Lookout®

BERICHT

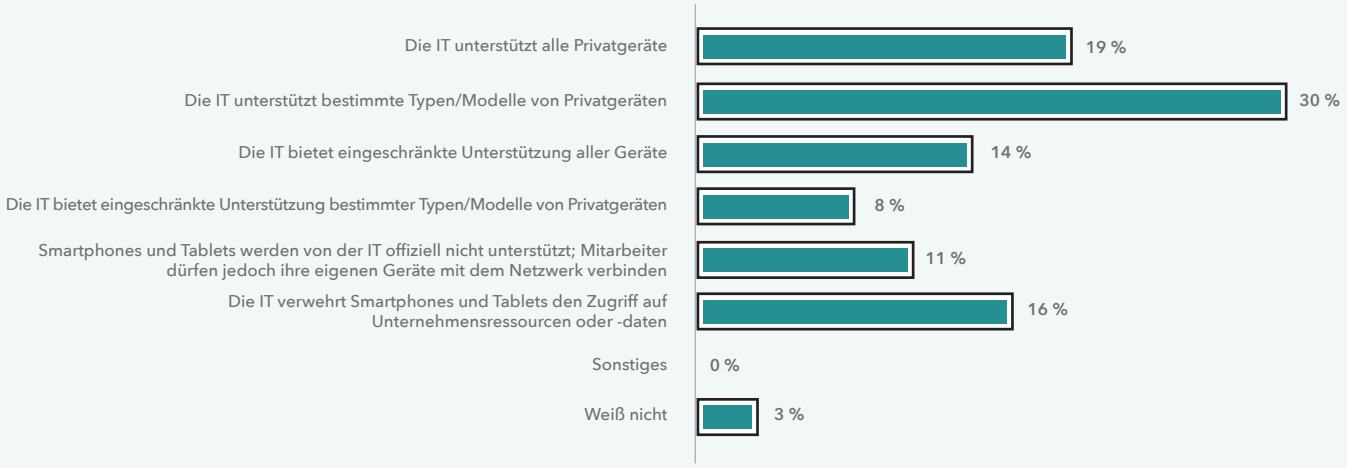
An alle europäischen Unternehmen:

Sie haben ein BYOD-Programm – ob es Ihnen gefällt oder nicht

„Wir haben kein BYOD-Programm."

Dies ist praktisch die Standardaussage vieler europäischer Organisationen zur Nutzung privater Mobilgeräte am Arbeitsplatz, wenn es um die Absicherung streng vertraulicher und personenbezogener Daten sowie die Verwaltung der Mitarbeiterberechtigungen und des Zugriffs auf diese Daten geht. Dahinter steckt oft die Annahme, dass sie von Cyberbedrohungen, die auf Mobilgeräte abzielen, verschont bleiben werden, weil sie den Mobilgeräten ihrer Mitarbeiter schließlich keinen Zugang zum Netzwerk erlauben. Mit dieser Einstellung setzen sie ihre Daten allerdings einem Risiko aus, denn in jedem Unternehmen gibt es BYOD – ob es Ihnen gefällt oder nicht.

Offizielle IT-Richtlinie zur Unterstützung mitarbeitereigener Smartphones und Tablets

