LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/3118**

10.07.2018

Antwort

der Landesregierung

auf die Kleine Anfrage 1119 vom 11. Juni 2018
des Abgeordneten Matthi Bolte-Richter BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/2808

Wird die Fußball-WM zum Einfallstor für Smart-TV-Hacker?

Vorbemerkung der Kleinen Anfrage

Am 14. Juni 2018 beginnt die Fußball-WM in Russland. Wie immer bei derlei öffentlichen Großereignissen erwartet der Handel laut Medienberichten bis dahin einen erhöhten Verkauf von Fernsehern der neuesten Generation. In diesem Jahr stehen dabei besonders die sogenannten Smart-TV im Blick.

Doch genau wie bei allen anderen digitalen Endgeräten bestehen bei Smart-TV Risiken mit Blick auf Datenschutz und Datensicherheit. So warnt das Bundesamt für die Sicherheit in der Informationstechnik schon seit geraumer Zeit:

„Schadprogramme und andere Sicherheitsprobleme können zum Beispiel über den Browser oder über die Installation von Apps auf das Gerät gelangen. Ein noch höheres Risiko besteht in der Datenspionage. Einerseits sind in den Kundenkonten von Pay-TV-Angeboten Zahlungsdaten hinterlegt, die für Cyberkriminelle immer anziehend sind. Andererseits ist es über das Smart-TV auch möglich, weitere persönliche Informationen auszuspähen. Dazu gehört vor allem das detaillierte Fernsehverhalten des Nutzers. Aber auch die in vielen Modellen integrierte Webcam oder Spracheingabe könnte missbraucht werden, um Menschen im Wohnzimmer akustisch oder visuell auszuspionieren.“[1]

[1] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Fussball-EM-SmartTV.html

Datum des Originals: 10.07.2018/Ausgegeben: 13.07.2018

Der Minister für Wirtschaft, Innovation, Digitalisierung und Energie hat die Kleine Anfrage 1119 mit Schreiben vom 10. Juni 2018 namens der Landesregierung im Einvernehmen mit dem Ministerpräsidenten, dem Minister des Innern und der Ministerin für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz beantwortet.

1. Wie hat sich die Zahl der Haushalte mit Smart-TV in Nordrhein-Westfalen in den letzten fünf Jahren entwickelt?

Laut der Erhebungen, die für die Digitalisierungsberichte der Landesmedienanstalten durchgeführt wurden, hat sich die Zahl der TV-Haushalte in Nordrhein-Westfalen, die über ein Smart-TV-Gerät verfügen, folgendermaßen entwickelt:
2013: 13,7 % (Basis 8,283 Mio. TV-Haushalte),
2014: 15,8 % (Basis 8,385 Mio. TV-Haushalte),
2015: 19,6 % (Basis 8,42 Mio. TV-Haushalte),
2016: 26,3 % (Basis 8,247 Mio. TV-Haushalte),
2017: 33,0 % (Basis 8,285 Mio. TV-Haushalte).

2. Wie bewertet die Landesregierung insgesamt die Risiken, die mit der Nutzung von Smart-TV einhergehen, insbesondere mit Blick auf die Datensicherheit, die Ausnutzung bestehender Sicherheitslücken durch Hackerangriffe und den verbreiteten Einsatz von Smart-TV auch in Firmennetzwerken?

Da es sich bei Smart-TV um Geräte mit eingebauten Rechnern handelt, sind diese so zu konfigurieren, dass Risiken reduziert oder ausgeschaltet sind. Ist das nicht sicher möglich, sind diese Geräte in Netzen zu betreiben, die separiert von sensiblen Systemen sind. Die Landesregierung schließt sich hier den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik BSI an:

Hinweise zu Smart-TV:
https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartTV/SmartTV_node.html

Artikel zur Europameisterschaft 2016: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Fussball-EM-SmartTV.html

3. Welche konkreten Maßnahmen unternimmt die Landesregierung für die Steigerung der IT-Sicherheit mit Blick auf Smart-TV einerseits hinsichtlich der Hersteller und Händler und ihrer Verantwortung, die IT-Sicherheit bereits bei der Entwicklung und der Inbetriebnahme der Geräte mitzudenken, andererseits aber auch hinsichtlich der Verbraucherinnen und Verbraucher, die Sicherheitsrisiken auch in ihrem Verantwortungsbereich minimieren sollten?

4. Welchen rechtlichen Anpassungsbedarf auf Landes-, Bundes- und Europaebene sieht die Landesregierung?

Die Fragen 3 und 4 werden zusammenfassend beantwortet.

