UP KRITIS

Stellungnahme zum vorliegenden* Referentenentwurf des UP-KRITIS Wirtschaftsbeirates

Dieses Dokument soll dazu dienen, den Wirtschaftsbeirat des UP KRITIS über die Sicht aller Sektoren/Branchen des UP KRITIS zu dem „Diskussionsentwurf“ eines IT-Sicherheitsgesetzes 2.0 zu informieren. Es ist das Ergebnis des sektorübergreifenden Themenarbeitskreises „Regulierung“ des UP KRITIS und aktualisiert hiermit die bereits übermittelte Stellungnahme zu einem 2. RefE vom 7.05.2020. Es soll dem Wirtschaftsbeirat, zur Wahrnehmung des UP KRITIS Mandates, als „Stütze“ bei möglichen Gesprächen mit Behördenvertretern dienen.

In diesem Dokument befinden sich keine Vorschläge für Neuformulierungen des Gesetzestextes. Aufgrund der sich abzeichnenden sehr kurzen Frist zur Stellungnahme wird auf konkrete Textvorschläge zur Anpassung des Gesetzentwurfs verzichtet.

Diese Stellungnahme ersetzt nicht die Beteiligung des UP KRITIS in der noch anstehenden offiziellen Verbändeanhörung. Der UP KRITIS hält sich eine weitere Äußerung in der Anhörung offen.

Inhalt:

Dieses Dokument ist TLP Green eingestuft und kann somit an alle Unternehmen und Behörden, die Teilnehmer des UP KRITIS sind, zu deren Verwendung weitergegeben werden.

*dem UP KRITIS liegt der „Diskussionsentwurf“ des IT-SIG 2.0 in der Fassung vom 01.12.2020 vor.

A. Kernaussagen:

1. **Von der Einholung der Garantieerklärung für kritische Komponenten, über deren Administration bis zu den potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Einbeziehung von Behörden bis hin zur Untersagung eines Komponenteneinsatzes, müssten Betreiber die Auswirkungen tragen. Das Vorgehen greift durch die Zwangsvorgaben auch in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen ein und führt ggf. zu Marktverzerrungen wegen Ungleichbehandlung. Die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ müssen zwingend festgelegt werden, um auf Betreiberseite Beschaffungsprozesse und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Informationssicherheit auch im Gefahrenfall zu ermöglichen. Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss ausgeschlossen werden (Bestandsschutz). Die angedachte Neuregelung birgt ansonsten die Gefahr die Informationssicherheit in Kritischen Infrastrukturen zu schwächen.**

2. **Es sind Prämissen für die Ausprägung von Systemen zur Angriffserkennung (Intrusion Detection) nach § 7b dargelegt. Allerdings ist die Heraustrennung von personenbezogenen Daten mit heutigen technischen Mitteln nicht angemessen leistbar. Das Vorhalten von für die Angriffserkennung und -nachverfolgung relevanten Daten über vier Jahre ist im Angesicht des erforderlichen Aufwands nicht verhältnismäßig (Archivierung und Speicherplatz). Wir schlagen eine Speicherzeit im Normalfall von mindestens drei Monaten und bei Verdacht auf einen Angriff von bis zu 12 Monaten vor, analog der Ausführungen in § 5a Absatz 2.**

   Eine Übergangsfrist von mindestens zwei Jahren ist für die grundsätzliche Einführung von Systemen zur Angriffserkennung notwendig.

   Ein zielführender Einsatz von Systemen zur Angriffserkennung erfordert neben der Einführung von geeigneter Hard- und Software den Aufbau entsprechender Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse im Unternehmen. Diese Aufgaben werden üblicherweise durch sogenannte Security Operation Center (SOC) wahrgenommen. Hierbei handelt es sich faktisch um den Aufbau von hochspezialisierten Teams, die 24/7 tätig sind. Der finanzielle und personelle Aufwand, der mit der Forderung nach Systemen zur Angriffserkennung einhergeht, ist beträchtlich und für die allermeisten KRITIS-Betreiber nicht leistbar.

   Der Anspruch des Gesetzgebers an den Einsatz solcher Systeme muss daher auf IT-technische Eigenschaften im Sinne von Mindestanforderungen begrenzt sein.

