4 Fehlender Einsatz einer IT-Lösung gefährdet die Netze des Bundes

(Kapitel 0602 Titel 894 51)

Zusammenfassung

Die Bedrohungslage im Cyberraum ist so hoch wie nie. Dennoch erfüllen viele Behörden und Einrichtungen des Bundes nicht die Sicherheitsanforderungen der Netze des Bundes (NdB) – und schützen sich mehrheitlich auch nicht mit einer vom Bund entwickelten ergänzenden IT-Lösung.

Für die sichere Kommunikation nutzt der Bund die Infrastruktur der NdB. Die derzeit angeschlossenen 106 Behörden und Einrichtungen des Bundes (nachfolgend Nutzer genannt) können dort Informationen bis zum Geheimhaltungsgrad „Verschlusssache – Nur für den Dienstgebrauch" (VS-NfD) übermitteln. Hierfür müssen sie grundsätzlich hohe Sicherheitsanforderungen erfüllen. Insgesamt 52 Nutzer erfüllen diese nicht vollständig. Sie sehen sich häufig nicht in der Lage, sie zu erfüllen. Einige haben bei ihrer Kommunikation auch einen geringeren Geheimhaltungsbedarf.

Um dennoch die Sicherheit der NdB zu gewährleisten, entwickelte das BMI im Jahr 2019 mit dem sogenannten Transport Layer Security-Proxy (TLS-Proxy) eine ergänzende IT-Lösung. Sie war insbesondere für Nutzer vorgesehen, die die Sicherheitsanforderungen der NdB nicht erfüllen. Allerdings setzen 45 der betroffenen 52 Nutzer den TLS-Proxy nicht ein. Dem BMI ist es weder gelungen, die Sicherheitsanforderungen durchzusetzen noch die alternative IT-Lösung zu etablieren. Dies gefährdet die Sicherheit der NdB insgesamt.

Langfristig sollen alle Nutzer der NdB den TLS-Proxy zusätzlich verwenden. Dazu will das BMI ihn ausbauen. Entsprechende Investitionen sind nur gerechtfertigt, wenn geeignete Maßnahmen seinen Einsatz sicherstellen. Das BMI sollte deshalb gemeinsam mit den Bundesministerien priorisieren und verbindlich festgelegen, welche Nutzer den TLS-Proxy wann einsetzen.

4.1 Prüfungsfeststellungen

Behörden und Einrichtungen des Bundes gefährden Sicherheit der NdB

Mit den NdB betreibt die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) ein eigenes Sprach- und Datennetz für die Behörden und Einrichtungen des Bundes. Derzeit sind 106 Behörden und Einrichtungen angeschlossen. Mehr als 300 000 Beschäftigte nutzen die NdB. Sie können damit Informationen bis zum Geheimhaltungsgrad VS-NfD übertragen. Hierfür müssen Behörden und Einrichtungen, die die NdB nutzen, grundsätzlich hohe Sicherheitsanforderungen erfüllen.

