Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

26.

Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016

Tätigkeitsbericht 2015-2016

26. Tätigkeitsbericht

Dieser Bericht wurde am 30. Mai 2017 dem Präsidenten des Deutschen Bundestages, Herrn Prof. Dr. Norbert Lammert, überreicht.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Andrea Voßhoff

schaft - Ressortbereich	sung bis Ende 2016 vorgesehen.
Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit Ressortbereich	Es gibt noch 122 Systeme mit Windows XP, deren Ablösung für 2016 vorgesehen ist.
Bundespräsidialamt	Es sind keine kritischen Systeme mit Windows XP im Einsatz.
Bundesministerium für Gesundheit	Es gibt noch 9 Systeme mit Windows XP ohne Netzanschluss, der Zeitpunkt der Ablösung ist noch offen.
Bundeministerium der Verteidigung	Es gibt noch ca. 12.000 Systeme mit Windows XP ohne Netzanschluss, deren Ablösung für Ende 2016 vorgesehen ist. Für diese Systeme gibt es Sonderverträge mit Microsoft.
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung	Es gibt noch 2 Systeme mit Windows XP ohne Netzanschluss, der Zeitpunkt der Ablösung ist noch offen.

10.2.11.4 Windows 10

Neue Betriebssysteme werben mit personalisierten Diensten und benötigen hierfür personenbezogene Daten. Hierüber informieren sie die Nutzerinnen und Nutzer in ihren Datenschutzerklärungen. Sind diese Datenschutzerklärungen jedoch verständlich und klar formuliert und, vor allem, halten sich die Hersteller daran? Ein guter Grund, sich die Datenschutzerklärung am Beispiel von Windows 10 einmal genauer anzusehen.

Der Trend bei der Entwicklung von Betriebssystemen geht in den letzten Jahren immer mehr in Richtung Onlinefunktionalität. Dabei ist der Austausch von Daten über das Internet, z. B. des Clientsystems mit einer Cloud, zum Standard geworden. Microsoft, der Hersteller des Betriebssystems Windows 10, folgt diesem Trend und bietet umfangreiche Dienste an, die dem Nutzer die tägliche Arbeit erleichtern und eine unbegrenzte Verfügbarkeit der Daten sicherstellen soll. Auch andere Hersteller wie Apple oder Google bieten diese Dienste an und nutzen die ständige Verbindung der Clientsysteme mit dem Internet. Allen Herstellern gemein ist, dass sie dafür Daten des Clientsystems, z. B. Positionsdaten, und Daten des Nutzers verwenden. Die größte Funktionalität bieten hier personalisierte Dienste, wie die Hersteller hervorheben. Um aber einen Dienst zu personalisieren, bedarf es personenbezogener Daten. Wie die Daten erhoben, verarbeitet und gespeichert werden und um welche Daten es sich handelt, darüber muss der Hersteller die Nutzerinnen und Nutzer in einer entsprechenden Datenschutzerklärung informieren.

Die Datenschutzerklärung von Microsoft zu Windows 10, die über die Webseite des Herstellers abgerufen werden kann, beschreibt sehr umfangreich, welche Daten vom Betriebssystem selbst und den dazugehörigen Diensten erhoben werden (Stand: Anfang März 2017). Gerade bei den Diensten wird deutlich, dass sich Microsoft vorbehält, umfangreiche personenbezogene Daten zu erheben und zu verarbeiten. Doch auch wenn man diese Dienste nicht nutzen will und deaktiviert, werden personenbezogene Daten erhoben und an den Hersteller gesendet, wie die Datenschutzerklärung verrät.

Bei der Aktivierung von Windows 10 werden neben einem Produktschlüssel, der dem Gerät zugeordnet wird, Daten zur Software und zum Gerät erhoben. Diese nicht genauer definierten Daten werden „bei Bedarf einer Lizenzvalidierung“ erneut erhoben und an Microsoft gesendet, wobei nicht erläutert wird, wie diese Daten verarbeitet, an wen sie weitergegeben und wie lange sie gespeichert werden.

Bei mobilen Geräten, auf denen Windows 10 installiert ist, werden Geräte- und Netzwerkidentifizierungsmerkmale („device and network identifiers“) erhoben. Da diese Identifizierungsmerkmale für jedes Gerät einmalig

sind und ein Bezug zu weiteren auf dem Gerät gespeicherten, persönlichen Daten hergestellt werden kann, können diese Daten als personenbezogene Daten angesehen werden. Das Auslesen und Verarbeiten dieser Daten wird seit Jahren von Datenschützern kritisiert. Darüber hinaus wird die Position des Gerätes beim Einschalten erfasst.

