Bundesministerium des Innern und für Heimat (BMI)
(Einzelplan 06)

24 Informationssicherheit: IT-Rat bleibt trotz erheblicher Defizite untätig

Zusammenfassung

Der IT-Rat blieb untätig, obwohl Berichte zur Informationssicherheit auf erhebliche Defizite hinwiesen. Er ließ sogar zu, dass die Ressorts das Berichtswesen aussetzten. Nun fehlen ihm Informationen, um die ressortübergreifende Informationssicherheit steuern zu können.

Die Bundesregierung hat im Jahr 2017 mit dem Umsetzungsplan Bund (UP Bund) eine Leitlinie beschlossen, die allen Bundesbehörden vorschreibt, wie sie sich vor Cyberangriffen schützen müssen. Das zugehörige Berichtswesen soll jährlich darüber informieren, wo und wie die Bundesverwaltung ihren Schutz zielgerichtet weiterentwickeln und verbessern muss. Das BMI koordiniert die Berichte der Ressorts und leitet dem IT-Rat jährlich einen Gesamtbericht zu. Die Gesamtberichte der Jahre 2017 bis 2019 wiesen u. a. deutlich darauf hin, dass fast jede zweite Behörde über kein Notfallkonzept verfügte und den Betrieb ihrer kritischen Geschäftsprozesse nicht sicherstellte. Der IT-Rat nutzte das Berichtswesen nicht, sodass er weder dessen Schwächen erkennen noch die in den Berichten aufgezeigten Defizite abstellen konnte.

Der letzte Gesamtbericht des BMI für das Jahr 2019 hat den Status zur Informationssicherheit zudem nur unvollständig dargestellt. So fehlten Daten zahlreicher Behörden und die Informationen der Ressorts fanden sich nur anonymisiert wieder. Der Bundesrechnungshof regte an, die Aussagekraft und die Wirksamkeit des Berichtswesens zu verbessern. Statt diesen Empfehlungen zu folgen, setzten die Ressorts auf Vorschlag des BMI das Berichtswesen aus. Daher fehlen dem IT-Rat ab dem Jahr 2020 Informationen, inwieweit die Bundesbehörden den UP Bund umgesetzt haben.

Das BMI muss das Berichtswesen umgehend wieder aufnehmen, dessen Schwächen zeitnah beheben und den IT-Rat über den aktuellen Status der Informationssicherheit aller Ressorts informieren. Diese Informationen muss der IT-Rat nutzen, um das Management der Informationssicherheit des Bundes anhand aktueller und vollständiger Daten professionell zu steuern.

24.1 Prüfungsfeststellungen

BMI muss dem IT-Rat über Informationssicherheit berichten

Die Bundesregierung hat im Jahr 2017 den UP Bund beschlossen. Dieser definiert u. a. die ressortübergreifenden Sicherheitsziele und das angestrebte Sicherheitsniveau. Er schreibt verbindlich vor, welche Pflichten Bundesbehörden haben, um die Sicherheit ihrer IT zu gewährleisten. Hierzu muss jede Behörde ein Informationssicherheitsmanagement betreiben, das erforderliche Managementprinzipien, Ressourcen und Sicherheitsprozesse definiert. Die Bundesbehörden müssen jährlich prüfen, ob sie die im UP Bund festgelegten Sicherheitsmaßnahmen einhalten. Die Ergebnisse fassen die Bundesministerien für ihr jeweiliges Ressort zusammen und leiten sie an das BMI.

Das BMI erstellt daraus einen Gesamtbericht für den IT-Rat. Der IT-Rat ist das höchste Steuerungsgremium für alle Fragen der IT. In ihm sind alle Bundesministerien auf Leitungsebene vertreten; den Vorsitz führt das BMI gemeinsam mit dem Bundeskanzleramt. Auf Grundlage des Gesamtberichts muss der IT-Rat regelmäßig prüfen, ob besondere Sicherheitsmaßnahmen ergriffen oder sogar der UP Bund angepasst werden muss, um die IT-Sicherheit des Bundes zu gewährleisten.

Berichte weisen auf Defizite hin

Die Gesamtberichte für die Jahre 2017/2018 sowie 2019 an den IT-Rat wiesen u. a. darauf hin, dass über 40 % der Bundesbehörden

- kein IT-Notfallkonzept hatten und keine IT-Notfallübungen durchführten,
- die Arbeitsfähigkeit ihrer IT-Systeme, die für ihre kritischen Geschäftsprozesse notwendig sind, nicht sicherstellten und
- das eigene Informationssicherheitsmanagement nicht kontrollierten.

