International Working Group
on Data Protection
in Telecommunications

675.41.19 7. September 2010

Arbeitspapier

"Mobile Verarbeitung personenbezogener Daten und Datensicherheit"

Hintergrund

Im April 2004 hat die Arbeitsgruppe ein Arbeitspapier über potentielle Risiken für die Privatsphäre in Verbindung mit drahtlosen Computernetzwerken (*engl. wireless networks*) angenommen.[1]

Seither wird durch die stark steigende Verbreitung und Vielfalt von mobilen Geräten, wie zum Beispiel Mobiltelefonen, Smartphones, Laptops und PDA's, einhergehend mit der ständigen Verfügbarkeit von öffentlichen Kommunikationsnetzen eine Verarbeitung jeglicher Art von vertraulichen und persönlichen Daten auf potenziell unsicheren Geräten in potenziell unsicheren öffentlichen Umgebungen immer einfacher.

Der Einsatz mobiler Geräte ist nicht ausschliesslich auf die Pflege von Kontaktdaten und die Bearbeitung von Kalendereinträgen beschränkt. Vielmehr ist ein Zugriff auf vertrauliche und persönliche Informationen in Unternehmens-Datenbeständen oder die Nutzung von Cloud-Computing-Diensten bequem möglich.

Die stetig steigenden Speicherkapazitäten der mobilen Geräte und die immer schneller werdenden drahtlosen Netzwerke erlauben eine mobile Datenverarbeitung in einer Art und Weise, die in der Vergangenheit nur in festen und sichereren Umgebungen möglich war. Die verstärkte Integration mobiler Anwendungen in herkömmliche betriebliche IT-Infrastrukturen und Prozesse hat zur Folge, dass zunehmend vertrauliche, persönliche sowie geschäftskritische Daten nicht nur in zentralen Systemen abgespeichert sind, sondern auf den mobilen Geräten bearbeitet werden. Dies kann sich unmittelbar auf die Integrität, Vertraulichkeit und Sicherheit der Daten auswirken.

Zudem werden mobile Geräte vermehrt zur Archivierung und temporären Speicherung von Daten genutzt, was die Risiken von Datenverlust oder Veröffentlichung mit sich bringt.

Datenschutz und Datensicherheitsrisiken

Naturgemäss besitzen mobile Geräte eine kleine Bauform und ein geringes Gewicht. Die grössten Gefahren für die Datensicherheit liegen in der Manipulation, dem Verlust und dem Diebstahl der Daten. Zur Erkennung einer Datenmanipulation existieren geeignete Mechanismen zur Sicherung der Datenintegrität. Während der Verlust von Daten sofort erkennbar ist, wird ein Datendiebstahl oftmals erst dann bemerkt, wenn die Daten selbst oder das Ergebnis einer Bearbeitung an einem anderen Ort wieder auftauchen.

Es ergeben sich durch den Einsatz mobiler Geräte eine Reihe von spezifischen Risiken:

- Verbindungen zu öffentlichen Netzwerkzugängen (z.B. offene Internetzugänge in Restaurants, Hotels, Internetcafes, usw.), ungeachtet der Anschlussart (z.B. Verbindung mit Netzwerkkabel oder Wireless

[1] http://www.datenschutz-berlin.de/attachments/196/1_de.pdf?1215693415

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

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

LAN), alleinig mit einem nicht vertrauenswürdigen Netzwerk. Zumindest die Verbindungsdaten oder unter Umständen sogar die Inhaltsdaten können abgehört und mitgelesen werden. Das Abhören vertraulicher Informationen in der Kommunikation ist nicht nur für den Betreiber des Netzwerks, sondern, bei nicht ausreichenden Sicherheitsvorkehrungen im entsprechenden Netzwerksegment, von jedem Netzwerkanschluss aus möglich.

- Bei der Verwendung offener unverschlüsselter drahtloser Netzwerkzugänge, sogar bei sonst sicherer Netzwerkverbindung, kann die Nutzerkommunikation unbemerkt ausspioniert werden.

- Durch die laufende unbemerkte Auswertung von Standortdaten eines mobilen Geräts, z.B. durch im Hintergrund laufender standortbezogener Dienste *(Location Based Services – LBS)*, kann ein Bewegungsprofil des Nutzers erstellt werden.[2]

- Angriffe auf die Verfügbarkeit von mobilen Geräten sind unter Umständen leichter durchführbar (z.B. Störsignale auf den entsprechenden Frequenzbändern) als vergleichbare Attacken auf Arbeitsplatzrechner.

- Durch die Nutzung von Kurzstreckenfunkverbindungen wie z.B. Bluetooth, die es einem Angreifer unter Umständen ermöglichen, die Kontrolle eines ungeschützten Geräts zu übernehmen.