Jedem Nutzer, der sich auf einem Windows 10 System anmeldet, wird ein Identifizierungsmerkmal, die Werbe-ID, zugeordnet („unique advertising ID for each user on a device“), durch das der Nutzer eindeutig identifiziert werden kann. Der Zugriff auf diese Werbe-ID muss explizit abgeschaltet werden, dabei wird sie allerdings nicht gelöscht.

Microsoft erfasst die präzise Position von Geräten, auf denen Windows 10 installiert ist. Dafür werden GPS-Daten, WLAN-Daten und die IP-Adresse des Gerätes ausgewertet und in einer Datenbank bei Microsoft gespeichert. Das Unternehmen gibt an, alle Daten, über die sich eine Person oder ein Gerät identifizieren lassen, vor der Weitergabe an Dritte zu entfernen. Dabei sagt es aber nicht, um welche Daten es sich bei den entfernten Daten handelt. Bei einer IP-Adresse handelt es sich z. B. um ein personenbezogenes Datum, über das die Position eines Gerätes in manchen Fällen bis auf einen Postleitzahlenbereich eingegrenzt werden kann. Der Lokalisierungsdienst kann durch den Nutzer abgeschaltet werden, die erhobenen Daten verbleiben jedoch in der Datenbank von Microsoft.

Microsoft bietet mehrere Dienste zur Gewährleistung der Sicherheit und zum Schutz des Gerätes an, wie Smart Screen und Windows Defender. Entsprechend seiner Datenschutzerklärung behält sich das Unternehmen vor, Dateien, die heruntergeladen werden bzw. sich auf dem System befinden und möglicherweise Schadsoftware enthalten können („it may also send files that could contain malware“), an Microsoft zu senden. Außerdem senden diese Dienste Berichte und wenn Microsoft personenbezogene Daten in diesen Berichten vermutet („report is likely to contain personal data“), muss der Nutzer den Versand bestätigen. Diese Dienste müssen explizit abgeschaltet werden.

Unter dem Merkmal „Getting to know you“ sammelt Microsoft personenbezogene Daten wie z. B. Sprachdaten, handschriftliche Daten und Daten, die über die Tastatur eingegeben werden. Letztere werden um IDs, IP-Adressen und andere mögliche Identifizierungsmöglichkeiten bereinigt („we scrub to remove IDs, IP addresses, and other potential identifiers“). Weitere Dienste erheben darüber hinaus Namen, Spitznamen, Kalenderdaten, Kontaktdaten, Namen von bevorzugten Orten und benutzten Anwendungen, allerdings erfolgt die Übertragung nur mit Zustimmung des Nutzers. Ein Teil dieser bei Microsoft gespeicherten Daten, wie Kontakte und Kalenderdaten, kann über ein Microsoft-Konto gelöscht werden, was mit den anderen personenbezogenen Daten passiert, wird nicht erklärt.

Ein umfangreicher Teil der erhobenen Daten betrifft die sogenannten Telemetriedienste. Telemetrie umfasst alle Daten eines Systems, die auf diesem System gemessen/erhoben und an Microsoft übertragen werden. Entsprechend der Datenschutzerklärung handelt es sich um Diagnose- und Nutzungsdaten, die das Unternehmen zur Identifizierung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Personalisierung des Systems nutzt. Bedenklich sind hier zwei Aspekte, die Microsoft in seiner Datenschutzerklärung angibt. Zum einen werden diese an Microsoft übertragenen Daten mit einem oder mehreren eindeutigen Identifizierungsmerkmalen verknüpft, die es dem Unternehmen ermöglichen, einen individuellen Nutzer auf einem individuellen Gerät und dessen Nutzungsmuster (wieder) zu erkennen („stored with one or more unique identifiers that can help us recognize an individual user on an individual device“). Zum anderen können diese Telemetriedienste nicht vollständig abgeschaltet werden und somit kann eine Übertragung personenbezogener Daten, wie z. B. der IP-Adresse, an Microsoft nicht verhindert werden.