Die Gesamtberichte zeigten auch auf, dass lediglich 50 bis 60 % der Stellen im behördenspezifischen Informationssicherheitsmanagement besetzt waren. Die Behörden bezeichneten den gravierenden Mangel an IT-Personal als größte Herausforderung.

IT-Rat wird trotz Kenntnis der Defizite nicht tätig

Der Bundesrechnungshof stellte fest, dass der IT-Rat seit dem Jahr 2019 zwar 16 Mal tagte, jedoch nichts gegen die ihm bekannten Defizite unternahm. Er fasste keine Beschlüsse, um die Notfallvorsorge, den Umgang mit kritischen Geschäftsprozessen oder die Kontrolle der Informationssicherheit zu verbessern. Auch prüfte er nicht, welche Schritte einzelne Ressorts diesbezüglich ergriffen hatten und inwieweit ein ressortübergreifendes Handeln erforderlich war.

Berichtswesen hat selbst Schwächen

Der Bundesrechnungshof prüfte auch das Berichtswesen zum UP Bund als solches. Er kam zu dem Ergebnis, dass die Informationen der Bundesbehörden zwar wichtige Erkenntnisse zum Status ihrer Informationssicherheit liefern. Dem Berichtswesen mangelte es aber im Wesentlichen daran, dass

- lediglich die Ergebnisse von knapp einem Drittel aller Bundesbehörden vollständig in den Gesamtbericht eingeflossen waren,
- wesentliche Defizite nicht klar benannt und
- der Sicherheitsstatus der einzelnen Ressorts gegenüber dem IT-Rat nicht offengelegt, sondern anonymisiert dargestellt waren.

Ressorts setzen das Berichtswesen auf Vorschlag des BMI aus

Der Bundesrechnungshof empfahl dem BMI, die Aussagekraft und die Wirksamkeit des vorhandenen Berichtswesens zu verbessern. So sollte das BMI im Gesamtbericht beispielsweise darauf verzichten, die Ergebnisse zu anonymisieren und deutlich auf fehlende Informationen hinweisen. Außerdem sollte es die Prozesse im Berichtswesen effizienter gestalten. Das BMI sagte dem Bundesrechnungshof im Juli 2021 zunächst zu, diesen Empfehlungen im Wesentlichen folgen zu wollen. Im Mai 2022 beschlossen die Ressorts jedoch auf Vorschlag des BMI, den Status für die Jahre 2020 und 2021 gar nicht zu erheben. Damit konnte das BMI dem IT-Rat ab dem Jahr 2020 keinen Gesamtbericht vorlegen. Das Berichtswesen, wie der UP Bund es fordert, setzten die Ressorts faktisch bis auf Weiteres aus. Das BMI begründete dies damit, dass das Berichtswesen in der jetzigen Form

- nicht wirtschaftlich sei,
- zu wenig steuerungsrelevante Informationen liefere und
- der Änderungsaufwand sehr hoch sei.

Wie die Bundesbehörden für den Gesamtbericht stattdessen den Status der Informationssicherheit erheben sollten, legte das BMI nicht fest. Weil die Bundesverwaltung zu wenig IT-Personal habe, solle sich dieses auf wichtigere Aufgaben als das Berichtswesen konzentrieren.

Aufgrund welcher Informationen der IT-Rat das ressortübergreifende Informationsmanagement des Bundes überwachen, evaluieren und steuern will, hat er nicht festgelegt. Alternative bundesweite Erhebungen zur Informationssicherheit gibt es derzeit nicht. Ein Informationssicherheitscontrolling, mit dem sich steuerungsrelevante Daten identifizieren, analysieren und interpretieren ließen, hat er bisher nicht eingeführt. Wann die Bundesverwaltung das Berichtswesen zum UP Bund reformiert und wieder aufnimmt, ist offen. Ebenso ist ungewiss, wie es sich als Teil eines Informationssicherheitscontrollings in ein übergeordnetes IT-Controlling integrieren lässt.

24.2 Würdigung

Der IT-Rat hätte die ihm vorgelegten Berichte nutzen müssen, um den dort aufgezeigten Defiziten in der Informationssicherheit rechtzeitig entgegenzutreten. Das unzureichende Notfallmanagement, die mangelnde Absicherung kritischer Geschäftsprozesse und fehlende Sicherheitskontrollen hätten genügend Anlass gegeben, Ursachen und Handlungsbedarfe zu erörtern. Als höchstes Entscheidungsgremium hätte der IT-Rat auf politischer Ebene um stärkere Unterstützung für die Informationssicherheit werben müssen. Dafür hätte er die vom Berichtswesen aufgezeigten Soll-Ist-Abweichungen als Nachweis anführen können.

