Schleswig-Holsteinischer Landtag
Umdruck 18/1491

An den
Bildungsausschuss
des Landtages Schleswig-Holstein
Frau Vorsitzende Anke Erdmann, MdL

Landeshaus
Düsternbrooker Weg 70
24105 Kiel

per E-Mail an das Ausschussbüro
Herrn Geschäftsführer Herr Ole Schmidt
bildungsausschuss@landtag.ltsh.de

Toppoint e. V.
Eckernförder Str. 20
24103 Kiel

Tel.: 0431 - 56 21 36 (Vereinsräume)

E-Mail: vorstand@toppoint.de
Web: www.toppoint.de

Vertretungsberechtigter Vorstand:
Frank Bartels, Daniel Ehlers
Eingetragen beim Amtsgericht Kiel:
502 VR 3441

Ihr Zeichen L213/Ihr Schreiben vom 7. Juni 2013
Unser Zeichen LTSH/Detek/07/2013

31. Juli 2013

Stellungnahme zum

- Antrag der Fraktion der PIRATEN „**Detektoren an Schulen untersagen**“ (Drucksache 18/625) sowie zum
- Änderungsantrag der CDU, „**Elektronische Schummelei bei Abschlussprüfungen unterbinden**“ (Drucksache 18/645)

Sehr geehrte Frau Erdmann,

für die Toppoint – Verein zur Förderung der privaten Datenkommunikation, Kiel, darf ich Ihnen herzlich für die Möglichkeit zur Stellungnahme zum Thema danken.

Zusammenfassend stellen wir Folgendes fest

Die Verwendung sogenannter Detektoren, mit dem Ziel, im Rahmen von schulischen Prüfungen Täuschungsversuche aufzudecken, die womöglich mit Mitteln der drahtlosen Kommunikation unternommen werden, ist unserer Ansicht nach technisch sinnvoll nicht machbar. Die Geräte dürften entweder nicht leisten, was sie versprechen, oder sie erfordern ein Eindringen in die Inhalte der Kommunikation, das weit über das Erfassen persönlicher Daten hinausgeht.

Darüber hinaus wünschen wir uns, dass die ernsthafte Vermittlung von technischen Grundlagen und Anwendungskompetenzen gerade auch im Bereich moderner Kommunikationsformen stärker in den Mittelpunkt gerückt wird, weil diese mit Sicherheit wichtig für die Zukunft der Lernenden sein wird. Dies wird viel weniger gelingen können, wenn man gleichzeitig die Nutzung vieler technischer Geräte erschwert, indem man krampfhaft versucht, ihre Nichtanwendung in bestimmten Situationen zu kontrollieren (was letztlich ja ohnehin scheitern muß, wie dargelegt).

Im Zusammenhang mit den Versuchen von Schülerinnen und Schülern, den Defiziten einer punktuellen und simplifizierenden Leistungsbeurteilung etwas entgegenzusetzen jedenfalls ist das Täuschungspotenzial nicht höher einzuschätzen als das des klassischen Spickers.

Begründung

Nach derzeitigem Stand kommen für Schülerinnen und Schüler Mobilfunkgeräte zwar hauptsächlich handelsübliche Mobilfunkgeräte (heute typischerweise sogenannte Smartphones) als Mittel möglicher „elektronischer Betrugsversuche“ in Betracht. Gleichwohl sind diese Geräte in der Lage, auf verschiedenen Wegen Daten drahtlos auszutauschen: a) über die Kommunikationsdienste der Mobilfunkanbieter und b) über drahtlose Computer-Netzwerkverbindungen, kurz WLANs.

Beide Kommunikationsformen benutzen nicht eine, sondern mehrere unterschiedliche und zum Teil sehr weit auseinanderliegende Frequenzen.

Für die Kommunikationsdienste der Mobilfunkanbieter sind dies die Frequenzbereiche um

- 0900 MHz, um
- 1800 MHz sowie um
- 3600 MHz.

Drahtlose Computernetze (WLANs/Bluetooth) arbeiten in den Bereichen um

- 2400 MHz sowie um
- 5000 MHz.

Entscheidend für unsere Bewertung ist die Tatsache, dass die dabei gewonnenen Ergebnisse sich kaum einem Klassenraum und schon gar nicht einem Schüler, einer Schülerin zuordnen lassen.

So muss im Bereich der von Mobilfunkanbietern gebotenen Kommunikationsdienste damit gerechnet werden, dass eventuell erfasste Signale nicht aus dem Prüfungsraum, sondern aus dem näheren Umfeld der Schule stammen. Naturgemäß wären Schulen in städtischer Umgebung davon stärker betroffen als solche in siedlungsferneren Gebieten.

Noch schwieriger stellt sich die Lage im Bereich drahtloser Computernetze dar. WLANs sind heute eine allgegenwärtige Erscheinung und in fast jedem Haushalt zu finden. Die Signale dieser Netze unterscheiden sich nicht von denjenigen, die Prüflinge mit ihren Geräten emittieren würden.