3. **Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Das vorgeschlagene, abgestufte Sanktionsmaß erachten wir als grundsätzlich angemessen und sachgemäß. Der in den Bußgeldvorschriften neu eingeführte Verweis auf das Ordnungswidrigkeitengesetz, der zu einer Erhöhung um das 200-Fache des jetzigen Sanktionsmaßes von 100.000 € auf 20 Mio. € führen kann, muss gestrichen werden, da ein derart enormes Sanktionsmaß wiederum zu einer extremen Unverhältnismäßigkeit führt.**

4. **Der Erfüllungsaufwand für die Wirtschaft ist aus Sicht der Wirtschaft nicht nachvollziehbar beziffert. Er sollte gemäß der kürzlich durchgeführten Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen dargelegt werden. Des Weiteren liegen weiterhin keine Entlastungsmaßnahmen für die Wirtschaft vor.**

5. **„Unternehmen im besonderen öffentlichen Interesse“ sowie „erhebliche volkswirtschaftliche Schäden“ sind im Gesetzestext näher zu bestimmen, z.B. über einen direkten Verweis auf § 44 Absatz 1 GWB (sog. Hauptgutachten, siehe Begründung). Hierbei muss die Gleichbehandlung**

aller vom Gesetz betroffenen Unternehmen und die EU-Harmonisierung (keine Wettbewerbsnachteile) berücksichtigt werden. Wir weisen auf die Gefahr einer Doppelregulierung von Unternehmen der Sektoren der Kritischen Infrastrukturen hin, die über Tochtergesellschaften, die kritische Dienstleistungen erbringen, zusätzlich erfasst werden könnten. Doppelregulierungen müssen vermieden werden. Der UP KRITIS sollte zur Ausgestaltung der Rechtsverordnung nach § 10 Absatz 5 einbezogen werden.

6. **Da als Basis weiterhin das Funktionieren des Gemeinwesen und die Gefährdung der öffentlichen Sicherheit herangezogen wird, muss der Gesetzgeber die von Unternehmen in der Regel geschaffenen Rückfallebenen und die Zeiträume von Ausfällen und Störungen zwingend mit betrachten (siehe auch EU NIS-Richtlinie), um die Kritikalität von IT-Störungen angemessen einschätzen zu können. Nur erhebliche Störungen von informationstechnischen Systemen mit Bezug zur Versorgung der Allgemeinheit sind meldepflichtig. Dieser Ansatz fehlt weiterhin im vorliegenden Entwurf.**

7. **Die Informationspflichten des BSI an die Betreiber Kritischer Infrastrukturen wurden in § 4b konkretisiert. Die Weitergabe von Erkenntnissen über Schwachstellen, Sicherheitslücken und weiteren Sicherheitsrisiken sollte allerdings unverzüglich, verpflichtend und unabhängig von weiteren Sicherheitsinteressen durch das BSI erfolgen.**

8. **Bei der Detektion von Sicherheitsrisiken für die Netz- und Informationssicherheit eines Betreibers Kritischer Infrastruktur durch das Bundesamt nach § 7b muss sichergestellt werden, dass es bei reinen Portscans bleibt und nicht weitere invasive Maßnahmen die Netz- und Informationssicherheit von betroffenen Betreibern gefährden.**
   Beim Einsatz von Honeypots muss wiederum sichergestellt werden, dass Informationen, die durch Maßnahmen nach § 7b Absatz 1 sowie Meldungen nach § 8b Absätze 4 und 4a erlangt wurden, nicht in die Architektur dieser Honeypots Einfluss finden (kein Aufbau von „Trainingsplattformen“ für Angreifer mit Bezug zu Kritischen Infrastrukturen). Der Ausschluss der Durchführung weitergehender, invasiver Maßnahmen durch das Bundesamt ist sachgemäß und vertrauensbildend.