Angesichts der Bedeutung des UP Bund für die Informationssicherheit hätte der IT-Rat nicht tolerieren dürfen, dass die Ressorts das zugehörige Berichtswesen aussetzen. Den Entscheidungsträgern im IT-Rat und den Ressorts fehlt nun in einer besonders kritischen geopolitischen Situation ein aktueller Überblick über den Status der Informationssicherheit in den Bundesbehörden. Inwieweit die Ressorts die Ziele des UP Bund erreicht haben, kann der IT-Rat kaum beurteilen. Auch kann er nicht bewerten, ob er den UP Bund anpassen sollte. Angesichts der ständig steigenden Bedrohung aus dem Cyberraum birgt dies erhebliche Risiken für die Funktionsfähigkeit der IT und damit letztlich für die Handlungsfähigkeit der gesamten Bundesverwaltung.

Trotz eines Personalmangels in der Informationssicherheit ist es weder sachgerecht noch wirtschaftlich, auf ein Berichtswesen zu verzichten. Je weniger Ressourcen verfügbar sind, umso wichtiger ist es, den Status und die akuten Handlungsbedarfe in der Informationssicherheit zu kennen. Dem IT-Rat fehlen nun Daten, um Sicherheitsmaßnahmen priorisieren und begrenztes Personal zielgerichtet einsetzen zu können.

Der IT-Rat muss daher unverzüglich darauf hinwirken, dass die Ressorts das Berichtswesen wieder aufnehmen und die Entscheidungsträger aktuelle und vollständige Statusinformationen zur Informationssicherheit erhalten.

Um die Aussagekraft der Berichte zu erhöhen, muss das BMI dessen Schwächen zeitnah beheben. Dabei sollte es die von ihm bereits zugesagten Empfehlungen des Bundesrechnungshofes berücksichtigen. Um die knappen Ressourcen in der Informationssicherheit zu schonen, könnten sich die Bundesbehörden zunächst darauf beschränken, die Daten nur für die besonders kritischen Bereiche zu erheben. Dies beträfe insbesondere die Notfallvorsorge, kritische Geschäftsprozesse sowie die Kontrolle der Informationssicherheit.

Um die Wirksamkeit des Berichtswesens zu steigern, sollte der IT-Rat dem BMI die Daten nennen, die er benötigt, um die Informationssicherheit besser evaluieren, überwachen und steuern zu können. Die Berichte sollten im Zeitverlauf vergleichbare Informationen liefern sowie Zusammenhänge zwischen ergriffenen Sicherheitsmaßnahmen und erzielter Wirkung aufzeigen.

Das verbesserte Berichtswesen zum UP Bund sollte der IT-Rat dann als Teil eines Informationssicherheitscontrollings in ein übergeordnetes IT-Controlling integrieren lassen.

24.3 Stellungnahme

Das BMI hat darauf hingewiesen, dass es nach dem Ressortprinzip den Ressorts selbst obliege, ein wirksames Informationssicherheitsmanagement einzurichten. Es sei nicht dafür verantwortlich, wie die Bundesbehörden den Status ihrer Informationssicherheit erheben.

Die Entscheidung, das Berichtswesen auszusetzen, hätten die Ressorts einvernehmlich beschlossen. Der Änderungsbedarf im Berichtswesen sei so umfangreich, dass er die Ressorts über Monate hinweg stark binde. Seit längerem gäbe es bereits Anzeichen dafür, dass das Informationssicherheitsmanagement des Bundes zunehmend überfordert sei. Ein effizienteres Berichtswesen sei nachrangig, beispielsweise gegenüber einer Weiterentwicklung des Regelungsrahmens.

Zwar pausiere das Berichtswesen, gleichwohl tausche sich das BMI mit dem Bundeskanzleramt und den Ressorts zur Informationssicherheit aus. Gemeinsam wolle man die Hauptprobleme herausarbeiten und neue Ansätze entwickeln, um die IT-Systeme zu härten.

