



LANDTAG  
Rheinland-Pfalz

18/3804

VORLAGE

Ministerium für Arbeit, Soziales, Transformation und Digitalisierung  
Postfach 31 80 | 55021 Mainz

Vorsitzender des  
Ausschusses Digitalisierung, digitale Infrastruk-  
tur und Medien  
Herrn Alexander Fuhr, MdL  
Landtag Rheinland-Pfalz  
55116 Mainz

DER MINISTER

Bauhofstraße 9  
55116 Mainz  
Telefon 06131 16-0  
Telefax 06131 16-2452  
Mail: [poststelle@mastd.rlp.de](mailto:poststelle@mastd.rlp.de)  
[www.mastd.rlp.de](http://www.mastd.rlp.de)

23. April 2023

<b>Mein Aktenzeichen</b> PuK	<b>Ihr Schreiben vom</b>	<b>Ansprechpartner/-in / E-Mail</b> Dagmar Rhein-Schwabenbauer <a href="mailto:Rhein-Schwabenbauer@mastd.rlp.de">Rhein-Schwabenbauer@mastd.rlp.de</a>	<b>Telefon / Fax</b> 06131 16-2415
---------------------------------	--------------------------	---	---------------------------------------

## 17. Sitzung des Ausschusses für Digitalisierung, digitale Infrastruktur und Me- dien am 20. April 2023

hier: TOP 6

### **Cybersicherheit für kleine und mittelständische Betriebe Antrag der Fraktion der CDU, Vorlage 18/3593**

Sehr geehrter Herr Vorsitzender Fuhr,

in der 17. Sitzung des Ausschusses für Digitalisierung, digitale Infrastruktur und Medien am 20. April 2023 wurde der oben genannte Tagesordnungspunkt mit der Maßgabe der schriftlichen Berichterstattung für erledigt erklärt.

Ich berichte daher wie folgt:

Die Digitalisierung schreitet in großen Schritten voran und eröffnet auch für rheinland-pfälzische Unternehmen neue Möglichkeiten. Mit der Digitalisierung gehen jedoch auch Risiken einher, die mehr Maßnahmen im Bereich der Cybersicherheit erfordern. Die allgemeine IT-Bedrohungslage ist seit einigen Jahren bereits auf anhaltend hohem Niveau und hat sich durch den russischen Angriffskrieg auf die Ukraine nochmals abstrakt erhöht.

Auch die Landesregierung hat diese Problematik erkannt und unterstützt die rheinland-pfälzischen Unternehmen bei der Erhöhung ihrer Cybersicherheit.



Allerdings liegt die Verantwortung für die Cybersicherheit im Unternehmen bei der Unternehmensführung. Sie entscheidet über Art und Umfang der Digitalisierung und des Einsatzes von IT und damit auch über die Fragen der Cybersicherheit, die untrennbar damit verbunden sind.

Die NIS2-Richtlinie der Europäischen Union, die EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau, die seit kurzem verabschiedet wurde, verlangt von den Mitgliedsstaaten, die Verantwortlichkeiten verbindlich für Unternehmen ab 50 Mitarbeitenden zu regeln, die in den von der NIS2-Richtlinie umfassten Wirtschaftsbereichen tätig sind.

Im Prinzip wurde die in der Cybersicherheit geltende Leitlinie „Cybersicherheit ist Cheffinnen- beziehungsweise Chefsache!“ in Artikel 20 festgehalten.

Danach werden die Unternehmensführungen für die Cybersicherheit in ihrem Unternehmen verantwortlich und haftbar gemacht. Sie werden darüber hinaus verpflichtet, zukünftig selbst an Schulungen und Fortbildungen im Bereich Cybersicherheit teilzunehmen.

In Rheinland-Pfalz setzt sich die Landesregierung aktiv dafür ein, Unternehmen und insbesondere auch KMU, über die Gefahren durch Cyberkriminalität zu sensibilisieren und sie zu unterstützen.

Die Landesregierung rückt das Thema Cybersicherheit durch thematische Veranstaltungen gezielt in den Fokus der Unternehmen und stellt entsprechende Unterstützungsangebote vor. Exemplarisch wird auf die Veranstaltung „Industrie-Dialog am Nachmittag“ verwiesen, die insbesondere an kleinere und mittlere Unternehmen der Metall- und Elektroindustrie sowie des Maschinenbaus adressiert war und zuletzt im März 2023 erneut durchgeführt wurde.

Zusätzlich greift die Landesregierung das Thema Cybersicherheit in ihrer Netzwerkarbeit auf, beispielsweise im Zuge des Industrie-Newsletters oder des Wirtschaftsförderer-Newsletters. Durch weitere Maßnahmen, wie die Übernahme der Schirmherrschaft des Cybersicherheitskongresses des Bundesverbandes mittelständische Wirtschaft, wird die Reichweite der IT-Sicherheitsangebote der Landesregierung erhöht.



Das Land stellt zudem Beratungsangebote durch die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes sowie Beratungsangebote der Verfassungsschutzabteilung des Innenministeriums zur Verfügung. Verwiesen wird beispielsweise auf das neue Sicherheitsportal „Cyberschutz RLP“ des Verfassungsschutzes. Hier werden unter anderem Informationen zu Cyberbedrohungen sowie Tipps zu Erstmaßnahmen im Falle eines Cyberangriffs angeboten.

Das Bundesamt für Sicherheit in der Informationstechnik bietet ebenfalls viele Hinweise und Tipps zur Erhöhung der Informationssicherheit. Nennenswert ist beispielsweise vor allem der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik. Dieser bietet auch eine niederschwellige Möglichkeit zu einer ersten umfassenden Absicherung mit relativ geringem personellen und finanziellen Aufwand.

Zudem bietet das Bundesamt für Sicherheit in der Informationstechnik an, der „Allianz für Cyber-Sicherheit“ beizutreten. Diese Allianz wurde mit dem Ziel gegründet, die Cyber-Sicherheit am Wirtschaftsstandort Deutschland zu stärken. Es ist ein Netzwerk von Unternehmen, die sich bei Cybersicherheit gegenseitig unterstützen. Aktuell gehören bundesweit 6.897 Unternehmen und Institutionen der „Allianz für Cyber-Sicherheit“ an. Die Allianz steht jedem Unternehmen offen.

Die Landesregierung begleitet diese Angebote mit eigenen Beratungs- und Unterstützungsangeboten. Letztlich verbleibt die Verantwortung für die IT und damit auch für die Cybersicherheit aber bei den Unternehmen selbst.

Mit freundlichen Grüßen

Alexander Schweitzer