9. **Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen an IT-Produkte nach § 3 Absatz 1 Satz 2 Nummer 20 durch das Bundesamt darf nicht in einen nationalen Alleingang münden. Der Stand der Technik sollte wie bisher auf Basis anerkannter Normen und Standards ausgelegt werden, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschafsverbände beteiligt sind.**

10. **Es ist nicht nachvollziehbar, dass das Bundesinnenministerium – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Referentenentwurfs –die Durchführung der gesetzlich verankerten Pflicht zu Evaluierung des Gesetzes nicht plausibel dargelegt und erläutert hat. Die Bundesregierung sollte die bisher eingeführten Cyber- und IT-Sicherheitsmaßnahmen auf ihre Wirksamkeit überprüfen und darauf aufbauend transparent weiterentwickeln. Der UP KRITIS regt an, die Evaluierung unter Heranziehung eines wissenschaftlichen Sachverständigen und innerhalb der etablierten staatlich-wirtschaftlichen Zusammenarbeit vorzunehmen. Die formale Beteiligung der betroffenen Kreise darf nicht durch eine voreilige Einbringung des Gesetzentwurfs in das Bundeskabinett unterbleiben. Eine offizielle Verbändeanhörung bedarf einer ausreichenden Frist von mindestens zwei Wochen.**

B. Stellungnahmen:

1. **Kernaussage: Von der Einholung der Garantieerklärung für kritische Komponenten, über deren Administration bis zu den potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Einbeziehung von Behörden bis hin zur Untersagung eines Komponenteneinsatzes, müssten Betreiber die Auswirkungen tragen. Das Vorgehen greift durch die Zwangsvorgaben auch in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen ein und führt ggf. zu Marktverzerrungen wegen Bevorzugung/Benachteiligung. Die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ müssen zwingend festgelegt werden, um auf Betreiberseite Beschaffungsprozesse und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Informationssicherheit auch im Gefahrenfall zu ermöglichen. Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss ausgeschlossen werden (Bestandsschutz). Die angedachte Neuregelung birgt ansonsten die Gefahr, die Informationssicherheit in Kritischen Infrastrukturen zu schwächen.**

Bei der Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller sind gesetzlich weitere Maßnahmen vorzusehen, die für die Aufrechterhaltung der kritischen Geschäftsprozesse (trotz Untersagung) sorgen, realistische Übergangsfristen geben, die Pflicht zur Nennung von verfügbaren Austauschprodukten enthalten und eine langfristige Verhinderung der Monopolbildung für Produkte verhindern. Wir regen dringend an, diese Punkte bei der Gesetzgebung zu beachten.

Betreiber werden an Stelle des Gesetzgebers in die Pflicht genommen, beim Hersteller eine Garantieerklärung einzuholen, welche an das BMI gesendet werden soll. Die Verwaltung und Übermittlung von Garantieerklärungen stellen einen erheblichen Aufwand dar. Daraus ergibt sich kein Mehrwert für den effektiven Schutz Kritischer Infrastrukturen.

2. **Kernaussage: Es sind Prämissen für die Ausprägung von Systemen zur Angriffserkennung (Intrusion Prevention) nach § 8a Absatz 1a dargelegt. Allerdings ist das Vorhalten von für die Angriffserkennung und -nachverfolgung relevanten Daten über vier Jahr nach § 8a Absatz 1b im Angesicht des erforderlichen Aufwands nicht verhältnismäßig (Speicherplatz und Archivierung). Die Heraustrennung von personenbezogenen Daten mit heutigen technischen Mitteln ist nicht angemessen leistbar. Wir schlagen eine Speicherzeit im Normalfall von mindestens drei Monaten und bei Verdacht auf einen Angriff von bis zu 12 Monaten vor, analog der Ausführungen in § 5a Absatz 2.**

   Eine Übergangsfrist von mindestens zwei Jahren ist für die grundsätzliche Einführung von Systemen zur Angriffserkennung notwendig.

   Ein zielführender Einsatz von Systemen zur Angriffserkennung erfordert neben der Einführung von geeigneter Hard- und Software den Aufbau entsprechender Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse im Unternehmen. Diese Aufgaben werden üblicherweise durch sog. Security Operation Center (SOC) wahrgenommen. Hierbei handelt es sich faktisch um den Aufbau von hochspezialisierten Teams, die 24/7 tätig sind. Der finanzielle und personelle Aufwand, der mit der Forderung nach Systemen zur Angriffserkennung einhergeht, ist beträchtlich und für die allermeisten KRITIS-Betreiber nicht leistbar.