Aus Sicht des BMI müsse die Informationssicherheit in der Bundesverwaltung dringend durch andere Verfahren geprüft und gesteuert werden. Bislang beruhe das Berichtswesen weitestgehend auf Selbsterklärungen der Behörden. Mittlerweile sei jedoch das Bundesamt für Sicherheit in der Informationstechnik (BSI) gesetzlich befugt, in der Bundesverwaltung umfassend zu prüfen. Dies erlaube es perspektivisch, den Sachstand zum UP Bund effizienter zu erheben und zielgerichteter zu steuern. Schon jetzt gebe es weitere Prüfaktivitäten des BSI sowie Kontrollpflichten der Bundesbehörden. Auch wenn das Berichtswesen ausgesetzt sei, entstehe demnach zu keiner Zeit ein „prüffreier Raum“.

24.4 Abschließende Würdigung

Die Stellungnahme des BMI lässt offen, wie der IT-Rat nun die Informationssicherheit des Bundes belastbar bewerten und wirksam steuern kann. Ohne ein Informationssicherheitscontrolling fehlen ihm ausreichende und aktuelle Statusinformationen. Diese müssen regelmäßig und standardisiert aus allen Bundesbehörden vorliegen.

Das BMI erweckt einen falschen Anschein, wenn es behauptet, es gebe aktuell keinen „prüffreien Raum“. Prüfungen des BSI in einzelnen Bundesbehörden können künftig zwar punktuell wichtige Informationen liefern. Für einen aktuellen, umfassenden und systematischen Überblick über den Status der Informationssicherheit in der gesamten Bundesverwaltung wird dies nicht ausreichen. Angesichts von über hundert Bundesbehörden und begrenzten Prüfkapazitäten des BSI wäre dies nicht realistisch. Auch wenn das BMI die Art und Weise anpasst, wie Informationssicherheit künftig geprüft und gesteuert wird, kann es derzeit nicht auf das im UP Bund vorgesehene Prinzip von Selbsterklärungen der Bundesbehörden verzichten. Es sollte die Selbsterklärungen mit den Prüfergebnissen des BSI abgleichen und so einer Qualitätskontrolle unterziehen.

Der UP Bund als Beschluss der Bundesregierung verpflichtet dazu, die Informationssicherheit in der Bundesverwaltung jährlich zu evaluieren. Das BMI lässt nicht erkennen, ob und wie es dieser Pflicht gemeinsam mit den übrigen Ressorts künftig nachkommen will. Sein Hinweis, es sei nicht dafür verantwortlich, wie die Bundesbehörden den Status ihrer Informationssicherheit erheben, ist zwar zutreffend, greift aber zu kurz. Das BMI verkennt dabei, dass der IT-Rat dafür sorgen muss, dass die Bundesbehörden den Status nach ressortübergreifend abgestimmten Vorgaben erheben. Weil das BMI für das Informationssicherheitsmanagement des Bundes und das dazugehörige Berichtswesen übergreifend verantwortlich ist, muss es im IT-Rat auf entsprechende Beschlüsse hinwirken.

Der Bundesrechnungshof befürchtet, dass das Berichtswesen ausgesetzt bleibt. Der Zustand eines in weiten Teilen „informationsfreien Raums“ würde sich damit auf unbestimmte Zeit fortsetzen. Dies wäre angesichts einer zunehmend verschärften Cybersicherheitslage besonders kritisch. Die Ressorts müssen das Berichtswesen daher umgehend wieder aufnehmen. Dies ist ohne Frage mit einem zusätzlichen Aufwand für das stark belastete IT-Personal verbunden. Aber ohne ein Minimum an Informationen lassen sich weder strukturelle Defizite noch erfolgversprechende Ansätze zu deren Behebung systematisch identifizieren.

Wenn das BMI beabsichtigt, mit den übrigen Ressorts gemeinsam die Hauptprobleme herauszuarbeiten, dann wird dies ohne Informationen aus den Geschäftsbereichen ebenfalls kaum möglich sein.

Gleiches gilt für die vom BMI gegenüber dem Berichtswesen als vorrangig bezeichnete Absicht, den Regelungsrahmen weiterzuentwickeln. Ohne grundlegende Informationen aus den Sachstandsberichten fehlen wichtige Erkenntnisse, um das zentrale Regelwerk für die Informationssicherheit, den UP Bund, zielgerichtet fortschreiben zu können.

Das BMI sollte sich im IT-Rat dafür einsetzen, dass dieser das Berichtswesen zu einem wirksamen Informationssicherheitscontrolling ausbaut. Mit dessen zentralen Erkenntnissen zu Defiziten, Risiken und Nachsteuerungsbedarf im Informationssicherheitsmanagement des Bundes muss sich der IT-Rat dann ebenso regelmäßig wie mit anderen IT-Themen befassen.