International Working Group
on Data Protection
in Telecommunications

675.49.11

**Arbeitspapier zu Datenschutz- und Datensicherheitsrisiken
bei der Nutzung von privaten Endgeräten in Unternehmensnetzwerken**

56. Sitzung, 14.–15. Oktober 2014, Berlin

– Übersetzung –

Anwendungsbereich

Dieses Arbeitspapier untersucht die mit der Nutzung privater, mobiler Endgeräte („Own Devices“) wie Tablet-Computer und Smartphones verbundenen Datenschutz- und Sicherheitsrisiken für den Zugriff auf Anwendungen und Daten einschließlich personenbezogener Daten, die in Unternehmensnetzwerken liegen.

Viele dieser Risiken sind bereits von der Arbeitsgruppe in den Arbeitspapieren zu „Mobile Verarbeitung personenbezogener Daten und Datensicherheit[1]“ und „Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes[2]“ behandelt worden, aber es gibt weitere, spezifische Fragestellungen bei der Nutzung von privaten Endgeräten in Unternehmensnetzwerken.

Hintergrund

„Bring Your Own Device“ (BYOD) -Praktiken sind im Geschäftsleben weit verbreitet, und es gibt einen zunehmenden Druck zu ihrer Einführung. Allerdings wächst auch die Besorgnis über die Auswirkungen auf Datenschutz und Datensicherheit bei der Einführung dieser Praktiken[3].

Organisationen empfinden BYOD als gesteigerten Komfort für ihre Beschäftigten, die ihnen bekannte Endgeräte bei der Arbeit nutzen können, und wenn sie unterwegs oder zuhause sind, und für leitende Angestellte, die häufig die erweiterten Funktionen und den Bedienungskomfort fordern, die ihre eigenen Endgeräte bieten.

Diesen möglichen Vorteilen stehen Risiken für die Vertraulichkeit und Integrität von Informationsverarbeitungssystemen von Unternehmen entgegen und das gesteigerte Risiko, dass personenbezogene Daten in diesen Systemen nicht länger adäquat geschützt sein könnten.

Jede Organisation, die BYOD erlaubt, muss adäquate Sicherheitsmaßnahmen anwenden, um den Schutz aller verarbeiteten Unternehmensdaten sicherzustellen. Organisationen müssen auch sicherstellen, dass die Auswirkungen dieser Sicherheitsmaßnahmen auf die Privatsphäre der einzelnen Nutzer minimiert werden[4].

---

[1] http://www.datenschutz-berlin.de/attachments/724/WP_Mobile_Verarbeitung_und_Datensicherheit_final_clean_675_41_19.pdf

[2] http://www.datenschutz-berlin.de/attachments/882/675.44.10.pdf

[3] http://enterprise-mobile-solutions.tmcnet.com/articles/359879-growth-byod-compels-companies-revisit-security-basics.htm

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

Nutzer könnten jedoch darüber besorgt sein, dass die Organisation exzessive Überwachungsmaßnahmen durchführt, um diesen Risiken zu begegnen; z. B. könnte der Administrator des Unternehmensnetzwerkes vollen Zugriff auf das private Endgerät (d. h. einschließlich des Zugriffs auf alle privaten Daten) haben, um Unternehmensdaten zu erkennen und zu schützen. Im Fall des Verlustes des Endgeräts oder wenn es gestohlen wird, könnte eine „Fernlöschung" dazu führen, dass auf dem Endgerät gespeicherte, private Informationen dauerhaft gelöscht werden. Dementsprechend können private Endgeräte zusätzliche Risiken für die personenbezogenen Daten ihrer Nutzer mit sich bringen. Die korrekte Nutzung einer Anwendung zur Verwaltung mobiler Endgeräte kann die personenbezogenen Daten von Nutzern privater Endgeräte sichern und gleichzeitig die Vertraulichkeit und Integrität von Unternehmensdaten schützen.

