

Richtlinien für mehr IT-Sicherheit in Autos

[Originalartikel](#)

[Backup](#)

<html> <div class=„meldung_wrapper druckversion“>

```

        <!-- RSPEAK_STOP -->
        <!-- RSPEAK_STOP -->
        <figure class="aufmacherbild"><figcaption><p class="source">(Bild:&#160;<a
href="http://www.automotiveisac.com/assets/img/executive-summary.pdf"
target="_blank" rel="external">Automotive Cybersecurity Best Practices -
Executive Summary (PDF)</a> )</p>
        </figcaption></figure><!-- RSPEAK_START --><!-- RSPEAK_START --><p
class="meldung_anrisstext"><strong>Die fortschreitende Vernetzung von Autos
erfordert neue Denkweisen bei deren Produktion . Ein neuer Leitfaden der US-
Automobilindustrie dokumentiert bew&#228;hrte Methoden im Umgang mit "Cyber
Security" in Fahrzeugen.</strong></p>
        <p>Der US-Industrieverband f&#252;r Sicherheit in der
Automobiltechnik <b>Auto ISAC [1]</b> hat ein "Best Practices"-Handbuch
herausgegeben, das Automobilherstellern und ihren Zulieferern bei der
<b>Erh&#246;hung der IT-Sicherheit in Fahrzeugen [2]</b> helfen soll.</p>

```

<p>Das Handbuch behandelt organisatorische und technische Aspekte der Fahrzeugproduktion in puncto Sicherheit, zum Beispiel Risikomanagement, Gefahrenerkennung und -behebung, Ausbildung von Mitarbeitern, Security by design, Zusammenarbeit mit Dritten und einiges mehr. Vom Handbuch steht derzeit nur eine Zusammenfassung als PDF zum Download bereit, die sich im Wesentlichen an Entscheider in Unternehmen sowie an Endkunden richtet. Laut FAQ [3] erhalten nur Auto-ISAC-Mitglieder Zugriff auf den detaillierten Best Practices Guide.</p> <h3

class=„subheading“>Muss sein</h3> <p>Die fortschreitende Vernetzung von Autos mit der Außenwelt und die zunehmende Digitalisierung der Steuerungssysteme in Fahrzeugen machen derlei Handeln dringend nötig, wie etwa der Hack des Jeep Cherokee [4] im vergangenen Jahr verdeutlicht.</p> <p>Auto ISAC ist vor rund einem Jahr aus der Alliance of Automobile Manufacturers [5] hervorgegangen. Zu dem Verband gehören unter anderem Ford, GM, Mercedes Benz und BMW. Ursprünglich wollte der Verband nur die Kommunikation zwischen den Automobilherstellern verbessern, bezieht nun aber auch die Zulieferer sowie Telekommunikationsanbieter mit ein.<!-- AUTHOR-DATA-MARKER-BEGIN -->

<!-- RSPEAK_STOP --> (ola [6]) <br class=„clear“/><!-- RSPEAK_START --><!-- AUTHOR-DATA-MARKER-END --></p>

```

        </div><hr/><p class="size80">
        <strong>URL dieses Artikels:</strong><br/>
https://www.heise.de/newsticker/meldung/Richtlinien-fuer-mehr-IT-Sicherheit-
in-Autos-3277252.html
        </p>
        <p class="size80">

```

Links in diesem Artikel:
[1] <http://www.automotiveisac.com/>
[2] <http://www.automotiveisac.com/best-practices/>
[3] <http://www.automotiveisac.com/faq.php>
[4] <http://heise.de/-2854127>
[5] <http://www.autoalliance.org/>
[6] <mailto:ola@ct.de>

</html>

From:
<https://schnipsel.qgelm.de/> - Qgelm

Permanent link:
<https://schnipsel.qgelm.de/doku.php?id=wallabag:richtlinien-fr-mehr-it-sicherheit-in-autos>

Last update: **2021/12/06 15:24**

