal ist. Die Informationen liefern mehr als 50 Millionen einzelne Apps und ein globales Sensornetzwerk, das das Vorkommen dieser Signale in Echtzeit verfolgt.

Damit Unternehmen sich auf die Anforderungen der DSGVO einstellen können, müssen sie diese zunähst verstehen und wissen, welche Auswirkungen sie auf ihre Mobilgeräteflotten haben. Im zweiten Schritt gilt es dann, effektive Lösungen zum Schutz mobiler Daten einzusetzen.

Leider gibt es hinsichtlich Datensicherheit und -schutz kein Weiß oder Schwarz; die Einschätzung, ob Compliance gegeben ist, fällt immer schwer. Und so ist dem einen Unternehmen zu lax, was im anderen als angemessen gilt und dem nächsten schon völlig übertrieben vorkommt. Was als adäquat empfunden wird, hängt eben von der jeweiligen Risikotoleranz ab. Eine mobile Lösung allein wird kein Unternehmen „compliant" machen, aber sie sollte sich um die mobilen Bedrohungen und Schwachstellen kümmern, denen das Unternehmen eventuell ausgesetzt ist.

Mit der DSGVO zieht ein neuer Standard für den Umgang mit und den Schutz von personenbezogenen Daten in die Wirtschaft ein. Das Konzept ist nicht neu – die meisten Unternehmen haben sich damit schon auf die ein oder andere Art befasst. Doch nun gilt es, vorhandene Datenschutzprogramme auf die mobile Infrastruktur auszuweiten.

Nächste Schritte: Transparenz über mobile Bedrohungen zur Ausweitung der DSGVO-Compliance auf Mobilgeräte

Mit der DSGVO zieht ein neuer Standard für den Umgang mit und den Schutz von personenbezogenen Daten in die Wirtschaft ein. Das Konzept ist nicht neu – die meisten Unternehmen haben sich damit schon auf die ein oder andere Art befasst. Doch nun steht die Wirtschaft unter starkem Druck, immer mehr behördliche sowie branchenspezifische Vorschriften zum Datenschutz umzusetzen, darunter auch die DSGVO. Nun gilt es also, vorhandene Datenschutzprogramme auf die mobile Infrastruktur auszuweiten.

Durch die Missachtung der Vorschriften drohen unter anderem erhebliche Bußgelder. So schreibt die DSGVO Strafen für die Nichteinhaltung von bis zu 4 % des globalen Jahresumsatzes des betroffenen Unternehmens vor – je nach Art des Verstoßes.

Datensicherheit und -schutz müssen auf mobile Umgebungen ausgeweitet werden, weil hier ein Großteil der alltäglichen geschäftlichen Vorgänge und Prozesse durchgeführt wird. Zudem lauern dort vielfältige Sicherheitsbedrohungen, Schwachstellen und riskantes Verhalten, die die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gefährden.

Die Einhaltung behördlicher Vorschriften bietet Unternehmen und Organisationen aber auch eine hervorragende Gelegenheit, ihre Sicherheitsmaßnahmen zu optimieren - inklusive der Absicherung ihrer wachsenden Mobilgeräteflotte.

Auf www.lookout.com/gdpr erfahren Sie mehr darüber, wie auch Sie die DSGVO-Compliance auf das mobile Arbeiten ausweiten können.

Über Lookout

Lookout sorgt für Cybersicherheit in einer mobilen Welt. Dank der weltweit größten Datenbank für mobilen Code setzt Lookout Maßstäbe für die Integrität von Mobilgeräten und den Datenzugriff. Lookout wird von über 100 Millionen Anwendern, Hunderten Unternehmen und Behörden sowie Technologieanbietern wie AT&T, Deutsche Telekom und Microsoft genutzt. Lookout hat seinen Hauptsitz in San Francisco und verfügt über Niederlassungen in Amsterdam, Boston, London, Sydney, Tokio, Toronto und Washington, DC.