Stadt Hamm
Stellungnahme der Verwaltung

Stadtamt	Stellungnahme-Nr.
40	0295/15

zur Anfrage Nr. 0200/15
d. Frau/Herrn/Fraktion
Georg Sander vom 13.05.2015

Datum: 08.06.2015

Genehmigungsvermerk: I, gez. OB Hunsteger-Petermann

Federführender Dezernent: II, gez. StK Kreuz

Bezeichnung: iPad an Schulen

Beteiligte Dezernenten:

Verteiler	Sitzungstermin
Schulausschuss	18.06.2015

Wortlaut der Anfrage:

Wir bitten um die Beantwortung folgender Fragen:

1) Inwieweit ist bei der Nutzung der iPads im Unterricht der Datenschutz gewährleistet? Kommt es konkret bei der Nutzung der eingesetzten Apps zum Tracking, mit dem alle Aktionen jedes einzelnen Nutzers protokolliert und an die Hersteller übertragen werden, die daraus personalisierte Profile erstellen können, oder ist dieses garantiert ausgeschlossen? Welche Gegenmaßnahmen werden ggf. ergriffen?
2) Wie sind in diesem Zusammenhang die Schulnetzwerke (Hardware, Software, Protokolle, Verschlüsselung) gesichert, mit denen in und ggf. zwischen den Schulen Daten ausgetauscht werden können?
3) Wird die digitale Kommunikation zwischen Lehrern und Schülern außerhalb der Schule verschlüsselt?

Stellungnahme der Verwaltung:

In jeder Schule werden zwei voneinander (physikalisch) getrennte Netze für Verwaltung und Pädagogik betrieben. Die nachfolgenden Aussagen beziehen sich daher ausschließlich auf das jeweilige pädagogische Netzwerk.

Zu1:
Der Datenschutz innerhalb der lokalen schulischen Netzwerke ist durch verschiedene Sicherheitsmechanismen hinsichtlich Zugangs- und Zugriffsberechtigung nach heutigem Stand gewährleistet, solange sich die Nutzer an die vorgegebenen Regelungen hinsichtlich der Auswahl und Verwendung von Benutzerkennungen und Kennwörtern und die Weitergabe von Daten halten. Inwieweit es bei der Nutzung von IPAD´s und damit verbundener Anwendungen zu „Tracking“ bei Internetzugang kommt, kann von hier nicht beurteilt und daher auch nicht ausgeschlossen werden. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) weist in seinem Gefährdungskatalog unter G 2.159 jedoch ausdrücklich darauf hin, dass diese Möglichkeit besteht. Um ein Apple-Gerät nutzen zu können, ist es notwendig, die von Apple vorgegebenen Bestimmungen zu akzeptieren. In der Datenschutz-Richtlinie des Unternehmens findet sich ein entsprechender Absatz. Demnach darf Apple u.a. „präzise Standortdaten“ erheben, nutzen und weitergeben. Es ist daher davon auszugehen, dass auch App-Anbieter derartige Daten über ihre

Anwendungen erheben und speichern. Um die Funktionsfähigkeit der Geräte und Anwendungen zu gewährleisten, ist es nach heutigem Stand nicht möglich, ein „Tracking“

zu verhindern. Es ist daher zu empfehlen, den Anwendern im Rahmen der zu vermittelnden Medienkompetenz den sensiblen Umgang mit personenbezogenen Daten und die vielfältigen system- und anwenderspezifischen Sicherungsmöglichkeiten zu vermitteln. Im Übrigen ist anzumerken, dass mit den schulischen iPads Unterrichtsinhalte bearbeitet werden sollen und dabei relevante personenbezogene Daten i.d.R. nicht anfallen. Anmeldungen zu bestimmten, unterrichtlich genutzten Webseiten (z.B. Foren) erfordern tlw. personenbezogene Daten.

Zu 2:
Die für den Datenaustausch und den Internetzugang erforderliche Anbindung mobiler Endgeräte in den lokalen pädagogischen Netzwerken der Projektschulen erfolgt zurzeit über WLAN Accesspoints (AP´s) der Firmen Hewlett Packard und Apple. Die Grundkonfiguration der AP´s ist so eingerichtet, dass die Geräteberechtigung und nachfolgende Verschlüsselung des Datenstromes im Pre-Shared Key (PSK) Verfahren oder durch Authentifizierung gegen einen Radius-Server für eine erfolgreiche Verbindung abgefragt wird. Die Verbindung selbst ist dann nach Sicherheitsstandard IEEE 802.11i mit Wi-Fi Protected Access 2 (WPA2) verschlüsselt.

Die AP´s sind in die kabelgebundenen lokalen Netze der Schulen integriert, in denen jeweils ein Datei- und Dienste-Server verfügbar ist. Dieser Server übernimmt auch die weitere Zugangs- und Zugriffskontrolle mit entsprechenden Authentifizierungsdiensten auf Basis einer Benutzer- und Gerätedatenbank. Unter anderem bietet dieser Server für mobile Endgeräte im Rahmen des WebDav-Protokolls die Möglichkeiten für einen lokalen Datenaustausch innerhalb der Schulen. Dieses Protokoll ist unverschlüsselt, über den Port 80 (http) und verschlüsselt über den Port 443 (https) nutzbar. Weitere auf den schon vorhandenen Verfahren zur Datei- und Kommunikationsverschlüsselung können bedarfs- und endgeräteabhängig eingesetzt werden. Ein Datenaustausch zwischen den Schulen ist über das Internet möglich (email, Clouddienste). Der Internetzugang erfolgt über einen Proxydienst, der Zugangs- und Filterregeln verwaltet. Die Kommunikation erfolgt gegenstellen- und anwendungsabhängig verschlüsselt oder unverschlüsselt über die Ports 80 (http)und 443 (https). Weiterhin regelt dieser Server mit Hilfe eines Firewall-Dienstes den Datenverkehr in das Internet und schützt das lokale Netzwerk der Schule gegen unberechtigte Zugriffe.

Die Anbindung der lokalen Netzwerke der Schulen an das Internet erfolgt zurzeit über einen ADSL Router der Firma AVM, der ebenfalls über einen Firewall-Dienst eine Zugangs- und Zugriffskontrolle ermöglicht.

Die Grundkonfiguration aller Komponenten hinsichtlich Zugangs- und Zugriffsmöglichkeiten ist restriktiv ausgelegt. Die Schulen haben jedoch die Möglichkeit, über ihre IT-Beauftragten, die Konfiguration an ihre jeweiligen pädagogischen und didaktischen Erfordernisse anzupassen. Die IT-Beauftragten sind daher in die Funktionen und Möglichkeiten eingewiesen und können entsprechend angebotene Schulungen besuchen, um die Auswirkung durchgeführter Konfigurationsänderungen unter Sicherheits- und Datenschutzaspekten beurteilen zu können.

zu 3:

Die Kommunikation von Schülern und Lehrern außerhalb der Schule ist nicht Gegenstand des Aufgabenspektrums des Schulträgers und ist wie die digitale Kommunikation von jedermann grundsätzlich anwendungs- und vor allem anwenderabhängig.