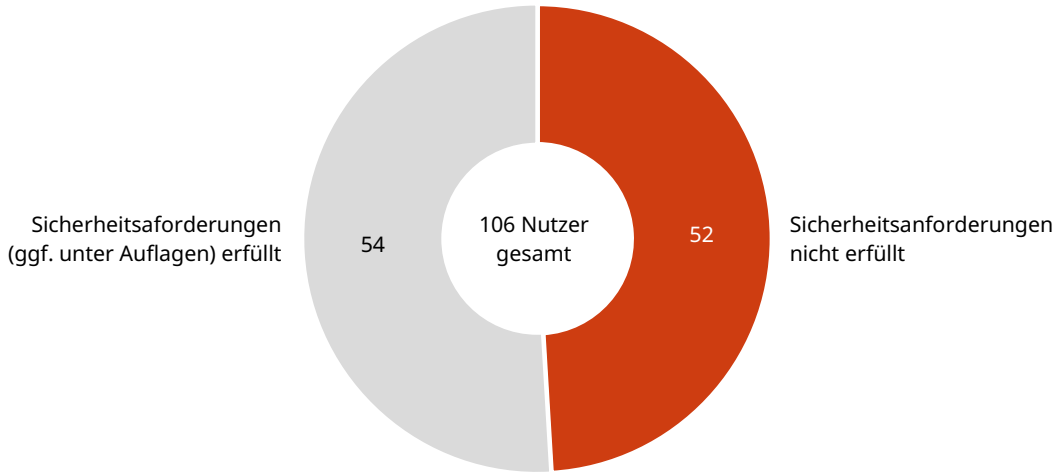
Die NdB gingen im Jahr 2019 aus mehreren staatlichen Vorgängernetzen mit zum Teil niedrigeren Sicherheitsstandards hervor. Mehrere der in die NdB einbezogenen Behörden und Einrichtungen sahen und sehen sich nicht in der Lage, die hohen Sicherheitsanforderungen der NdB zu erfüllen. Einige haben bei ihrer Kommunikation auch einen geringeren Geheimhaltungsbedarf als VS-NfD. Für solche Nutzer beschloss der Bund im Jahr 2019, eine sogenannte „NdB-Grundschutzzone/NdB-Extranet“ (Grundschutzzone) mit geringeren Sicherheitsanforderungen einzurichten. Das BMI sicherte allen Nutzern zu, die NdB nutzen zu können, bis die Grundschutzzone fertiggestellt ist. Sie ging im Januar 2023 in Betrieb, stieß bislang allerdings bei den Behörden und Einrichtungen auf wenig Interesse. Viele Dienste sind in der Grundschutzzone noch nicht verfügbar, z. B. eine elektronische Aktenführung oder ein Personalverwaltungssystem. Das BMI will die Grundschutzzone frühestens bis Juni 2025 um diese Dienste erweitern. Behörden und Einrichtungen, die die Sicherheitsanforderungen der NdB nicht erfüllen, können bis dahin weiterhin die NdB nutzen.

Derzeit erfüllt knapp die Hälfte der Nutzer der NdB nicht vollständig die Sicherheitsanforderungen (vgl. Abbildung 4.1):

Abbildung 4.1

Sicherheitsanforderungen der NdB häufig nicht erfüllt

Die Netze des Bundes (NdB) sind ein Sprach- und Datennetz für Behörden und Einrichtungen des Bundes. Die hohen Sicherheitsanforderungen erfüllen derzeit 52 von 106 Nutzern nicht.



Grafik: Bundesrechnungshof.

Zugleich schätzt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Lagebericht aus dem Jahr 2023 die Bedrohungslage im Cyberraum als so hoch wie nie ein.

BMI will Sicherheit mit einer Übergangslösung verbessern

Den Nutzern, die die Sicherheitsanforderungen der NdB nicht erfüllten, bot das BMI im Jahr 2019 einen TLS-Proxy als Übergangslösung bis zum Wechsel in die Grundschutzzone an.

Mit einem TLS-Proxy kann die BDBOS den verschlüsselten Internetverkehr der NdB entschlüsseln, mit einem Schadprogramm-Erkennungssystem analysieren und wieder verschlüsseln. Ein entsprechender Schutz ist erforderlich, da mittlerweile über 85 % des Internetverkehrs in den NdB verschlüsselt sind. Sind Behörden und Einrichtungen nicht hinreichend geschützt, kann Schadsoftware über diesen Weg bei ihnen eindringen, sich ausbreiten und die NdB insgesamt und deren Nutzer gefährden (vgl. Abbildung 4.2).