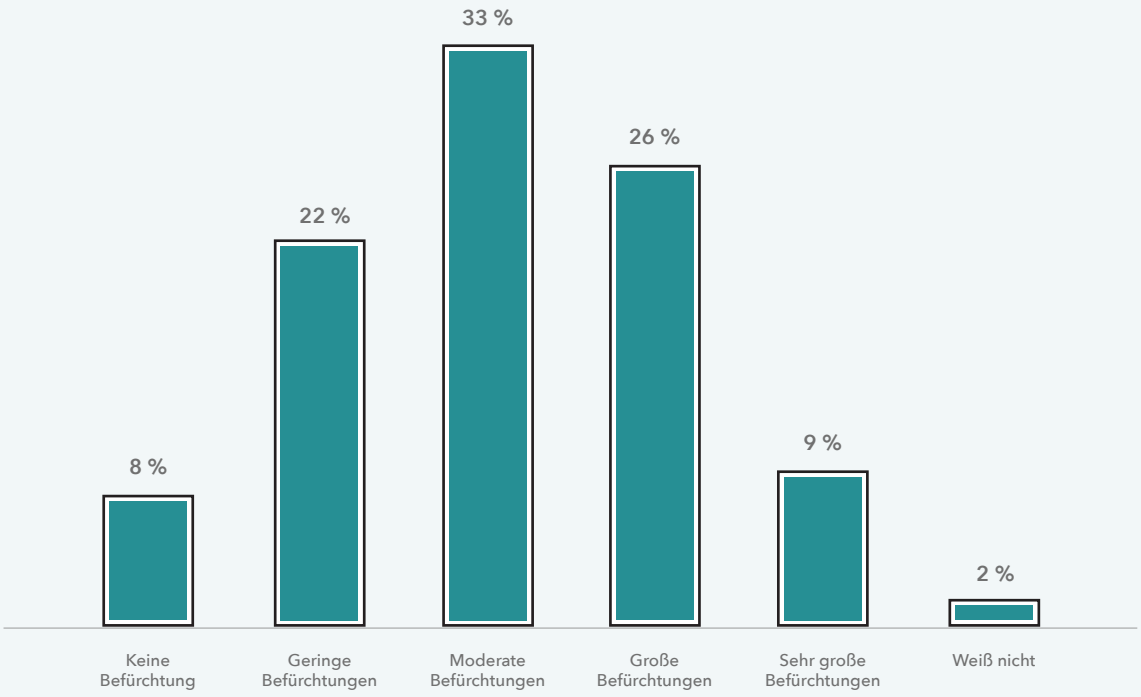


Datenbasis: N=37 (Nord- und Südamerika; Behörden, Bildungswesen oder Gesundheitswesen) Entscheidungsträger für Client-Sicherheit
Quelle: Forrester, „Global Business Technographics Security Survey, 2016"

Durch eine Befragung zum Thema unter US-Bundesbehörden, also Institutionen mit extrem hohem Anspruch an die Datensicherheit, erhielt Lookout eine belastbare Fallstudie für europäische Unternehmen und Organisationen. Wir kamen zu dem Schluss, dass Mitarbeiter auch ohne das Wissen der Organisation ihre privaten Mobilgeräte in kontrollierte Umgebungen einbringen.

Unsere Ergebnisse dürften alle weltweit tätigen Organisationen interessieren, die ihre Unternehmens-, Mitarbeiter- und Kundendaten absichern und sich vor Industriespionage oder kriminellen Machenschaften schützen müssen.

Befürchtungen hinsichtlich des Datenrisikos/möglicher Auswirkungen auf die Organisation:
Nutzung von privater Technik und Cloud-Technologie durch Mitarbeiter



Datenbasis: N=171 (Nord- und Südamerika; Behörden, Bildungswesen oder Gesundheitswesen) Entscheidungsträger für Sicherheit
Quelle: Forrester, „Global Business Technographics Security Survey, 2016"

Unkontrolliertes BYOD ist ein echtes Problem

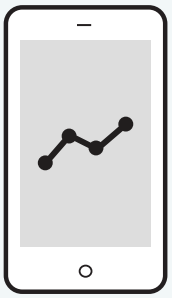
Lookout befragte mehr als 1.000 Mitarbeiter in insgesamt 20 US-Behörden und stellte fest, dass sich in den Behördennetzwerken 14.622 mit Lookout ausgestattete Geräte befinden. Daraus folgt, dass die Mitarbeiter ihre Privatgeräte mit Behördensystemen verknüpfen. Hinzu kommt die enorme Menge von Bedrohungen pro Jahr, die auf solche Mobilgeräte abzielen: 11 Prozent.

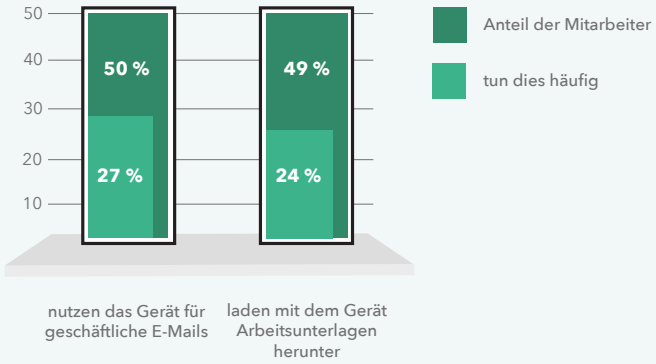
Das Problem sind nichtverwaltete oder gar unbekannte Mobilgeräte in einem Netzwerk („unkontrolliertes BYOD"). Ebenso wie andere unkontrollierte IT-Komponenten (z. B. privat beschaffte Anwendungen) birgt unkontrolliertes BYOD die Gefahr, dass sensible Daten abfließen, weil nicht bekannt, geschweige denn festgelegt ist, welche Geräte worauf zugreifen können.

