Stellungnahme

zur Überarbeitung der NIS-Richtlinie und dem IT-Sicherheitsgesetz 2.0

September 2020

DATEV eG ist das Softwarehaus und der IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren zumeist mittelständische Mandanten. Das Unternehmen zählt mit 8.000 Mitarbeitern zu den größten IT-Dienstleistern und Softwarehäusern in Deutschland und Europa.

Das Leistungsspektrum der DATEV reicht von mehr als 200 PC-Programmen über Cloud-Dienste wie Online-Anwendungen, Datenverarbeitung und -archivierung im Rechenzentrum bis hin zu Outsourcingleistungen sowie Sicherheitsdienstleistungen. Beratungsleistungen und Angebote zur Wissensvermittlung runden das Angebot ab.

Mit über 40.000 Mitgliedern unserer Genossenschaft erreichen wir über 2,5 Mio. KMU, deren Daten bei uns im Auftrag verarbeitet werden.

DATEV entwickelte sich konsequent zu einem international agierenden Dienstleister, der heute auch in weiteren EU-Staaten (Italien, Österreich, Tschechien, Polen, Slowakei, Ungarn und Spanien) unterstützt.

Die Stellungnahme der DATEV eG erfolgt ausschließlich aus dem Blickwinkel des Unternehmens als berufsständischer IT-Dienstleister, insofern wird sie unabhängig von Stellungnahmen berufsständischer Organisationen wie Kammern und Verbänden abgegeben.

EU-Transparenzregister-Nummer: 5027241291-41

Aufgrund der zunehmenden Herausforderungen für die IT-Sicherheit, die durch die Covid-19-Krise noch einmal verdeutlicht wurden, plant die EU-Kommission eine Überarbeitung der 2016 in Kraft getretenen *Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union* **(NIS-Richtlinie)**. Parallel hierzu laufen in Deutschland nun schon seit knapp zwei Jahren die Diskussionen um die Überarbeitung des *Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* **(IT-Sicherheitsgesetz)**.

Anlässlich des von der EU-Kommission angestoßenen Konsultationsprozesses möchte DATEV die Möglichkeit nutzen, Stellung zu nehmen. Da beide Gesetze sehr ähnliche Ziele verfolgen und auch in ihrer Umsetzung und Wirkung nicht voneinander getrennt betrachtet werden sollten, gehen wir in dieser Stellungnahme auf beide Initiativen ein.

IT-Sicherheit ist Teil der DNA der DATEV. Seit unserer Gründung vor über 50 Jahren zählen die Sicherheit und der Schutz der uns anvertrauten Daten zu unseren Kernkompetenzen. DATEV sorgt mit ihrem Rechenzentrum dafür, dass Unternehmen ihren Anforderungen bestmöglich und sicher gerecht werden können. IT-Sicherheit spielt hierbei eine entscheidende Rolle. Aus dieser Erfahrung heraus und als IT-Genossenschaft der Steuerberater, Wirtschaftsprüfer und Anwälte mit dem spezifischen Wissen über 2,5 Millionen kleine und mittelständische Unternehmen (KMU) in Deutschland wissen wir, dass IT-Sicherheit eine wesentliche und unverzichtbare Grundlage für eine erfolgreiche digitale Transformation darstellt und auch für die Akzeptanz ebendieser unverzichtbar ist. Dementsprechend unterstützen wir das Ziel der EU-Kommission und der Bundesregierung, die IT-Sicherheit weiter voranzutreiben.

In unseren Ausführungen möchten wir uns auf die folgenden Aspekte fokussieren:

Um den Herausforderungen der Cyber- und IT-Sicherheit gerecht zu werden, braucht es ein harmonisiertes europäisches Vorgehen.

Das Internet macht nicht an Grenzen halt, die Cyber- und IT-Sicherheit kann national nicht gewährleistet werden. Diese Umstände erfordern es, bei der Cyber- und IT-Sicherheit über nationale Grenzen hinauszugehen, um zielführende Ansätze zu entwickeln. Statt eines unilateralen deutschen Ansatzes befürworten wir ein **koordiniertes europäisches Vorgehen**. Die Überarbeitung der NIS-Richtlinie und das deutsche IT-Sicherheitsgesetz 2.0 müssen aufeinander abgestimmt und konsistent sein. Der aktuell absehbare parallele Gesetzgebungsprozess gefährdet dies. **Divergierende nationale und europäische Vorgaben** sowie ggf. daraus resultierende zeitlich eng aufeinander folgende Anpassungen machen das tagtägliche Geschäft der Unternehmen unnötig komplex und führen zu kostenrelevanten **Mehraufwänden**.