   Der Anspruch des Gesetzgebers an den Einsatz solcher Systeme muss auf IT-technische Eigenschaften im Sinne von Mindestanforderungen begrenzt sein.

Für den verpflichtenden Einsatz von Systemen zur Angriffserkennung nach §8a Absatz 1a sind aus Sicht des UP KRITIS Prämissen für die Ausprägung dargelegt.

Der Aufbau eines umfassenden Systems zur Angriffserkennung (Aufbau und Betrieb von Security Operation Center - SOC) kann jedoch je nach Komplexität des Netzwerks und der Art der Vernetzung (oder Trennung) zu erheblichem Aufwand, insbesondere bzgl. Personalkapazitäten und den Betrieb erforderlicher Prozesse und Verfahren zur Reaktion auf Alarme führen.

Der UP KRITIS gibt zu bedenken, dass des Weiteren aufgrund der oben genannten Herausforderungen (Zeit, Personal, Know-How, Technik) anzunehmen ist, dass die Mehrheit der KRITIS-Betreiber hierzu einen Managed Security Services beauftragt. Da somit Zugang von wenigen Providern auf eine hohe Anzahl von Kritischen Infrastrukturen aufgebaut wird, müssen Angreifer auch nur noch wenige Provider zum Ziel haben, um größtmöglichen sektorübergreifenden Schaden zu verursachen. Dem muss unbedingt entgegengewirkt werden.

Kritisch zu sehen ist jedoch die Trennung personenbezogener Daten von nicht personenbezogenen Daten, da dies technisch nicht im angemessenen Verhältnis leistbar ist. Die Forderung einer Vorhaltung von Protokollierungsdaten über 4 Jahre würde den Aufbau eines technisch komplexen Archivierungssystems erfordern. Die zu erwartenden Mengen an anfallenden Protokollierungsdaten können in den Angriffserkennungssystemen selbst technisch nicht vorgehalten werden.

Der UP KRITIS schlägt eine Reduzierung der Speicherpflicht im Normalfall von mindestens drei Monaten und bei Verdacht auf einen Angriff von bis zu 12 Monaten vor. Dies orientiert sich an der Pflicht des Bundesamts zur Verarbeitung und Speicherung von behördeninternen Protokollierungsdaten nach § 5a Absatz 2, die als angemessen angesehen wird.

Im Angesicht der administrativen und finanziellen Aufwände für Archivierung und Speicherplatz erscheinen die Fristen aus Sicht des UP KRITIS daher nicht als angemessen. Eine Übergangsfrist von mindestens zwei Jahren ist auf Grund der zeitlichen Vorgaben und Restriktionen bei der Beschaffung und Einführung von Komponenten sowie der Bereitstellung von qualifiziertem Personal für den Betrieb von Systemen zur Angriffserkennung notwendig.

3. **Kernaussage: Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Das vorgeschlagene, abgestufte Sanktionsmaß erachten wir als grundsätzlich angemessen und sachgemäß. Der in den Bußgeldvorschriften neu eingeführte Verweis auf das Ordnungswidrigkeitengesetz, der zu einer Erhöhung um das 200-Fache des jetzigen Sanktionsmaßes von 100.000 € auf 20 Mio. € führen kann, muss gestrichen werden, da ein derart enormes Sanktionsmaß wiederum zu einer extremen Unverhältnismäßigkeit führt.**

Es ist begrüßenswert, dass sich das Strafmaß an einem europäischen Bußgeldrahmen orientiert. Das vorgeschlagene, abgestufte Sanktionsmaß erachten wir als grundsätzlich angemessen und sachgemäß.

Der Verweis auf das Ordnungswidrigkeitengesetz für das Sanktionsmaß von 2 Mio. € bewirkt im Endeffekt ein Höchstmaß von 20 Mio. € bei Verstößen nach § 14 Absatz 2 Satz 1. Die Erhöhung des Höchstmaßes auf die Strafhöhe der Datenschutzgrundverordnung erscheint unverhältnismäßig, da es um Verstöße von Unternehmen gegen die Pflichten des IT-Sicherheitsgesetzes gilt und nicht um die Grundrechte von Bürgerinnen und Bürgern. Der UP KRITIS fordert die ersatzlose Streichung des Verweises auf das Gesetz über Ordnungswidrigkeiten.