Die Richtlinien des Weißen Hauses für Bundesbehörden[5] sprechen sich für BYOD aus, aber warnen davor, dass „*die Einführung eines BYOD-Programms Behörden vor unzählige Herausforderungen für die Sicherheit, vor konzeptuelle, technische und rechtliche Herausforderungen nicht nur für die interne Kommunikation, sondern auch in Bezug auf Beziehungen und das Vertrauen zwischen privatwirtschaftlichen und administrativen Partnern stellt.*"

Empfehlungen für öffentliche Stellen der britischen Regierung klingen vorsichtiger; sie empfehlen: „*Es ist notwendig, dass das Endgerät für den gesamten Zeitraum, in dem es auf dienstliche Informationen zugreifen kann, unter die Verwaltungshoheit des Unternehmens gestellt wird. Somit ist ein BYOD-Modell möglich, jedoch aus verschiedenen technischen und nicht-technischen Gründen nicht empfohlen.*

Die französische nationale Sicherheitsbehörde (ANSSI) rät gegenwärtig von der Anwendung von BYOD ab[6].

Vom britischen Information Commissioner veröffentlichte Empfehlungen für verantwortliche Stellen[7] betonen: „*Die Erlaubnis, Endgeräte, mit IT-Systemen von Unternehmen zu verbinden, über die sie keine Kontrolle haben, kann zu einer Reihe von Risiken für die Verletzung der Sicherheit und anderen Datenschutzbedenken führen, wenn dies nicht richtig gehandhabt wird.*"

Das „Überblickspapier Consumerisation und BYOD"[8] des Deutschen Bundesamt für Sicherheit in der Informationstechnik betont, dass „*die zunehmende berufliche Nutzung von Endgeräten aus dem privaten Umfeld durch Consumerisation und BYOD [..] zu großen Herausforderungen für die Informationssicherheit, aber auch für den Datenschutz [führt]. Dies muss als strategische Herausforderung angesehen und von der Leitungsebene einer jeden Institution sinnvoll gestaltet werden. [...] Technische Maßnahmen alleine [reichen] nicht aus, sondern diese müssen durch organisatorische Maßnahmen flankiert werden, die im Einklang mit der Gesamtstrategie der Institution stehen.*"

Das Büro der Beauftragten für Datenschutz und Informationsfreiheit von Ontario (Kanada) hat gemeinsam mit TELUS[9] ein Papier veröffentlicht, das Risiken für das Informationsmanagement untersucht und Hinweise zu Maßnahmen gibt, um diesen zu begegnen.

Die Nutzung privater Endgeräte ist nicht auf BYOD begrenzt, sondern schließt auch Endgeräte ein, deren Eigentümer Dritte sind oder die von Dritten kontrolliert werden, z. B. Mit-Auftragnehmer, Unterauftragnehmer, Kunden und Klienten. Darüber hinaus beseitigt die Beschränkung der Verarbeitung personenbezogener Daten auf unternehmenseigene und von diesem verwaltete Geräte nicht alle Risiken, die in einer zunehmend mobilen Arbeitnehmerschaft vorkommen, da die Nutzung nicht-genehmigter Software oder von Online-Diensten,

---

[4] Z. B. durch die Anwendung von „Sandbox"-Techniken, bei denen ein Endgerät zwei verschiedene „Sandboxen" enthält, eine persönliche und eine geschäftliche.

[5] http://www.whitehouse.gov/digitalgov/bring-your-own-device#key-considerations

[6] http://www.ssi.gouv.fr/IMG/pdf/Communique_de_presse_Assises_de_Monaco_2012_v2.pdf

[7] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

[8] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html

[9] http://www.ipc.on.ca/site_documents/pbd-byod.pdf

manchmal als „Bring Your Own App“, „Bring Your Own Software“ oder sogar „Bring Your Own Anything (BYOx“)[10] bezeichnet, gleichartige Bedenken hinsichtlich Datenschutz und Datensicherheit aufwirft.