Es braucht klare Kriterien für das Identifizieren kritischer Infrastruktur sowie für das Meldeverfahren und einheitliche begriffliche Definitionen.

Die Mitgliedstaaten gehen bei der Definition sowie bei der Methodik zur Identifizierung kritischer Infrastruktur unterschiedlich vor. In vielen Fällen führt dies dazu, dass in den Mitgliedstaaten unterschiedliche Sektoren als kritische Infrastrukturen eingestuft werden und somit in den Anwendungsbereich der Gesetzgebung fallen. Diese **Fragmentierung** in der EU schafft ein unübersichtliches Umfeld für Unternehmen, die die Einhaltung gesetzlicher Vorgaben grenzüberschreitend gewährleisten müssen. Aus Gründen der Kohärenz ist ein **einheitliches europäisches Identifikationsmodell** wünschenswert.

Einheitliche Definitionen von Begrifflichkeiten sind ebenso nötig, um eine kohärente Umsetzung und Anwendung der Gesetze zu ermöglichen. Derzeit mangelt es hier an Klarheit. So weichen beispielsweise schon die Grundbegriffe wie Informationssystem und Sicherheit eines Informationssystems zwischen EU-Richtlinie und nationaler Umsetzung im BSIG (BSI-Gesetz) ab.

Außerdem müssen die Voraussetzungen der **Meldepflicht und das Meldeverfahren** bei erheblichen Störungen europaweit vereinheitlicht werden, um einerseits unnötigen und teuren Mehraufwand für Unternehmen zu vermeiden und andererseits vergleichbare Daten zu erhalten.

KMU brauchen bei der IT-Sicherheit Unterstützung und müssen sich auf einen klaren europäischen Rechtsrahmen verlassen können.

KMU sind durch die Komplexität und die schnelle Entwicklung im IT-Sektor im Allgemeinen und hinsichtlich der IT-Sicherheit im Speziellen oft überfordert. Sie verfügen nicht über die notwendigen

Ressourcen, um ihre individuelle Situation bei Rechtsunsicherheiten oder gar einem rechtlichen Flickenteppich beurteilen zu können. Deswegen ist ein **eindeutiger und europaweit konsistenter Rechtsrahmen** hinsichtlich der IT-Sicherheit insbesondere für KMU von hoher Bedeutung.

Bei der Formulierung von gesetzlichen Anforderungen an Unternehmen sollte immer die **Kritikalität der erbrachten Leistung/Tätigkeit im Vordergrund** stehen, nicht die Größe eines Unternehmens. Mitarbeiteranzahl oder Umsatzgrößen sind nicht geeignet, um den Kreis der Verpflichteten zu definieren.

Betroffene KMU dürfen jedoch bei der gesetzlichen Umsetzung und der Interpretation der Vorgaben nicht allein gelassen werden. Unabdingbar sind **klare, einfache und europaweit einheitliche Meldestrukturen**. Gerade bei Ereignissen, die mehrere Aspekte betreffen, wie beispielsweise ein Sicherheitsvorfall mit Datenschutzbezug, kann es nicht sein, dass erst nach Durchlaufen eines mehrstufigen Fragekatalogs klar ist, was und wo zu melden ist.

Idealerweise wird in den **gesetzlichen Vorgaben** auch die **notwendige Beratung der Unternehmen** durch staatliche Stellen in den Mitgliedstaaten geregelt. So wichtig auch eine **allgemeingültige Formulierung** von gesetzlichen Vorgaben in einer sich technisch schnell ändernden Umgebung ist, so wichtig ist es auch, die Umsetzung dieser Vorgaben durch **Beratung und Konkretisierung handhabbar** zu machen. Nur so kann die latente Verunsicherung, die allgemeine Formulierungen bei KMU regelmäßig erzeugen, behoben werden und die Zielsetzung einer echten Verbesserung der Cyber- und IT-Sicherheit erreicht werden.

Es braucht eine klare Trennung von Beratungs- und Kontrollinstanzen sowie zwischen Maßnahmen zur Erhöhung der IT-Sicherheit und zur Erhöhung der öffentlichen Sicherheit.