Zudem ergeben sich Risiken im Zusammenhang mit der Speicherung und der direkten Datenverarbeitung auf mobilen Geräten:

- Mobile Geräte werden oft vom Anbieter mit zahlreichen zusätzlichen Anwendungen zur Datenverarbeitung ausgeliefert. Von einem seriösen Anbieter ist zu erwarten, dass dieser entdeckte Mängel und Verwundbarkeiten vor der Veröffentlichung der Software behebt. Allerdings können andere Firmen und Privatpersonen durch teilweise offene und dokumentierte Programmierschnittstellen und Entwicklungsumgebungen Software (so genannte „Apps“) für mobile Geräte entwickeln und über das Internet einfach und kostengünstig verbreiten. Durch die Installation solcher Fremdanwendungen von Dritt-Anbietern steigt das Risiko der Infektion durch Schadsoftware bzw. der Datenbeschädigung durch unsichere Applikationen. Die Stabilität des gesamten Systems kann durch die nachträgliche Installation von nicht beglaubigter (zertifizierter) Drittsoftware beeinträchtigt werden.[3]

- Durch die Entwicklung einheitlicher Betriebssysteme und Standards für mobile Geräte wird zwar die Softwareentwicklung vereinfacht. Diese Standardisierung kann aber bei Verwundbarkeiten zu einem erhöhten Risiko der Verbreitung von Schadsoftware führen, wie es bereits in der Welt des „personal computing“ sichtbar ist. Allerdings ermöglichen einheitliche Betriebssysteme die Implementierung einheitlicher Sicherheitsmaßnahmen.

- „Push-Dienst“ oder „Server-Push-Dienst“ beschreibt eine meist internetbasierte Methode der Inhaltsverbreitung. Dabei werden Informationen von einem zentralen Server direkt an das mobile Geräte exportiert und dort unmittelbar verarbeitet. Durch eine ungeprüfte Verarbeitung der eingehenden Nachrichten entstehen Risiken, die heute aus dem Bereich der Email-Verarbeitung auf Arbeitsplatzrechnern bereits bekannt sind (z.B. Schadsoftware in Anhängen, Ausnutzung von Schwachstellen in der Verarbeitungssoftware, usw.).

---

[2] Gemeinsamer Standpunkt der IWGDPT zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, http://www.datenschutz-berlin.de/attachments/192/local_neu-de.pdf

[3] Im gegenständlichen Arbeitspapier bleiben sämtliche Aspekte der Privatsphäre im Zusammenhang mit Drittanbieter-Software unberücksichtigt.

Die Erfahrung zeigt, dass eine Balance zwischen der Implementierung von zu restriktiven und möglicherweise von den Nutzern daher nicht akzeptierten Sicherheitsvorgaben im Umgang mit mobilen Datenträgern sowie Geräten einerseits und der Bereitstellung eines sicheren Umfelds mit ausreichendem Schutz der Daten andererseits gefunden werden muss.

Die blosse Verschlüsselung der Daten und sensitiver Informationen *ohne* die Anwendung begleitender Massnahmen und von Verhaltensstandards ist *kein* effektiver Weg, um jeglichen Risiken und Sicherheitsbedenken zu begegnen.

Empfehlungen

Basierend auf den oben angeführten Risiken richtet die Arbeitsgruppe folgende (vorläufige) Empfehlungen an Anbieter und Nutzer mobiler Endgeräte.

Anbieter

Die grundlegenden Sicherheitseinstellungen des mobilen Geräts sollten bei der Auslieferung das höchste Mass an Sicherheit berücksichtigen und im Einklang mit dem Zweck stehen, für den das Gerät vermarktet wird.

Ein oder mehrere Nutzerprofile mit konfigurierbar eingeschränkten Rechten sollte existieren, zusammen mit einem „Super-User“, der den Zugriff auf die Sicherheitseinstellungen für diese Nutzerprofile kontrollieren und einschränken kann.

Der Nutzer sollte in einfacher Weise über jegliche Änderung an den Sicherheitseinstellungen informiert werden. Dies könnte zum Beispiel bei der Aktualisierung von Systemsoftware (z.B. Firmware- oder Betriebssystem-Update) oder durch die Installation von zusätzlichen Anwendungen der Fall sein.

Das Handbuch sollte jedenfalls ein eigenes Kapitel zum Thema „Sicherheit“ und den „Sicherheitseinstellungen“ enthalten. Dabei sollte auf die Risiken der Benutzung mobiler Geräte eingegangen und dem Nutzer ein übersichtlicher und verständlicher Leitfaden zur sicheren Handhabung gegeben werden.

Eingebaute Hardwarekomponenten und Schnittstellen, die zur Erhebung und Übermittlung von Daten dienen (z. B. Kamera, GPS, Mikrofon, IrDA, Bluetooth, WLAN, usw.), sollten werksseitig deaktiviert sein; diese Schnittstellen sollte, abhängig von den Rechten des entsprechenden Nutzerprofils, für den Nutzer verfügbar sein, und bei Bedarf aktiviert werden können.

Bei Mobiltelefonen kann der unbefugte Zugriff auf die SIM-Karte durch eine PIN geschützt werden. Über eine entsprechende Sicherheitseinstellung sollte dieser Zugriffsschutz auf den Telefonspeicher ausgeweitet werden können. Ein Nutzer sollte eine Zeitspanne bestimmen können, nach der das Gerät bei Inaktivität das Display/Tastatur sperrt und erst wieder nach erneuter Eingabe der PIN oder eines frei wählbaren Passworts freigibt.