US-Behördenmitarbeiter nehmen es manchmal mit den Regeln nicht zu genau und nehmen Arbeit mit nach Hause. Ganze 50 Prozent von ihnen greifen über Privatgeräte auf geschäftliche E-Mails zu und 49 Prozent laden Arbeitsunterlagen damit herunter. Dies ist nur ein Beispiel für den ausgedehnten Datenaustausch zwischen privaten und geschäftlichen Konten. Jede Organisation – ob Behörde oder nicht – muss Einblick in ihre Datenströme haben und sie steuern können.

Private Gerätenutzung

Wissen Sie, wie viele Ihrer Mitarbeiter ein privates Mobilgerät für die Arbeit nutzen?





Lookout-Umfrage unter 1.002 US-Bundesbediensteten, Juni 2015

Sicherheitsbeschränkungen lassen sich bei Mobilgeräten schnell umgehen

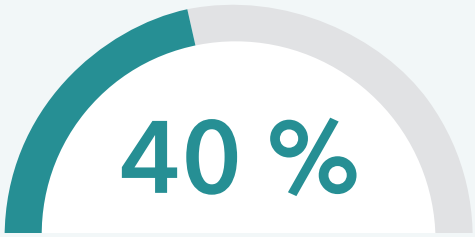
Ein großer Anteil der Behördenmitarbeiter greift also über Privatgeräte auf arbeitsrelevante Unterlagen und E-Mails zu. Aber eine ebenfalls nicht zu vernachlässigende Anzahl versucht auch, Geräte per Jailbreak oder Rooting zu verändern, sei es, um Apps aus anderen als den offiziellen App-Stores herunterzuladen oder um einfach nur die Schriftart auf dem Startbildschirm zu ändern.

Rund sieben Prozent der befragten US-Behördenmitarbeiter gaben an, gerootete oder per Jailbreak „entsperrte“ Geräte für die Arbeit zu nutzen oder dorthin mitzubringen. Eine solche Zahl lässt den Schluss zu, dass nicht nur Tüftler oder Technikbegeisterte ihre Geräte manipulieren.

Leider setzen Jailbreaking und Rooting das Betriebssystem des jeweiligen Mobilgeräts Schwachstellen aus, die nicht gepatcht werden, und erlauben es den Nutzern, Apps von Drittplattformen herunterzuladen, auf denen auch infizierte Software angeboten wird. Diese Probleme können später Tür und Tor für Datenlecks und -manipulationen öffnen.

Gegen die Regeln

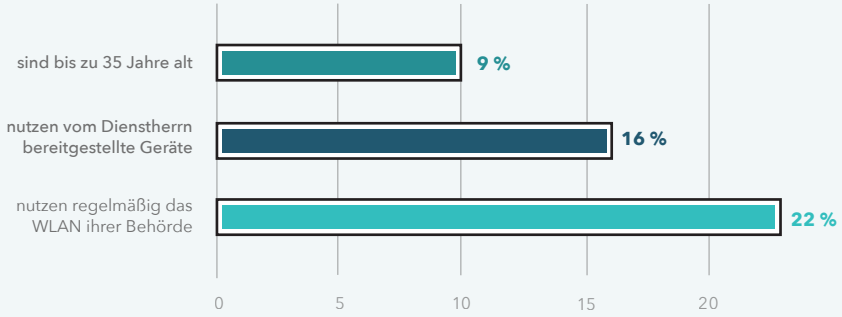
Restriktive, isolierende Richtlinien für das mobile Arbeiten wirken nicht



der Mitarbeiter von Behörden, in denen der Gebrauch privater Smartphones für die Arbeit verboten ist, geben an, sie würden sich von den Regeln kaum bis gar nicht aufhalten lassen

SIE MANIPULIEREN SOGAR IHRE GERÄTE

7 % der Mitarbeiter bringen Geräte mit, deren Funktionsumfang und Zugriffsrechte mittels Rooting oder Jailbreak erweitert wurden, und nutzen sie für die Arbeit. Diese Mitarbeiter ...