Es ist ferner sicher zu stellen, dass es nicht zu einer Doppelregulierung /-bestrafung durch DSGVO und IT-SIG 2.0 kommen kann (sobald personenbezogene Daten betroffen sind).

4. **Der Erfüllungsaufwand für die Wirtschaft ist aus Sicht der Wirtschaft nicht nachvollziehbar beziffert. Er sollte gemäß der kürzlich durchgeführten Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen dargelegt werden. Des Weiteren liegen weiterhin keine Entlastungsmaßnahmen für die Wirtschaft vor.**

Neben drohenden Bußgeldern, soll es nach Schätzung der Behörden durch das geplante Regelungsvorhaben der Bundesregierung für die Wirtschaft zu einmaligen Personalkosten von knapp 70.000 Euro sowie zu einer Veränderung der jährlichen Sach- und Personalkosten von 9 Millionen Euro kommen. Die Angaben sind nicht nachvollziehbar, da bereits heute ein deutlich höherer Aufwand betrieben werden muss, um die Verwaltungsanforderungen aus dem IT-SiG 1.0 zu erfüllen. Soweit durch das Regelungsvorhaben für die Wirtschaft zusätzlicher laufender Erfüllungsaufwand entsteht, soll dieser durch geeignete Entlastungsmaßnahmen kompensiert werden.

Der Erfüllungsaufwand für die Wirtschaft sollte gemäß der kürzlich durchgeführten Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen beziffert werden. Des Weiteren liegen weiterhin keine Entlastungsmaßnahmen für die Wirtschaft vor.

Wir bitten um Vorlage von Erkenntnissen bezüglich der Erhebung des Statistischen Bundesamts in der Sache sowie um Benennung, welche Entlastungsmaßnahmen für die Wirtschaft vorgesehen sind und wann diese umgesetzt werden.

5. **Kernaussage: Unternehmen im besonderen öffentlichen Interesse“ sowie „erhebliche volkswirtschaftliche Schäden“ sind im Gesetzestext näher zu bestimmen, z.B. über einen direkten Verweis auf § 44 Absatz 1 GWB (sog. Hauptgutachten, siehe Begründung). Hierbei muss die Gleichbehandlung aller vom Gesetz betroffenen Unternehmen und die EU-Harmonisierung (keine Wettbewerbsnachteile) berücksichtigt werden. Wir weisen auf die Gefahr einer Doppelregulierung von Unternehmen der Sektoren der Kritischen Infrastrukturen hin, die über Tochtergesellschaften, die kritische Dienstleistungen erbringen, doppeltzusätzlich erfasst werden könnten. Doppelregulierungen müssen vermieden werden. Der UP KRITIS sollte zur Ausgestaltung der Rechtsverordnung nach § 10 Absatz 5 einbezogen werden.**

Eine Gleichbehandlung der Unternehmen ist nachvollziehbar sicherzustellen.

Um Wettbewerbsnachteile nationaler Unternehmen zu vermeiden, muss eine Harmonisierung mit der EU NIS-Richtlinie und der AEUV („AEUV fördert den Binnenmarkt, indem er alle Maßnahmen verbietet, die den freien Warenverkehr zwischen den Mitgliedstaaten behindern“) erfolgen.

Die Termini „Unternehmen im besonderen öffentlichen Interesse“ sowie „erhebliche volkswirtschaftliche Schäden“ sind näher zu bestimmen. Der Gesetzgeber sollte direkt im IT-Sicherheitsgesetz die Wesens-merkmale derartiger Infrastrukturen spezifizieren sowie inhaltlich von den Kritischen Intrastrukturen i.S.d. § 2 Abs. 10 BSIG abgrenzen und eine Risikoorientierung auf Basis von Sektorstudien, die mit den Branchenverbänden im jeweiligen Sektor abgestimmt sein müssen, als Grundlage heranziehen.