Wie zusammenfassend festzustellen ist, kann bei der Verwendung von Windows 10 auch trotz optimaler Konfiguration aller Datenschutzeinstellungen die Übertragung und Verarbeitung personenbezogener Daten auf Serversystemen von Microsoft in den USA nicht verhindert werden. Dies bestätigen u. a. Untersuchungen des Bayerischen Landesamtes für Datenschutzaufsicht, das sich im Rahmen seiner Mitarbeit in der Artikel-29-Gruppe der europäischen Datenschutzbehörden mit Windows 10 beschäftigt. Das Bundesamt für Sicherheit in der In-

formationstechnik (BSI) ist zu den gleichen Erkenntnissen gekommen. Die ausgelesenen Daten können nicht geprüft werden, da sie verschlüsselt übertragen werden. Weder gegenüber dem BSI noch gegenüber meinen europäischen Kollegen, die sich bereits in zwei Briefen an Microsoft gewandt haben, hat das Unternehmen offengelegt, welche Daten gesammelt und wofür sie verwendet werden.

Solange der Hersteller hier nicht für Transparenz sorgt, muss ich ihn in Form seiner Datenschutzerklärung beim Wort nehmen und davon ausgehen, dass personenbezogene Daten erhoben und übertragen werden. Des Weiteren muss der Hersteller neben der nötigen Transparenz dem Nutzer ermöglichen, die Übertragung seiner Daten ganz zu unterbinden bzw. die gesammelten Daten einsehen und vollständig löschen zu können. Hier hat der Hersteller nur halbherzig Maßnahmen ergriffen.

Das intransparente Vorgehen von Microsoft kritisiere ich und empfehle dem Hersteller, hier für Klarheit und Abhilfe zu sorgen. Dies auch vor dem Hintergrund, dass die neue Datenschutz-Grundverordnung jeden Verantwortlichen ab Mai 2018 verpflichten wird, die Grundsätze von privacy by design und privacy by default zu beachten und Verletzungen dieser Grundsätze mit hohen Geldbußen belegt. Ich werde die weitere Entwicklung bei Windows 10 beobachten und - insbesondere im Rahmen eines möglichen Einsatzes in der Bundesverwaltung - kritisch begleiten.

10.2.11.5 Das Standard-Datenschutzmodell

Die Arbeiten am „Standard-Datenschutzmodell“ (SDM) wurden weitergeführt. Der Blickwinkel richtete sich zunächst auf die Definition von geeigneten Schutzzielen und Verfahren zur Herstellung von Datensicherheit.

Schutzziele und ein darauf aufbauendes IT-Sicherheitsmanagement werden schon seit einigen Jahren im Bereich der IT-Sicherheit eingesetzt, beispielsweise in den IT-Sicherheitsbewertungskriterien, dem sog. Orange Book oder den Common Criteria. Bei der Umsetzung werden allerdings auch Defizite dieser Verfahren und Schutzziele erkennbar. So bringen sie keine Struktur in den Bereich der Schutzziele, sodass im Laufe der Zeit eine immer unübersichtlichere Sammlung von nebeneinander stehenden Schutzzielen entstanden ist und weiter entsteht. Die verschiedenen Verfahren beschäftigen sich auch nicht mit Wechselwirkungen von Schutzzielen, d. h. ob und inwiefern sich diese gegenseitig verstärken oder schwächen oder gar implizieren oder gegenseitig ausschließen. Aufgrund dieser mangelnden Harmonisierung gibt es keine Gesamtschau von den einzeln nebeneinander stehenden Schutzzielen und keine Überlegungen zu ihrer Vollständigkeit.

Nach vielen Jahren des Erprobens solcher Verfahren entwickelte Mitte der 1990er Jahre das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Modell des Grundschutzes, um die Umsetzung solcher Verfahren zu vereinfachen. In der Zwischenzeit ist der IT-Grundschutz zu einem praktikablen Werkzeug zur Sicherstellung der IT-Sicherheit geworden. Das Verfahren beruht auf einem einfachen Modell (vgl. Kasten a zu Nr. 10.2.11.5).

Das BSI überarbeitet zwar derzeit den Grundschutz, aber an den grundsätzlichen Erwägungen wird sich auch in Zukunft nichts ändern. Bereits in meinem 15. Tätigkeitsbericht (Nr. 30.8) habe ich den Einsatz von Grundschutz befürwortet und dies auf eine einfache Formel gebracht:

DATENSCHUTZ = Grundschutz + X

In den vielen Jahren der Anwendung dieser Formel wurde darüber diskutiert, wie denn die X-Komponente zu bestimmen und welcher „Wert“ angemessen sei. Dies hängt natürlich von den konkreten Rahmenbedingungen, Systemen, Daten usw. ab und konnte bislang nur sehr rudimentär ermittelt werden.