65 % haben Zugriff auf geschäftliche E-Mails auf dem Gerät

57 % haben Zugriff auf Arbeitsunterlagen auf dem Gerät

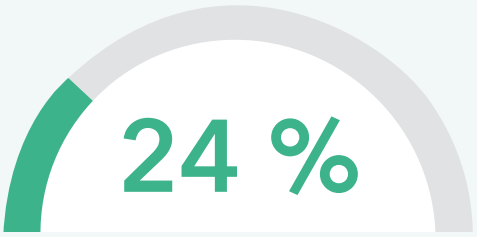
Lookout-Umfrage unter 1.002 US-Bundesbediensteten, Juni 2015

Möglicherweise ungeprüfte und unsichere Apps gelangen ins Netzwerk

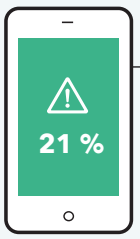
Überraschend viele Mitarbeiter von US-Behörden (24 %) installieren Apps aus anderen als den offiziellen Quellen wie dem Play Store von Google oder dem App Store von Apple. Damit setzen sie ihre Mobilgeräte Gefahren aus, denn solche Apps wurden wahrscheinlich nicht so streng geprüft, wie das bei Google und Apple der Fall ist. Das Umfrageergebnis beseitigt dann auch den Irrtum, dass sich Apps nur per App Store auf ein iPhone herunterladen lassen. Tatsächlich geht das auch einfach über eine Website oder einen Link.

Herunterladen von Apps

Mitarbeiter beziehen ihre Apps nicht nur aus offiziellen App-Stores

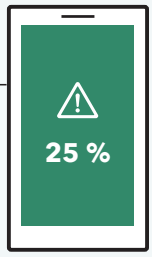


der Mitarbeiter beziehen Apps auch aus inoffiziellen App-Stores



21 % der iPhone-Nutzer beziehen Apps auch aus inoffiziellen App-Stores

25 % der Android-Nutzer beziehen Apps auch aus inoffiziellen App-Stores



Lookout-Umfrage unter 1.002 US-Bundesbediensteten, Juni 2015

Eine echte Gefahr

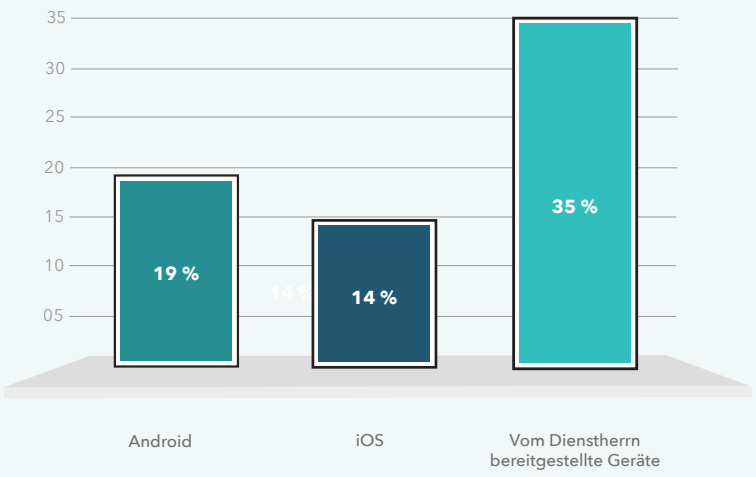
Ein großer Anteil der Befragten (18 %) hatte schon einmal Malware auf ihren Mobilgeräten, sowohl privaten als auch vom Dienstherrn bereitgestellten. Von ihnen waren 19 Prozent Android-Nutzer und 14 Prozent iPhone-Nutzer. Dies ist unerwarteterweise mehr als die durchschnittlich sieben Prozent Malware-Entdeckungen auf Android-Geräten, die Lookout im Jahr 2014 feststellte. Zu bedenken ist allerdings, dass die eigenverantwortliche Natur solcher Umfragen die Möglichkeit offenlässt, dass die Befragten bestimmte Erlebnisse mit potenziell schädlicher Software verwechseln. Trotz dieser Erkennungsrate haben 49 Prozent der Mitarbeiter in US-Behörden immer noch keine Sicherheits-App oder -Lösung auf den Mobilgeräten, die sie für die für die Arbeit nutzen oder dorthin mitbringen.

Malware auf Mobilgeräten

Überraschend viele Behördenmitarbeiter hatten schon einmal Malware auf Mobilgeräten

18 % **der Behördenmitarbeiter mit Smartphones (privat oder vom Dienstherrn bereitgestellt) berichten von Schadsoftware (oder Malware)**

WELCHE GERÄTETYPEN WURDEN VERWENDET?