Betreiber, die durch die KritisV nicht erfasst sind (z.B. unter Schwellwerte), sollten nicht als „Unternehmen im besonderen öffentlichen Interesse“ erfasst und über diesen Weg dann reguliert werden.

6. **Kernaussage: Da als Basis weiterhin das Funktionieren des Gemeinwesen und die Gefährdung der öffentlichen Sicherheit herangezogen wird, muss der Gesetzgeber die von Unternehmen in der Regel geschaffenen Rückfallebenen und die Zeiträume von Ausfällen und Störungen zwingend mit betrachten (siehe auch EU NIS-Richtlinie), um die Kritikalität von IT-Störungen angemessen einschätzen zu können. Nur erhebliche Störungen von informationstechnischen Systemen mit Bezug**

zur Versorgung der Allgemeinheit sind meldepflichtig. Dieser Ansatz fehlt weiterhin im vorliegenden Entwurf.

7. **Kernaussage: Die Informationspflichten des BSI an die Betreiber Kritischer Infrastrukturen wurden in § 4b konkretisiert. Die Weitergabe von Erkenntnissen über Schwachstellen, Sicherheitslücken und weiteren Sicherheitsrisiken sollte allerdings unverzüglich, verpflichtend und unabhängig von weiteren Sicherheitsinteressen durch das BSI erfolgen.**

Wir begrüßen es, dass das BSI in die Lage versetzt werden soll, weiter ein bundesweites Lagebild zu erstellen und Betreiber über mögliche Risiken zu warnen. Dieses ist aber auch schon durch das IT-SIG 1.0 gegeben. Hier zusätzlich die Möglichkeit der Teilung von Erkenntnissen mit anderen Behörden einzuräumen (Erfüllungshilfe) entspricht nicht dem Sinne (Schutz Kritischer Infrastrukturen) dieses Gesetzes und ist zu überdenken.

Der UP KRITIS begrüßt grundsätzlich auch die in §4b konkretisierten Informationspflichten des BSI an die Betreiber. Sollte das BSI durch Meldungen von Betreibern, anderen nationalen CIRTs (EU NIS-Richtlinie) oder anderen Behörden (z.B. Verfassungsschutz) Erkenntnisse über Schwachstellen oder Bedrohungen gewinnen, muss es diese Erkenntnisse jedoch verpflichtend und unverzüglich den betroffenen Unternehmen zukommen lassen. Nur zügig geschlossene Schwachstellen stärken die Cyberresilienz Deutschlands. Dieser Aspekt ist in die Konkretisierung aufzunehmen und entsprechend auszugestalten.

8. **Kernaussage: Vor der Detektion von Sicherheitsrisiken für die Netz- und Informationssicherheit eines Betreibers Kritischer Infrastruktur durch das Bundesamt nach § 7b sollte eine Abstimmung mit dem betroffenen Betreiber unverzüglich und ohne Ausnahmen erfolgen.**
   Angriffssimulationen vom BSI auf Betreiber Kritischer Infrastrukturen können zu Systemabstürzen führen. Sie müssen auf Schwachstellendetektion eingeschränkt werden. Zudem muss die Haftung, für die durch Schwachstellenanalysen ggf. hervorgerufenen Schäden, geklärt werden. Beim Einsatz von Honeypots muss ausgeschlossen werden, dass Kennungen von informationstechnischen Systemen von Betreibern Kritischer Infrastruktur durch das Bundesamt genutzt werden. Der Ausschluss der Durchführung weitergehender, invasiver Maßnahmen durch das Bundesamt ist sachgemäß und vertrauensbildend.

Zukünftig soll das BSI Angriffssimulationen auf gesetzlicher Basis durchführen dürfen. Der reinen automatisierten Detektion von Sicherheitslücken in IT-Systemen, die aus dem Internet heraus erreichbar sind, spricht nichts entgegen. Schon heute werden tagtäglich sogenannte „Portscans“ millionenfach aus allen möglichen Quellen heraus vorgenommen.

Der Gesetzestext schränkt den Umfang der Angriffssimulation auf die Durchführung von „Portscans“ ein, d.h. weiterführende, invasive Maßnahmen wie „Penetrationsanalysen“ durch das Bundesamt sind gesetzlich ausgeschlossen.