Datenschutz- und Datensicherheitsrisiken

Viele der Risiken, die mit der Nutzung von privaten Endgeräten verbunden sind, sind ebenso relevant für die persönliche Nutzung unternehmenseigener Endgeräte, einschließlich:

a) Private Endgeräte sind in vielen Fällen klein und mobil; daher sind jegliche Daten, die auf ein privates Endgerät übertragen werden, anfällig für Verlust, Diebstahl und unkontrollierten Zugriff;

b) private Endgeräte können Unternehmensdaten zugänglich machen und technische Datenschutzkontrollen umgehen; und

c) private Endgeräte können für unbemerkte externe Attacken und Überwachung anfällig sein (z. B. durch Missbrauch von WiFi oder Bluetooth-Technologie und durch den Zugriff auf unsichere Internetseiten). Dies kann „social engineering“-Attacken einschließen, die von der Nutzung sozialer Medien oder anderen Online-Dienste für berufliche Zwecke herrühren.

Risiken, die in besonderer Weise mit der Nutzung privater Endgeräte verknüpft sind, umfassen:

d) Es ist schwierig, die Betriebssysteme privater Endgeräte zur Reduktion von Funktionalität und Erhöhung der Sicherheit anzupassen, wie dies bei unternehmenseigenen Endgeräten üblich ist, die im Besitz der Organisation sind und von dieser verwaltet werden;

e) private Endgeräte können oft einen größeren Umfang potenziell weniger sicherer Kommunikationsnetzwerke aus verschiedenen Umgebungen einschließlich des Arbeitsplatzes, des Zuhauses und nationaler oder internationaler öffentlicher Orte verwenden, auf die unternehmenseigene Geräte nicht zugreifen können, die im allgemeinen ein von dem Unternehmen verwaltetes Kommunikationsnetzwerk nutzen, z. B. ein Kabel-gestütztes LAN, das sich in einer sicheren Büroumgebung befindet;

f) vorhandene Unternehmensanwendungen und die Netzwerkinfrastruktur könnten nicht mit adäquaten Sicherheitseinrichtungen versehen sein, um dem Zugriff privater Endgeräte zu ermöglichen;

g) Unternehmensrichtlinien zur akzeptierten Nutzung des Internet oder von Webmail oder sozialen Netzwerken am Arbeitsplatz könnten schwieriger durchzusetzen sein, wenn Beschäftigte private Endgeräte nutzen;

h) das Betriebssystem privater Endgeräte könnte nicht so ausgereift sein wie die traditionelle Unternehmensendgeräte und anfällig für eine Reihe von Angriffen oder Sicherheitslücken sein, die nicht innerhalb eines angemessenen Zeitraums beseitigt werden; darüber hinaus ist die Aktualisierung eines privaten Endgeräts typischerweise in der Verantwortung des Nutzers,

i) ein wesentlicher Teil der Nutzung privater Endgeräte wird persönlicher Natur sein und die Nutzung des Endgeräts könnte auf andere Mitglieder der Familie oder des Haushaltsbesitzers ausgedehnt werden;

j) Dienste, die eine automatische Datensicherung verwenden oder Software Dritter, die durch den Nutzer installiert wird, könnten in der unerwarteten oder nicht-autorisierten Nutzung von Cloud-Diensten resultieren;

k) der Nutzer eines privaten Endgeräts könnte weniger aufmerksam sein oder größere Sicherheitsrisiken mit einem privaten Endgerät eingehen;

l) personenbezogene Daten könnten nicht wirksam von dem Endgerät vor dessen Entsorgung, Wiederverkauf oder Recycling entfernt werden; und

[10] https://byox.eq.edu.au/SiteCollectionDocuments/byox-project-research-report.pdf

m) die unangemessene Nutzung von Management-Werkzeugen und –techniken zur Verwaltung mobiler Endgeräte könnte zu überzogener Überwachung der Beschäftigten führen.