Grundlage einer produktiven Zusammenarbeit zwischen den für IT-Sicherheit zuständigen **Behörden**, in Deutschland z. B. das Bundesamt für Sicherheit in der Informationstechnik (BSI), mit **anderen Ministerien, Institutionen und der Wirtschaft** ist gegenseitiges **Vertrauen**. Unternehmen müssen sich darauf verlassen können, dass ihre konstruktive Mitarbeit an einem größtmöglichen IT-Sicherheitsniveau nicht an anderer Stelle für die Erreichung weiterer sicherheitspolitischer Ziele genutzt wird. Dieses Vertrauen kann hergestellt werden, wenn die für **IT-Sicherheit zuständigen Behörden** mit größtmöglicher **Unabhängigkeit** agieren. Es braucht unabhängige und organisatorisch getrennte Beratungs- und Kontrollinstanzen. Nur so kann gewährleistet werden, dass der vertrauensvolle Austausch mit den Beratungsinstanzen nicht zum Nachteil beim Vorgehen der Kontrollinstanzen ausgelegt wird. Jene Behörden, die für IT-Sicherheit zuständig sind, sollten daher nicht unter der Fachaufsicht von Ministerien stehen, die gleichzeitig öffentliche Sicherheit garantieren sollen. Das Modell der Datenschutzbeauftragten kann dabei als organisatorisches Vorbild dienen.

Dieser Aspekt sollte auch bei der weiteren Entwicklung der **Agentur der Europäischen Union für Cybersicherheit** (ENISA) berücksichtigt werden.

Darüber hinaus sollte vermieden werden, regulatorische Vorgaben zur (präventiven) Erhöhung der IT-Sicherheit mit jenen zu vermischen, die eher auf die strafrechtliche Verfolgung als Folge des Ausnutzens von Lücken im Bereich der IT-Sicherheit abzielen. Der Versuch, in einem regulatorischen Vorhaben gleichzeitig öffentliche Sicherheit und IT-Sicherheit zu erreichen und strafrechtliche Konsequenzen aufzuzeigen, macht die Zielsetzung einiger Punkte in den legislativen Vorhaben weniger nachvollziehbar. Wir regen daher an, **Maßnahmen zur Erhöhung** der **IT-Sicherheit** und zur Erhöhung der **öffentlichen Sicherheit** wie auch zur **strafrechtlichen Verfolgung von IT-Sicherheitsverstößen** jeweils in **getrennten** Vorhaben zu behandeln, um eine trennscharfe Diskussion der jeweiligen dahinterstehenden Ziele zu ermöglichen.

IT-sicherheitspolitische Regelungen müssen evidenzbasiert und die behördlichen Strukturen effizient sein.

Das **Einholen wissenschaftlicher Expertise** wie auch die Berücksichtigung von detailliertem **Feedback** aus betroffenen Teilen der **Wirtschaft und Zivilgesellschaft** sollte am Anfang eines jeden Gesetzgebungsprozesses stehen. Dies ermöglicht eine **zielgenauere Regulierung**. Gleichzeitig wird dadurch im Idealfall großes Vertrauen in vorgesehene Kompetenz- und Anforderungsausweitungen der Sicherheitsbehörden geschaffen, mindestens trägt es aber zur Vereinfachung und Versachlichung der Debatte bei.

Im Zusammenhang mit dem **IT-Sicherheitsgesetz 2.0** bedauern wir, dass die vorgesehene **Evaluierung** bis heute nicht durchgeführt wurde. Zwar soll diese Evaluierung noch stattfinden und in den Gesetzgebungsprozess des IT-Sicherheitsgesetzes 2.0 einfließen. Aus unserer Sicht erschwert dieser nachgelagerte Prozess jedoch eine saubere Analyse bestehender regulatorischer Lücken und das anschließende Schließen ebendieser.

Schließlich muss im Bereich der Cyber- und IT-Sicherheit die europäisch zu wenig koordinierte, aber auch in einzelnen Mitgliedstaaten, wie Deutschland, immer komplexer werdende behördliche **Cybersicherheitsarchitektur verschlankt** werden. Nur so können Doppelstrukturen vermieden und Lücken in der Architektur zweifelsfrei identifiziert werden, um sie im Anschluss evidenzbasiert auszubessern. Die Stiftung Neue Verantwortung zeigt in ihrer Studie anschaulich die herrschende Unübersichtlichkeit der Cybersicherheitsarchitektur in Deutschland und Europa auf.[1]

[1] Herpig, Sven & Beigel, Rebecca (2020), Akteure und Zuständigkeiten in der deutschen Cybersicherheitsarchitektur, Stiftung Neue Verantwortung, unter: https://www.stiftung-nv.de/sites/default/files/snv_papier_cybersicherheitsarchitektur_final.pdf (abgerufen am 04.09.2020).

Kontakt

Johannes Holtz (Policy Advisor)
DATEVBrusselsOffice@DATEV.DE