Berlin, 21.11.2023

Offener Brief an den IT-Planungsrat

Nehmen Sie den Beschluss zur Nicht-Umsetzung der NIS-2-Richtlinie zurück!

Der Bundesverband IT-Sicherheit e. V. (TeleTrusT) fordert den IT-Planungsrat auf, den Beschluss 2023/39 zurückzunehmen.

Im Beschluss 2023/39 hat der IT-Planungsrat die Länder und den Bund gebeten, den Anwendungsbereich der NIS-2-Richtlinie *nicht* auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene sowie Bildungseinrichtungen zu erstrecken. Das Gegenteil ist notwendig: zur Herstellung eines angemessenen IT-Sicherheitsniveaus in Deutschland ist es erforderlich und dringend geboten, insbesondere die Kommunen, aber auch die Bildungseinrichtungen gesetzlich auf IT-Sicherheit zu verpflichten und diese nicht pauschal aus dem Anwendungsbereich herauszulassen.

Zur Umsetzung der NIS-2-Richtlinie

An der Umsetzung der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148) der EU wird derzeit intensiv gearbeitet. Der vom Bundesministerium des Innern und für Heimat federführend entwickelte Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) befindet sich derzeit in der Ressortabstimmung. Nach zwei an die Öffentlichkeit gelangten Referentenentwürfen, einem nicht mit der Bundesregierung abgestimmten "Diskussionspapier" und dem anschließenden "Werkstattgespräch" des BMI mit den Verbänden ist deutlich geworden: die durch die NIS2-Richtlinie umzusetzenden Regelungen sind anspruchsvoll, aber für das Gemeinwohl, die Bürgerinnen und Bürger, die Unternehmen und auch Behörden und öffentlichen Stellen als wichtig und wesentlich erkannt. Die Anstrengungen, funktionierende Regeln auf Bundesebene zu definieren, wird von den unmittelbar und mittelbar Beteiligten mit großer Ernsthaftigkeit betrieben. Das tut auch nicht zuletzt Not, da die Umsetzungsfrist am 17.10.2024 endet.

Der Bund darf mit einem NIS2UmsuCG die Umsetzung der NIS-2-Richtlinie jedoch nur im Rahmen seiner Kompetenzen für den Bund regeln. Die europäischen Umsetzungsvorgaben gehen darüber allerdings hinaus und umfassen zum einen auch "Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene". Die Bundesländer haben also eigene IT-Sicherheitsgesetze zu schaffen respektive anzupassen.

Zum anderen bestimmt die NIS-2-Richtlinie, dass die Mitgliedstaaten die Anwendbarkeit für "Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene" sowie "Bildungseinrichtungen" vorsehen können. Die lokale Ebene sind in Deutschland die Kommunen. Ob die Kommunen und Bildungseinrichtungen gesetzlich auf IT-Sicherheit verpflichtet werden, liegt also im Ermessen der Mitgliedstaaten, hier der Bundesländer.

Der IT-Planungsrat veröffentlicht nun am 03.11.2023 den Beschluss 2023/39, in dem es unter anderem heißt:

"*2. Er [der IT-Planungsrat] nimmt den Sachstandsbericht der AG Informationssicherheit zur Kenntnis und bittet die Länder und den Bund, von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch zu machen."*

Diese ausdrückliche Bitte an Bund und Länder beinhaltet, die Kommunen und Bildungseinrichtungen vom Anwendungsbereich der NIS2-Richtlinie kategorisch auszunehmen. Würde dieser Bitte Folge geleistet, gäbe es auch in Zukunft keinen gesetzlichen Mindestanforderungen an die IT-Sicherheit für die genannten Bereiche. Und dies bei einer IT-Sicherheitslage, die noch zu keiner Zeit schlechter war als sie dieser Tage ist.

Deshalb fordert TeleTrusT den IT-Planungsrat auf, den Beschluss zurückzunehmen und zu Ziff. 2 des Beschlusses das Gegenteil zu beschließen. Das gemeinsame Ziel muss eine IT-Sicherheit auf bestmöglichem Niveau

sein. Dazu leisten IT-Sicherheitsgesetze einen wichtigen Beitrag. Der Anspruch muss sein, auf jeder staatlichen Ebene alles dafür zu tun, IT-Sicherheit bestmöglich zu planen und umzusetzen.

IT-Sicherheit lässt sich nur flächendeckend verbessern.

Ohne eine funktionierende IT-Sicherheit kann der Staat bei Erfüllung seiner Aufgaben seinen Schutzpflichten nicht nachkommen und gefährdet das notwendige Vertrauen für eine Digitalisierung aller Lebensbereiche nachhaltig. Der "Weg für eine effiziente, sicherere und gut vernetzte digitale Verwaltung in Deutschland" (gem. Selbstbeschreibung des IT-Planungsrats) wird so nicht geebnet.

Der Ausschluss aus dem Regelungsregime ignoriert auch die Signalwirkung auf Unternehmen und Gesellschaft. Wie vermieden werden soll, dass die vom künftigen Recht erfassten Unternehmen keine sachlich ungerechtfertigte Ungleichbehandlung erkennen, bleibt offen. Zumal sich die fatalen Folgen unzureichender digitaler Infrastruktur und fehlender IT-Sicherheitsmaßnahmen in den Kommunen aktuell besonders bemerkbar machen: eine Vielzahl von Cyberattacken führt gegenwärtig zu einem flächendeckenden Ausfall zahlreicher Bürgerämter, wodurch Bürger und Bürgerinnen über einen längeren Zeitraum Verwaltungsleistungen nicht in Anspruch nehmen können. Prognosen zeigen, dass Angriffe auf informationstechnische Systeme kommunaler Behörden in Zukunft weiter ansteigen werden. Auch Bildungseinrichtungen, wie Schulen oder Universitäten, sind vermehrt betroffen.