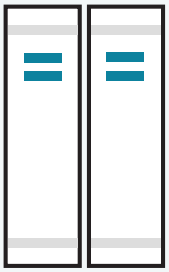
Lookout-Umfrage unter 1.002 US-Bundesbediensteten, Juni 2015

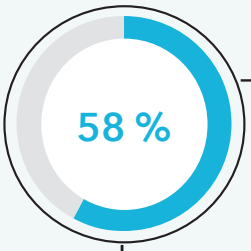
Mitarbeiter zu schulen, reicht nicht

Es zeigte sich, dass Mitarbeiter bekannte Cyberrisiken für die behördliche Sicherheit in Kauf nehmen, um am Arbeitsplatz private Mobilgeräte zu nutzen. 58 Prozent der Befragten wissen angeblich um die Konsequenzen, die dem Netzwerk durch Privathandys für die Arbeit entstehen können. Dennoch sind 85 Prozent von ihnen bereit, ihr Handy für potenziell riskante Aktivitäten zu nutzen. Sie sind einfach zu bequem und gehen den Weg des geringsten Widerstands, um ihre Ziele zu erreichen – riskant hin oder her. Mitarbeiter auf die Risiken aufmerksam zu machen, zum Beispiel durch Schulungen, ist wichtig. Ihre Arbeitgeber müssen jedoch auch über die richtige Technologie verfügen, die einspringt, wenn Vorgaben nicht eingehalten werden.

MITARBEITER ZU SCHULEN, reicht nicht

37 % der Mitarbeiter nehmen bekannte Cyberrisiken für die behördliche Sicherheit in Kauf, um am Arbeitsplatz private Mobilgeräte nutzen zu können



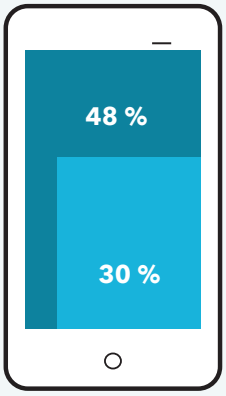


kennen die Konsequenzen für die Cybersicherheit, die sich aus dem Gebrauch von Privathandys für die Arbeit ergeben können,

dennoch geben 85 % zu, ihre Privatgeräte für potenziell risikoreiche Aktivitäten zu nutzen

48 % geben an, keine arbeitsrelevanten Informationen oder Dateien auf Privatgeräten speichern zu dürfen,

dennoch tun es 30 % trotzdem



Lookout-Umfrage unter 1.002 US-Bundesbediensteten, Juni 2015

Fazit

Immer mehr Mitarbeiter möchten ihre Mobilgeräte in allen Bereichen des Lebens nutzen. Das stellt viele Organisationen vor die schwierige Herausforderung, eine funktionierende Mischung aus Offenheit für BYOD und Absicherung sensibler Daten zu finden.

Zahlreichen Unternehmen und Behörden weltweit fehlt ein offizielles internes Programm für sicheres mobiles Arbeiten und generell eine Strategie für den Umgang mit Privatgeräten am Arbeitsplatz. Dieser Mangel, das zeigt die Studie eindeutig, setzt sensible Daten Risiken aus, denn er bedeutet, dass sich Mitarbeiter über Regeln (sofern vorhanden) hinwegsetzen, um ihre Geräte trotzdem zu nutzen.

Fortschrittliche Organisationen begrüßen Privatgeräte am Arbeitsplatz mittlerweile sogar, weil sie sie mit modernen Gerätemanagement- und Schutzlösungen unter Kontrolle haben. Außerdem betrachten sie das Thema Sicherheit nicht punktuell, sondern allumfassend, und wissen daher, dass Mobilgeräte und mobiles Arbeiten wegen der enormen Datenbewegungen eine zentrale Rolle spielen.

Jedes Unternehmen und jede Organisation sollte unkontrolliertes BYOD als großes Sicherheitsproblem betrachten. Mobilität beim Absichern von Daten auszuklammern, bedeutet schließlich, Daten ungeschützt zu lassen. Europäische Unternehmen müssen daher auch Fremdgeräte im Netzwerk ins Visier nehmen, denn auch sie greifen auf sensible Daten zu, ob das so gewollt ist oder nicht.

Methodik: *Market Cube führte die Umfrage im Auftrag von Lookout im Zeitraum vom 19. bis 26. Juni 2015 durch. Ausgewertet wurden die Antworten von 1.002 US-Bundesbediensteten. Die Fehlertoleranz beträgt 3,1 %.*