Gerade die WLAN-Frequenzen werden zudem von zahlreichen anderen Diensten verwendet. Als Teil der für „Industry, Science and Medical“-Bänder (ISM) teilen sich WLANs ihre Bänder mit zahlreichen anderen Diensten. Mögliche Nutzungen wären beispielsweise Handsprechfunkgeräte, Babyphones und drahtlose Mikrofone ebenso wie Kfz-Schlüssel, Türöffner,

Videoübertragungsanlagen oder Bewegungsmelder. selbst Mikrowellenöfen benutzen Frequenzen im WLAN-Bereich, um Speisen und Getränke zu erwärmen. Unter Umständen ist dann damit zu rechnen, dass der warme Kakao der Kollegin in der Freistunde die Prüfung lahm legt. Da die WLAN-Frequenzen darüber hinaus zu den ISM-Bändern vom Typ B gehören, ist zum Betrieb der Geräte keine Genehmigung erforderlich; jedwede Störung ist hinzunehmen. Unter diesen Bedingungen lässt sich nicht im Ansatz sagen, aus welchem Grund ein Detektor gerade anschlägt.

Derzeit keine technische Lösung

Technisch ist der Problematik kaum beizukommen. Es brächte zunächst wenig, die Reichweite des Detektors zu verringern. Da sich elektromagnetische Wellen konzentrisch ausbreiten, würde man entweder nur Teile des Raumes erfassen oder eben größere Bereiche außerhalb des Prüfungsortes.

Gegen ein Eindringen von „Fremdsignalen“ abschirmen ließe sich der Prüfungsraum nur, indem man ihn zu einem Faraday'schen Käfig ausbaute. Das hätte zwar auch den Vorteil, dass keine Kommunikation mit „außen“ möglich wäre, ist aber wohl allein baulich schon ein undurchführbares Vorhaben; vom finanziellen Aufwand ganz abgesehen.

Sicher zu einem belastbaren Ergebnis würde man kommen, würde man den Inhalt der Verbindung mitlesen. Eine Zuordnung zu einem Gerät und letzten Endes zu einer Schülerin, einem Schüler wäre fast mit Sicherheit möglich. Allerdings wäre dazu in jedem Fall die Erfassung persönlicher Daten und darüber hinaus das Erbrechen der standardmäßig durch Verschlüsselung die drahtlose Kommunikation umgebenden Siegel notwendig.

Als einziger Ausweg bliebe also, die Prüfung bei jedem Anschlagen des Detektors so lange zu unterbrechen bis die Herkunft des auslösenden Signals einwandfrei geklärt ist und einer Schülerin/einem Schüler zugerechnet wurde. Es gehört wenig Fantasie dazu, wie leicht sich SchülerInnen damit einen Klagegrund schaffen könnten, um das Prüfungsergebnis anzufechten. Ergänzend darf man anführen, dass eine Prüfungssituation unter den Bedingungen einer vollständigen, digitalen Dauerüberwachung kaum dazu geeignet sein dürfte, Höchstleistungen zu ermöglichen.

Nutzungsfremde Störquellen

Alle bis hierhin betrachteten Störungen haben ihre Ursache in der hinzunehmenden Nutzung der infrage kommenden Frequenzbänder durch andere Dienste. Es sei abschließend noch auf zwei mögliche nutzungsfremde Störquellen hingewiesen. So kann (erstens) nicht ausgeschlossen werden, dass andere technische Gerätschaften im Falle eines Defekts Störsignale aussenden, die den Gebrauch von WLAN und Mobiltelefon unmöglich machen. Ein solches Signal würde selbstverständlich auch von einem Detektor erfasst und als Betrugsversuch gemeldet.

Zweitens: Die indifferente Signalauswertung eines Detektors würde es Schülerinnen und Schülern erlauben, Prüfungen ihrer Interessenlage entsprechend zu manipulieren. So wäre es durchaus denkbar, dass eine Schülerin/ein Schüler im Bestreben, ihre/seine Leistung zu unterstreichen, einen für wenig Geld erworbenen und in Betrieb genommenen WLAN-Router benutzt, um die Prüfung der vermeintlichen KonkurrentInnen zu stören. Und mindestens ebenso wahrscheinlich dürfte es sein, dass eine Schülerin/ein Schüler eine Prüfung, auf die sie oder er schlecht vorbereitet ist, auf die gleiche Art und Weise stört, um so eine Prüfungswiederholung zu erzwingen.

Abschließend möchten wir darauf hinweisen, dass unserer Ansicht nach in der Diskussion um den

Einsatz der sogenannten Detektoren ein wichtiger Aspekt unbeachtet bleibt: Um ein drahtlos arbeitendes Kommunikationsgerät für einen Täuschungsversuch benutzen zu können, müssen damit Daten übermittelt und/oder wenigstens entgegengenommen werden. Dazu muss beispielsweise ein Display abgelesen werden, es muss gesprochen werden, wenigstens müssen Zahlen/Buchstaben eingegebenen werden und selbst rein bildliche Verfahren (Fragefoto hin/Antwortfoto zurück) verlangen von der Schülerin/dem Schüler die gleiche oder sogar mehr Aufmerksamkeit als der Gebrauch eines Spickzettels. Ein Betrugsversuch über Handy/Smartphone oder ähnliche Geräte dürfte mindestens so gut zu erkennen sein wie das Ablesen eines „Spickers“ oder der mündliche "Datenaustausch" mit dem Nachbarn/der Nachbarin.

Aus technischer Sicht und auf Basis der uns zur Verfügung stehenden Informationen sprechen wir uns klar gegen den Änderungsantrag der CDU und für den Antrag der Fraktion der PIRATEN aus.

Autoren:
Daniel Ehlers, Informatiker, Vereinsvorstandsvorsitzender
Benny Baumann, Software-Entwickler, IT-Sicherheitsexperte
Dieter Hoogestraat, Journalist , Vorstandsmitglied
Frank Bartels, Informatiker, Vereinsvorstandsvorsitzender

Für den Verein Toppoint

Frank Bartels
Vereinsvorstandsvorsitzender