Im Bericht "Die Lage der IT-Sicherheit in Deutschland 2023" des BSI wird dazu festgestellt: "Kleine und mittlere Unternehmen (KMU) sowie besonders Kommunalverwaltungen und kommunale Betriebe wurden überproportional häufig angegriffen". "Im Berichtszeitraum wurden insgesamt 27 kommunale Verwaltungen und Betriebe als Opfer von Ransomware-Angriffen bekannt." Die betroffenen Kommunen hatten dabei knapp sechs Millionen Einwohnerinnen und Einwohner.

Die Gefahr eines weitreichenden Zusammenbruchs von Verwaltungs- und Bildungseinrichtungen ist evident, ebenso das damit einhergehende datenschutzrechtliche Risiko.

Der Beschluss des IT-Planungsrats ist kontraproduktiv.

Denn er negiert eine konstruktive Beteiligung an den Aufgaben und enthält zudem auch keinerlei Vorschläge, wie auf anderem Weg für IT-Sicherheit gesorgt werden solle.

Es ist wichtig, die offensichtlichen Handlungsnotwendigkeiten für eine gute IT-Sicherheit allseits zu erkennen und konsequent zu handeln. Wer eine Regulierung ablehnt, womöglich auch aus Gründen praktischer Umsetzungsschwierigkeiten, dem wird man schwerlich zutrauen, die IT-Sicherheit auch ohne eine solche Regulierung freiwillig umzusetzen.

Der Möglichkeit, Kommunen und Bildungseinrichtungen auf nationaler Ebene von den europarechtlichen Vorgaben freizuhalten, sollten Bund und Länder verantwortlich entgegentreten. Der IT-Planungsrat sollte hier als politisches Steuerungsgremium von Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung von Verwaltungsleistungen seiner Aufgabe gerecht werden.

Der Bundesverband IT-Sicherheit bietet seine Mitwirkung auf dem Weg zu mehr IT-Sicherheit auf allen Ebenen an und ist für Gespräche jederzeit offen.

Unterzeichner:

Vorstand und Geschäftsführung Bundesverband IT-Sicherheit e. V. (TeleTrusT)

- RA Karsten U. Bartels LL.M.
- Prof. Dr. Norbert Pohlmann
- Dr. André Kudra
- Dr. Holger Mühlbauer

Erstzeichner:

CISO Alliance e.V., Ron Kneffel, Vorstandsvorsitzender

Mitzeichner:

- Tomasz Lawicki, Leiter TeleTrusT-AK "Stand der Technik"
- RA Stephan Schmidt, TCI Rechtsanwälte Mainz
- Dr. Frank Schemmel
- G DATA CyberDefense AG
- Christian Schröder, DSK360 GmbH
- Yvonne Aurich
- Jürgen Mayershofer
- Patrick Schnell
- Ives Laaf
- Carsten Reffgen, Enterprise Open Systems GmbH
- Shieldmaiden Cybersecurity UG
- Tatjana Kiefer
- Stefan Sander, SDS Rechtsanwälte Sander Schöning PartG mbB
- HK2 Rechtsanwälte
- HK2 Comtection GmbH
- Patrick Schnell
- Dr. Mohamad Sbeiti, Ruhr Security GmbH
- Tobias Hess, DSGVO-Service
- Dr.-Ing. Stefan Pokorny, IT-Sicherheitsberater
- David Goebel, DaGo Consulting GmbH
- Hermes Könnecke
- Thomas Scholz
- Wolfgang Pinner
- Alexander Fuchs, NEXT GENERATION IT SOLUTIONS
- Max Imbiel, ahead Security
- Tilmann Dietrich
- Christian Leipold
- Steffen Hellinger
- Stefan Bergmann
- Robin Stieber
- Carsten Vossel
- networker NRW
- Florian Kaiser
- Patrick Grihn, nextindex GmbH & Co. KG
- Susanne Kersten
- Steffen Müller, Infosec.de
- Marc Lindike, 222 Degree Consulting GmbH
- Thomas Fauser, DMARC24
- Claus Hofmann
- Tobias Bergmann, Bergmann IT
- Christian Meyer
- Christian Kohl
- Regina Mühlich
- Tilo Schneider
- Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
- Katarina della Peruta, Informationssicherheitsbeauftragte Landratsamt Ebersberg
- Hermann Oehrle
- Christian Grimm
- Manfred vom Sondern
- Yannick Gries
- Mathis Greve
- Ari Albertini, FTAPI Software GmbH
- Dietmar Wyhs, SSH Germany
- Martin Pasch
- Carsten Pinnow, Herausgeber datensicherheit.de
- Dirk C. Pinnow, Herausgeber datensicherheit.de
- Pierre Gronau, Informationssicherheitsberater
- Dr. Johannes Loxen, SerNet GmbH
- Alexander Rabe, eco - Verband der Internetwirtschaft e.V.
- Philipp Trouillier

- Marc Dauenhauer, IT Management Consulting
- Dr. Robin Pohl, Organisations- und Prozessberatung
- Richard Peddi, CISO, SIGNATA Group
- Werner Spielhaupter
- Carsten Dingendahl, ndaal GmbH & Co. KG
- Stefan Depping, digit solutions GmbH
- Matthias Kirchhoff, digitronic computersysteme gmbh
- Stefan Cink, NoSpamProxy
- Oliver Pietsch, Staatlich geprüfter Techniker
- Claudia Stecken
- RA Kristian Borkert
- Stefanie Wachter
- Der Mittelstand. BVMW e.V.
- Ralf Kowalewski
- Sandra Wiesbeck, IT-Sicherheitscluster e.V. - im Namen aller Vorstände -
- Oliver Dehning

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www.teletrust.de