Die Landesregierung sieht die Hersteller in der Verantwortung, Aspekte des Datenschutzes und der IT-Sicherheit von Anfang an bei der Entwicklung neuer Produkte und Dienste einzubeziehen.

Auf der 14. Verbraucherschutzministerkonferenz am 15. Juni 2018 hat das nordrhein-westfälische Verbraucherschutzministerium den gesetzlichen Handlungsbedarf zur Verbesserung der IT-Sicherheit bei vernetzten bzw. digitalen Verbraucherprodukten festgestellt und sich für die Einführung einer Haftung der Hersteller für nach dem Kauf eintretende oder bekanntwerdende IT-Sicherheitslücken ausgesprochen. Sicherheit-Updates sind den Verbraucherinnen und Verbrauchern über eine transparente Mindestfrist, die die erwartete Lebensdauer eines Produkts berücksichtigt, zeitnah und kostenfrei bereitzustellen. Der Bund wird gebeten, sich auch auf europäischer Ebene hierfür einzusetzen und die Entwicklung verbindlicher Mindeststandards zur IT-Sicherheit voranzutreiben.

Das Thema „digitale Souveränität“ nimmt einen hohen Stellenwert in der Verbraucherbildung und Verbraucherinformation in Nordrhein-Westfalen ein. Die Landesregierung möchte die Verbraucherinnen und Verbraucher motivieren und befähigen, sich mit den Chancen und Risiken der zunehmenden Digitalisierung im Verbraucheralltag selbstbewusst und verantwortlich auseinanderzusetzen. Dazu zählt ein souveräner und sorgsamer Umgang mit den eigenen persönlichen Daten.

Das Für und Wider intelligenter und vernetzter Haustechnik („Smart Home“) stand am 25.6.2018 im Mittelpunkt eines verbraucherpolitischen Dialogs des Verbraucherschutzministeriums in Düsseldorf, an dem Anbieter, Verbraucher- und Datenschützer sowie Vertreter aus Forschung und Wissenschaft teilgenommen haben.

5. Welche – aktuellen und vergangenen – Fälle von Sicherheitslücken bei Smart-TV – auch im Hinblick auf den Datenaustausch zwischen TV-Gerät und Hersteller bzw. Drittanbieter – sind der Landesregierung bekannt? (Bitte einzeln nach Herstellern auflisten)

In 2017 hat das CERT NRW eine Handreichung für die Landesverwaltung erarbeitet, die sich mit Gefahren von Smart-TV befasst. Diese ist als Anlage beigefügt.
Der Landesregierung liegen keine weiteren Informationen vor.

Gefahren beim Einsatz von Smart-TVs[1] im behördlichen Umfeld

[1] Fernsehgeräte mit Computer- und Netzwerkfunktionen

Die meisten aktuellen TV-Modelle bieten dem Benutzer neben der Hauptfunktion der Fernsehprogrammdarstellung weitere Zusatzfunktionen an: So können z.B. Mediendateien abgespielt, Webinhalte dargestellt, Sendungen gespeichert oder Zusatzinformationen in das laufende Programm eingeblendet werden.

Diese Fernseher sind mittlerweile längst normale Computer mit speziellem Anwendungszweck, so dass für diese Geräte Sicherheitsrichtlinien anzuwenden sind, die zumindest zum Teil denen aus anderen Bereichen der Informationstechnik entsprechen.

Insbesondere bei den Modellen, die Videokonferenzmöglichkeiten (z.B. via Skype) bieten ist besondere Vorsicht geboten, da diese über fest eingebaute Kameras und Mikrofone verfügen und dies gerade dann ein Problem sein kann, wenn sie in Besprechungsräumen oder Dienstzimmern aufgestellt sind, in denen vertrauliche Gespräche geführt werden. Kameras und Mikros sollten idealerweise abgeklebt werden.

Ein weiteres Problem, das sich bei normalen Computern so nicht stellt, ist dass die Hersteller ihre Plattformen gegenüber den Anwendern absichern wollen, so dass durch den Anwender keine Veränderungen an der Software vorgenommen werden können. Dies ist meist durch ein Programm realisiert, das den Inhalt der Festplatte auf Änderungen überprüft und das Gerät nicht mehr starten lässt, sollten Änderungen festgestellt werden. Ein simples Einspielen von Patches wird dadurch erschwert und die meisten Hersteller vermitteln auch dadurch den Eindruck, der Informationssicherheit keinen oder nur einen geringen Stellenwert einzuräumen, was dazu führt, dass Schwachstellen lange Zeit oder dauerhaft ausnutzbar bleiben.