Bei dem Einsatz von Systemen und Verfahren des BSI, welche einem Angreifer einen erfolgreichen Angriff vortäuschen (Honeypot, Artikel 1 § 7b (4) BSI-G) muss im Gesetz geregelt sein, dass der Einsatz von branchenspezifischen Lösungen (z.B. Produktionsanlagen, Industrielle Kontrollsysteme) mit den Betreibern abgestimmt sein muss, um hier keine „Lernplattform“ für Angreifer zu schaffen.

9. Kernaussage: Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen an IT-Produkte nach § 3 Absatz 1 Satz 2 Nummer 20 durch das Bundesamt darf nicht in einen nationalen Alleingang münden. Der Stand der Technik sollte wie bisher auf Basis anerkannter Normen und Standards ausgelegt werden, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschafsverbände beteiligt sind.

Betreiber Kritischer Infrastrukturen sind nach § 8a BSIG verpflichtet zur Umsetzung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik. Die Betreiber Kritischer Infrastrukturen sind daher als unmittelbar Betroffene bei der Entwicklung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte einzubeziehen, analog zu Beteiligungsmöglichkeiten in der nationalen, europäischen und internationalen Normung.

Der Stand der Technik entwickelt sich dynamisch weiter und wird durch etablierte Strukturen der nationalen, europäischen und internationalen Normung entwickelt. Betroffene und interessierte Kreise sind hieran beteiligt. Es darf keine Abkehr von diesen etablierten Verfahren insbesondere von branchenspezifischen Sicherheitsstandards (B3S) geben, die in einen nationalen Alleingang in der Sache münden würde. Zertifizierungen, die nach dem Stand der Technik anderer Organisationen bzw. Branchenverbänden für Informationssicherheit erfolgen, sind ebenfalls anzuerkennen. Ein Verbot von bereits im Einsatz befindlichen Komponenten muss vermieden werden.

Der UP KRITIS schlägt vor, den Passus dahingehend zu ergänzen, dass ein Stand der Technik unter Berücksichtigung von bestehenden, anerkannten Normen und Standards erfolgen muss unter Beteiligung der betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschaftsverbände.

10. Kernaussage: Es ist nicht nachvollziehbar, dass das Bundesinnenministerium – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Referentenentwurfs –die Durchführung der gesetzlich verankerten Pflicht zu Evaluierung des Gesetzes nicht plausibel dargelegt und erläutert hat. Die Bundesregierung sollte die bisher eingeführten Cyber- und IT-Sicherheitsmaßnahmen auf ihre Wirksamkeit überprüfen und darauf aufbauend transparent weiterentwickeln. Der UP KRITIS regt an, die Evaluierung unter Heranziehung eines wissenschaftlichen Sachverständigen und innerhalb der etablierten staatlich-wirtschaftlichen Zusammenarbeit vorzunehmen. Die formale Beteiligung der betroffenen Kreise darf nicht durch eine voreilige Einbringung des Gesetzentwurfs in das Bundeskabinett unterbleiben. Eine offizielle Verbändeanhörung bedarf einer ausreichenden Frist von mindestens zwei Wochen.

Generell erkennen die am UP KRITIS teilnehmenden Unternehmen nur ansatzweise, dass Erfahrungen aus der Umsetzung des IT-SiG 1.0 sowie Erkenntnisse und Rückmeldungen von KRITIS-Betreibern in die aktuelle Fassung des Referentenentwurfs eingeflossen sind. Es ist nicht nachvollziehbar, dass das Bundesinnenministerium – trotz des nunmehr zweijährigen Zeitraums zur Erarbeitung des vorliegenden Referentenentwurfs –der gesetzlich verankerten Pflicht zu Evaluierung des Gesetzes nicht nachgekommen zu sein scheint.

Der UP KRITIS empfiehlt, den vorliegenden Referentenentwurf so zu überarbeiten, dass Änderungen am IT-SiG nachvollziehbar aus den gewonnenen Erkenntnissen („Lessons Learned“) resultieren, die im Zuge der Evaluation gewonnen werden müssten.