Empfehlungen

Im Lichte der Risiken für den Schutz personenbezogener Daten und die IT-Sicherheit sollte jede Organisation, die die Erlaubnis der Nutzung privater Endgeräte in Erwägung zieht, vor der Entscheidung über die Anwendung eines solchen Systems eine Vorabkontrolle (Privacy Impact Assessment – PIA) durchführen. Es ist wichtig, dass die Vorabkontrolle die Risiken sowohl für geschäftliche personenbezogene Daten als auch für die personenbezogenen Daten der Nutzer privater Endgeräte einbezieht. Die Vorabkontrolle sollte auch untersuchen, ob eine Verarbeitung dieser personenbezogenen Daten mit privaten Endgeräten angemessen ist, sowie die Auswirkungen von Sicherheitsvorfällen im Hinblick auf die Sensitivität der Daten, die Auswirkungen auf die Betroffenen und die möglichen Reputationsschäden, die aus dem Verlust oder der Verbreitung resultieren. Die Einführung sollte in vorsichtigen, wohlüberlegten Schritten erfolgen und mit nicht-sensitiven und nicht-vertraulichen Informationen beginnen. Die Verarbeitung sensitiver Daten bedingt zusätzliche Bedenken und verlangt zusätzliche Sicherheitsmaßnahmen[11].

Jede Organisation, die entscheidet, die Nutzung privater Endgeräte zu erlauben, muss angemessene Sicherheitsmaßnahmen etablieren, einschließlich, aber nicht beschränkt auf die Folgenden:

a) Eine Untersuchung der vertraulichen und personenbezogenen Daten, die von der Organisation verarbeitet werden und eine Überprüfung, ob es angemessen ist, diese mit privaten Endgeräten zu verarbeiten. Als generelle Regel sollte die Verarbeitung sensitiver Daten mit privaten Endgeräten nur als angemessen betrachtet werden, wenn die mit der Verarbeitung verbundenen Risiken auf ein akzeptables Minimum reduziert werden können;

b) Eine Untersuchung des Schadens potenzieller Datenschutz- und Sicherheitsvorfälle in Hinsicht auf deren Auswirkungen auf die Betroffenen, die Sensivität der Daten und die durch Verlust oder Offenlegung verursachte Rufschädigung;

c) Festlegung, auf welche Unternehmensanwendungen von privaten Endgeräten zugegriffen werden muss;

d) Festlegung, welche Kategorien von Daten mit privaten Endgeräten zugänglich sein müssen;

e) Schriftliche Festlegung von Richtlinien über die Verpflichtungen von Beschäftigten im Zusammenhang mit der Nutzung privater Endgeräte, die mindestens Folgendes beinhalten:

1) Regeln über die Löschung personenbezogener Unternehmensdaten von privaten Endgeräten;

2) Die Verpflichtung Beschäftigter, das Unternehmen zu informieren, wenn ein privates Endgerät oder personenbezogene Unternehmensdaten, die auf einem privaten Endgerät gespeichert sind, gestohlen oder kompromittiert wurden;

3) Personenbezogene Unternehmensdaten, die auf privaten Endgeräten gespeichert oder mit privaten Endgeräten zugänglich sind, gegen unbefugten Zugriff zu sichern, einschließlich der Fälle, in denen andere Teile des privaten Endgeräts von einer berechtigten dritten Partei wie einem Familienmitglied genutzt werden können.

f) Sicherstellung fortlaufender Unterstützung der Nutzer von privaten Endgeräten in Bezug auf die Meldung von Vorfällen und allgemeine Einbeziehung in Verfahrensabläufe; und

g) die Festlegung der notwendigen Erweiterungen für die Sicherheitspolitik und die technische Infrastruktur der Organisation, um den Zugriff mit privaten Endgeräten zu ermöglichen, wie:

1) Die Absicherung von Prozessen zur Nutzerauthentifikation und Nutzung sicherer Kommunikationsmethoden zur Ermöglichung des Zugriffs mit privaten Endgeräten;