Wie bei den meisten „Internet of Things“ Geräten üblich existiert auf den Geräten meist nur ein Benutzer, unter dessen Kennung alle Dienste gestartet wurden, so dass die Übernahme eines Systemteils durch einen Schadcode zur vollständigen Systemkontrolle durch die Schadsoftware führt. Getätigte Sicherheitseinstellungen, wie die Abschaltung von Bluetooth oder das softwareseitige Deaktivieren der Kamera und des Mikrofons können dann durch die Schadsoftware wieder rückgängig gemacht werden.

Alle obigen Punkte zusammengenommen führen zu dem Schluss, dass das Hauptaugenmerk darauf liegen sollte, Schadcode gar nicht erst auf das System kommen zu lassen, was sich als schwierig darstellt, da auf diesen Geräten in der Regel keine Virenschutzsoftware zum Einsatz kommt und die möglichen Zugänge zahlreich sind:

- TCP/IP basierte Ethernet Netzwerke (kabelgebunden und drahtlos)
- Bluetooth
- ZigBee
- USB-Datenträger
- HDMI-Schnittstellen
- CI/CI+ Module
- der Infrarotempfänger der Fernbedienung
- das digitale Fernsehsignal selbst (DVB-T/C/S)

Die Geräte sollten daher insbesondere nicht mit dem Behördennetz verbunden sein, da dies einem Angreifer einen dezentralen Zugang zum Behördennetz und damit zu weiteren Systemen ermöglicht und der Aufbau eines Rückkanals zum Datenabfluss leicht zu realisieren ist.

Funkprotokolle wie 802.11 (WLAN), Bluetooth und ZigBee sollten durch die Geräteeinstellung im Menü der Geräte unterbunden werden, was eine Schadsoftware jedoch übergehen könnte. Im besten Fall sollten die Geräte gar nicht über die genannten Hardwarekomponenten verfügen. USB-Datenträger sollten nur aus vertrauenswürdiger Quelle entgegengenommen werden und an die HDMI-Schnittstellen sollte nur dienstliche Hardware angeschlossen werden (u.a. das CEC-Protokoll kann hier problematisch werden und sollte in den Einstellungen deaktiviert werden). Für sogenannte Common-Interface-Module, die tiefe Eingriffe in die SmartTVs haben können, gilt Ähnliches wie für die vorgenannten Punkte: auch hier sollte eine Manipulation weitestgehend ausgeschlossen werden. Angriffe über den Infrarotempfänger wurden bisher nicht bekannt gemacht, sind jedoch theoretisch machbar. Ein möglicher Weg sich gegen diese zu verteidigen wäre es, den Empfänger abzukleben und die Bedienung nur am Gerät selbst durchzuführen.

Ein relativ neuer Angriffsweg ist die Unterbringung des Schadcodes im TV-Signal (z.B. DVB-T). Hierbei werden Auswertemechanismen angegriffen, die auf Zusatzdaten aus dem TV-Signal zurückgreifen, beispielsweise kann über einen manipulierten hbbTV Datenstrom der darstellende Webbrowser angegriffen, und für Codeausführungszwecke missbraucht werden. Betroffen von diesem Angriffsvektor sind DVB-T, DVB-C und DVB-S. Auf Zusatzfunktionen wie hbbTV, EPG und Ähnliche sollte daher verzichtet werden.

Kabelgebundene oder drahtlose Netzwerke wie WLAN, Bluetooth, ZigBee oder HDMI lassen sich einfach für einen Datenabfluss nutzen. Auf derartige Verbindungen sollte, soweit möglich, verzichtet werden. Ebenso ist davon abzuraten, fremde USB-Datenträger am Gerät zu betreiben. Bei einer DVB-C Verbindung lässt sich möglicherweise der Rückkanal nutzen, so dass hier DVB-T und DVB-S vorzuziehen sind.

Ist ein Schadcode bereits auf dem Smart-TV, so lässt sich noch ein weiterer Weg des Datenabflusses nutzen. Da der Schadcode alle Systemfunktionen beeinflussen kann, ist es ihm auch möglich einen Smart-TV ein- und auszuschalten, sofern sich dieses im Standbymodus befindet. So könnte von einem benachbarten Gebäude das entstehende Licht erkannt werden, das sich bei einem eingeschalteten Fernseher ergibt und so ein unidirektionaler (durch Zuhilfenahme des Infrarotempfängers sogar ein bidirektionaler), bitweiser Kommunikationskanal aufbauen. Zur Vermeidung ist es sinnvoll, den Fernseher bei Nichtbenutzung vom Stromnetz zu trennen, z.B. durch eine mechanisch schaltbare Steckdose.