

Datensicherheit im Internet & Spielen

28.06.2019

Aktuelle Nachrichten

- Innenminister wollen Daten von KI's wie Alexa, Siri und Ähnliche auswerten. Das betrifft nicht nur Handy's, oder kleine Geräte wie bei Alexa, sondern Fernseher, Kühlschränke und Sprachassistenten.

Quelle:

<https://www.spiegel.de/netzwelt/netzpolitik/innenminister-wollen-offenbar-daten-von-alexa-siri-und-co-auswerten-a-1270870.html>

- Bundestagspräsident Wolfgang Schäuble und Manfred Weber (Spitzenkandidat der EVP) wollen eine Klarnamenpflicht.

Quelle:

<https://www.spiegel.de/netzwelt/netzpolitik/klarnamenpflicht-im-internet-warum-anonymitaet-im-netz-so-wichtig-ist-a-1268306.html>

Aktuelle Nachrichten

- Bundesinnenminister Horst Seehofer will die Verschlüsselungen durch Anbieter wie Whatsapp u.Ä. auf richterliche Anordnung aufheben lassen.

Quelle:

<https://www.spiegel.de/netzwelt/netzpolitik/horst-seehofer-will-messengerdienste-zum-entschluesseln-zwingen-a-1269121.html>

Wer spielt welche Spiele?

1. On-/Offline-Spiele
2. Plattformen wie Steam u.Ä.
3. Browserbasierte Spiele
4. Mobilegames
5. Personenbezogene Daten
6. Spiele-Piraterie
7. Faustregeln

1. Gefahren in On- und Offline-Spielen

- Über Modifikationen und Addons, kann vieles heruntergeladen werden - einschließlich Malware! Bilder zu den Addons oder Mods, sagen nichts darüber aus, was wirklich drin ist!
- Private Server bieten beliebte Spiele an, die i.d.R. mit monatlichen Kosten verbunden sind. Aber: Auch hier kann niemals sicher sein, ob bei der Installation / Patches durch den privaten Anbieter, nicht mehr installiert wird, als gewünscht.
- Malware kann auch über die Entwickler selbst eingeschleust werden, wenn die verwendeten Tools bereits infiziert sind!
<https://www.spiegel.de/netzwelt/games/spieleentwickler-vertreiben-versehentlich-infizierte-spiele-a-1264181.html>

Plattformen wie Steam u.Ä.

- Auch über Plattformen wie Steam, kann Malware verbreitet werden. In bekannten Fällen über die Chatfunktion:
<https://www.pcgames.de/Steam-Software-69900/News/hacker-betrueger-account-malware-video-link-valve-1209954/>

3. Browserbasierte Spiele

Auch in Browserbasierten Spielen kann Malware verbreitet werden.
Hier in der Regel durch Buttons: <http://www.was-ist-malware.de/it-sicherheit/sicherheit-online-games/>

4. Mobile Games

Handys sammeln wahnsinnig viele Infos über uns: Wo du häufig bist, wo du warst, deine Kontakte, deine Kalendereinträge u.v.m. Mit mehreren Standorten, lassen sich sogar Bewegungsmuster erkennen! Mobilegames können dabei ein Einfallstor für Schadsoftware sein: <https://www.netzwelt.de/news/170032-malware-ueber-200-android-apps-habt-spiele-installiert.html>

5. Personenbezogene Daten

Es gibt Daten, die alle Arten von Spielen sammeln können, und das auch machen! - Standort. - Welches Gerät verwendet wird - mit welcher Konfiguration. - ...

6. Spiele-Piraterie

Mal davon abgesehen, dass es echt uncool ist, eine Dienstleistung in Anspruch zu nehmen, ohne dafür den angemessenen Preis zu zahlen, können Raubkopien von Spielen auch Malware einschleusen:
<https://www.kaspersky.de/blog/malware-in-pirated-games/18563/>

7. Zum Abschluss noch einige Faustregeln

- [1.] Anti-Viren-Programme (AVP) immer verwenden.
- [2.] Falls das AVP ausschlägt, immer das warum hinterfragen, nichts einfach blind zulassen.
- [3.] Backups sind niemals eine schlechte Idee. Selbst wenn alle deine Daten verschlüsselt wurden, kannst du den PC neu aufsetzen, und mit dem Backup alles wiederherstellen.
- [4.] Öffne keine Links in Emails, wenn du den Absender nicht zu 100 Prozent zuordnen kannst!
- [5.] Makros sind ein beliebtes Einfallstool für Malware (siehe z.B. Emotet, Heise). Wenn du aufgefordert wirst, Makros zu aktivieren, lass lieber die Finger davon.