2) die Erweiterung der Sicherheit des Unternehmenssystems für Anwendungen, auf die von privaten Endgeräten zugegriffen werden soll;

[11] Vgl. das Arbeitspapier „Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes“ – „Sopot Memorandum“ (Sopot (Polen), 23./23. April 2012), Fußnote 2 oben

3) die Erweiterung der Kommunikationsinfrastruktur zur Einbindung von Ende-zu-Ende-Verschlüsselung für die Kommunikation mit privaten Endgeräten;

4) die Erstellung eines Registers genehmigter privater Endgeräte, deren Nutzung erlaubt ist und von deren Nutzern;

5) die Erstreckung existierender Verfahren zur Zugriffskontrolle, wie z. B., wenn ein Nutzer die Organisation verlässt oder keinen Zugriff mehr benötigt;

6) die regelmäßige Sicherung von Unternehmensdaten, die auf privaten Endgeräten gespeichert sind;

7) klare Regeln zur Fernlöschung von Unternehmensinformationen, die auf privaten Endgeräten gespeichert sind, die als verloren oder gestohlen gemeldet sind oder in anderer Weise nicht länger autorisiert sind, auf das Unternehmensnetzwerk zuzugreifen;

8) Verfahren, um den Auswirkungen von Schadsoftware und Botnetzen auf Unternehmensnetzwerke zu begegnen. Wenn diese auf privaten Endgeräten entdeckt werden und Organisationen die Möglichkeit eines unrechtmäßigen Zugriffs auf personenbezogene Daten nicht ausschließen können (z. B. durch effektive Netzwerksegmentierung oder Zugriffsprotokolle), sollte von einem Sicherheitsvorfall ausgegangen und angemessene Schritte zu dessen Behebung ergriffen werden;

9) angemessene Fortbildung für Nutzer privater Endgeräte zum Datenschutz, zur Vertraulichkeit und zu den Praktiken und Maßnahmen, die die Organisation dazu ergriffen hat, einschließlich zusätzlicher Fortbildungen zu Sicherheit und der akzeptablen Nutzung;

10) die Isolierung privater Endgeräte in einem separaten Netzwerk;

11) die Implementierung, den Test und die Validierung technischer Maßnahmen einschließlich von Firewalls und „Sandboxing“ auf privaten Endgeräten, um den Zugriff anderer Anwendungen auf Unternehmensdaten zu verhindern, während gleichzeitig die Privatsphäre der Nutzer respektiert wird;

12) die angemessene, relevante und proportionale Kontrolle von Verarbeitungsaktivitäten, die von privaten Endgeräten unternommen werden – insbesondere Minimierung der Notwendigkeit zum Zugriff auf den persönlichen Datenbereich der Nutzer und zur Überwachung des Standorts privater Endgeräte außerhalb festgelegter Arbeitszeiten. Es ist zwingend, dass Sicherheitsmaßnahmen zum Schutz der Daten der Organisation nicht die Privatsphäre der Nutzer oder eines anderen Betroffenen (eines Dritten) verletzen, dessen Daten in dem privaten Bereich des Endgeräts gespeichert sein können (z. B. in Adressbüchern, im Posteingang privater E-Mails, auf Familienfotos, usw.);

13) Verfahren zur Validierung der Integrität privater Endgeräte und zur Bestätigung, dass diese definierten, akzeptablen Standards entsprechen, wie mindestens: Versionen des Betriebssystems, Endgerätetyp, Passwortschutz, Verschlüsselung (einschließlich Verschlüsselung des Dateisystems) und aktueller Schutz gegen Schadsoftware; und

14) Verfahren zur Entdeckung und Verhinderung der Nutzung von Software, die nach den Regeln der Organisation verboten ist, wie File-sharing-Anwendungen, Anwendungen für Streaming und peer-to-peer-Anwendungen. Dies muss in einer Weise erfolgen, die die Privatsphäre der Beschäftigten respektiert.