<u>Die formale Beteiligung der betroffenen Kreise darf nicht durch eine voreilige Einbringung des Gesetzentwurfs in das Bundeskabinett unterbleiben. Eine offizielle Verbändeanhörung bedarf einer ausreichenden Frist von mindestens zwei Wochen.</u>

Der UP KRITIS sieht Wettbewerbsnachteile und Einschränkungen der unternehmerischen Freiheit der Betreiber und empfiehlt, dies aktiv abzuwenden. Wirtschafts- und geopolitische Interessen dürfen nicht auf dem Rücken der nationalen Betreiber ausgetragen werden.

Die zugrundeliegenden Abwägungen bedürfen generell einer nachvollziehbaren Erläuterung.

Weitreichende Datenschutz- und Geschäftsgeheimnisschutz-Aspekte im IT-SiG 2.0 verkomplizieren die zugrundeliegende Gesetzgebung (DSGVO, GeschGehG) und sollten daher in gesonderten Artikeln des IT-SiG 2.0 zusammengeführt und in den jeweils zugrundeliegenden Gesetzen vorgenommen werden (Änderung des Umsetzungsgesetzes der DSGVO sowie des GeschGehG, anstatt Änderungen an TKG, TMG, BSIG).

Mitglieder des Themenarbeitskreises (TAK) Regulierung und Ersteller_innen dieses Dokumentes

Vertreter_innen aus 8 Wirtschaftssektoren:
Finanz und Versicherungswesen, Transport und Verkehr, IT und TK, Wasser, Gesundheit, Energie (Strom/Gas/Fernwärme), Ernährung, Medien und Kultur

TAK Mitglied		Unternehmen
Albrecht	Frank	REWE Systems GmbH
Bleschke	Sebastian	Initiative Erdgasspeicher e.V.
Bendjebbour	Yassin	Bundesverband der Energie- und Wasserwirtschaft e.V. (Energie)
Berndt	Andreas	50 Hertz GmbH
Bott	Daniel	AXA
Dambach	Stephan	Stadtwerke Speyer GmbH
Ebner	Michael	EnBW Energie Baden-Württemberg AG
Freudensprung	Rolf	Deutsche Lufthansa AG
Heiko	Hußmann	Landeshauptstadt Hannover
Huber	Hermann	Hubert Burda Media Holding KG
Jensen	Ingo	Bayernwerk Netz GmbH
Jochem	Rainer	Saarländischer Rundfunk
Junker	Wolfgang	Südzucker
Jünger	Andreas	Berliner Verkehrsbetriebe AöR
Kaminski	Peter	Santander Consumer Bank AG
Kastl	Andreas	Verband der Auslandsbanken in Deutschland e.V.
Kibittel	Petra	MEDIA BROADCAST GmbH
Knosowski	Yvonne	Kreiskliniken Gummersbach-Waldbröl GmbH
Kopper	Christoph	Sparkasse Lörrach-Rheinfelden
Krauhausen	Thomas	innogy SE
Kršić	Boban	DENIC eG
Mizera	Sascha	Südzucker
Münster	Enno	Deutsche Lufthansa AG
Marcus	Popp	EDEKA
Nash	André	Bundesverband deutscher Banken e.V.
Prechtel	Andreas	Verband der Auslandsbanken in Deutschland e.V.
Sabet	Stefanie	Bundesvereinigung der Deutschen Ernährungsindustrie e.V.
Sachgau	Christian	Deutsche Telekom AG
Saxena	Sunita-Ute	T-Systems International GmbH
Schmitz	Michaela	Bundesverband der Energie- und Wasserwirtschaft e.V. (Wasser)
Schulte	Gisbert	Bochum-Gelsenkirchener Straßenbahnen
Schützler	Michael	frischli Milchwerke GmbH
Sieck	Gabriele	Gesamtverband der deutschen Versicherungswirtschaft e.V.
Simon	Frank	Zürich Gruppe Deutschland
Stoffel	Matthias	SIZ GmbH
Stracke	Ralf	EWE AG
Van den Berg	Hans-Rainer	van den Berg Service AG
Wagner	Kirsten	Deutscher Verein des Gas- und Wasserfaches e.V.
Weise	Sven	Currenta
Wirtz	Frank	ERGO Group AG