Zur Kommunikation

Ein Nutzer sollte gewarnt werden, wenn möglicherweise unsichere Kommunikationskanäle für die Datenübertragung genutzt werden.

Wenn ein mobiles Gerät den Kontakt zu einer sicheren WLAN-Verbindung verliert und sich anschliessend automatisch mit einem unsicheren WLAN Netzwerk verbindet, sollte eine Warnung an den Nutzer ausgegeben werden.

Es sollte für einen Nutzer einfach erkennbar sein, ob externe Kommunikationskanäle und Schnittstellen aktiv oder inaktiv sind. Zusätzliche Dienste, wie z.B. Schnittstellen für die Kommunikation, sollten auf einem mobilen Gerät durch den Nutzer einfach ein- und ausgeschaltet werden können.

Zur Speicherung und Datenverarbeitung

Bei der nachträglichen Installation oder dem Herunterladen von nicht beglaubigter (zertifizierter) Software eines Drittanbieters sollte ein entsprechender Warnhinweis an den Nutzer ausgegeben werden.

Ein Nutzer sollte vor dem Herunterladen und vor der Installation von Applikationen die Möglichkeit haben, insbesondere den Namen und die elektronische Signatur des Anbieters, die Nutzungsbedingungen, die zur Ausführung erforderlichen Zugriffsrechte auf Gerätehardware sowie bereits installierter Software, Hinweise zur Deinstallation als auch weitere sicherheitsrelevante Informationen und Warnhinweise in einfacher Weise und in einer selbst gewählten Sprache einzusehen.

Ein Nutzer sollte die Möglichkeit haben, den Zugriff jeder installierten Applikation auf die verfügbare Gerätehardware (z.B. Netzwerkkarte, Kamera, usw.) sowie auch auf gespeicherte Daten (z.B. auf den Kalender oder das Adressbuch) einzuschränken.

Es sollte für den Nutzer einfach nachvollziehbar sein, welche Daten im mobilen Gerät verschlüsselt und welche unverschlüsselt abgespeichert werden.

Nutzer

Die Bewusstseinsbildung ist ein erster wichtiger Schritt zur Vorbeugung von Missbrauch, Datenverlust und Diebstahl. Die Nutzer sollten auf ihre Eigenverantwortung im Zusammenhang mit der Datensicherheit und Integrität hingewiesen werden. Unterstützend dazu folgende Empfehlungen:

Der Nutzer sollte nach einer Aktualisierung der Systemsoftware (z.B. Firmware-Update) die lokalen Sicherheitseinstellungen des mobilen Geräts überprüfen und wenn erforderlich auf die eigenen Bedürfnisse anpassen.

Bei Verwendung eines mobiles Geräts in einem öffentlichen Bereich, sollte der Nutzer alle Anstrengungen unternehmen, um sicherzustellen, dass der Bildschirm und die Tastatur durch Passanten oder Überwachungskameras eingesehen werden kann.

Bei der Nutzung mobiler Geräte eines Unternehmens, sind die durch die Fachabteilung erarbeiteten organisatorischen Massnahmen unbedingt einzuhalten. Technische Manipulationen und Änderungen an den Systemeinstellungen sollten unterlassen werden.

Zur Kommunikation

Öffentliche Internetzugänge sollten mit Vorsicht verwendet werden. Vertrauliche Informationen und Daten sollten nicht über unsichere Netzwerkverbindungen verarbeitet werden, wenn die Übertragung nicht ausreichend durch zusätzliche Sicherheitsmassnahmen, wie z.B. einen virtual private network (VPN) -Tunnel, geschützt ist.

Vor dem Austausch von *vertraulichen* Informationen sollte die Identität des Kommunikationspartners geprüft werden. Jede unbekannte Meldung oder Unregelmässigkeit im Betrieb sollte hinterfragt und im Zweifel ein Experte oder in einem Firmenumfeld die verantwortliche Stelle Informiert bzw. zu Rate gezogen werden.

Für den unmittelbaren Betrieb nicht benötigte Schnittstellen sollten über die Einstellungen des mobilen Geräts deaktiviert werden (z.B. Einrichtungen zur Datenübertragung mit Bluetooth, Infrarotsignalen (IrDA),

drahtlosen Netzwerken (WLAN), usw.). Speziell standortbezogene Dienste *(Location Based Services – LBS)* sollten deaktiviert sein, wenn sie nicht unmittelbar genutzt werden.

Zur Speicherung und Datenverarbeitung

Vor der Installation von Fremdapplikationen sollte die Quelle genau geprüft werden. Signaturen und Herstellerangaben können das Risiko einer Infektion minimieren. Im Zweifel sollte von einer Installation abgesehen werden.

Der Zugriff der installierten Fremdapplikationen sollte auf die für den ordnungsgemässen Betrieb erforderlichen Daten eingeschränkt werden. So benötigt zum Beispiel nicht jede Anwendung den Zugriff auf das Adressbuch oder den Kalender des mobilen Geräts.