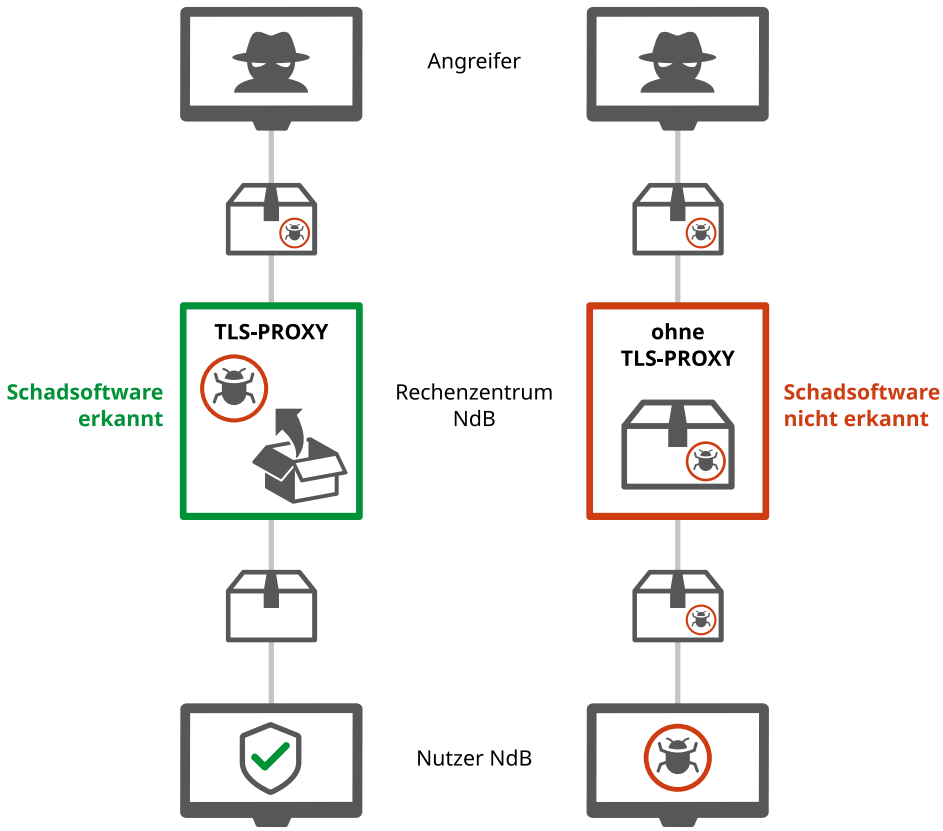
Inzwischen verfolgt das BMI das Ziel, dass langfristig alle Nutzer der NdB den TLS-Proxy verwenden. Dies gilt auch für Nutzer, die die Sicherheitsanforderungen erfüllen. Damit will es die Sicherheit der NdB insgesamt weiter verbessern. Das BMI beabsichtigt

daher, die Kapazität und Leistungsfähigkeit des TLS-Proxy auszubauen. Die BDBOS will dazu u. a. ihre Rechenzentren erweitern. Für den TLS-Proxy gab es bisher rund 1,1 Mio. Euro aus.

Abbildung 4.2

Die NdB sind mit TLS-Proxy besser vor Angriffen zu schützen

Verschlüsselte Inhalte werden bei Angriffen zum Sicherheitsrisiko für die Netze des Bundes (NdB). Mit einem TLS-Proxy kann der verschlüsselte Internetverkehr entschlüsselt, auf Schadprogramme analysiert und wieder verschlüsselt werden. Ohne TLS-Proxy ist dies nicht möglich.



Grafik: Bundesrechnungshof.

Nur wenige Behörden und Einrichtungen nutzen den TLS-Proxy

Im Oktober 2022 hatte der Bundesrechnungshof dem Haushaltsausschuss des Deutschen Bundestages berichtet, dass nur wenige Nutzer den TLS-Proxy verwenden. Er empfahl, dass insbesondere diejenigen Nutzer den TLS-Proxy umgehend verwenden sollen, die die Sicherheitsanforderungen der NdB nicht erfüllen.

Die Situation hat sich seitdem nicht verbessert. Anfang 2024 erklärte die BDBOS, dass von den 52 Nutzern, die die Sicherheitsanforderungen nicht erfüllen, 45 den TLS-Proxy der BDBOS nicht einsetzen. Weitere Kapazitäten seien verfügbar.

4.2 Würdigung

BMI und BDBOS ist es bislang nicht gelungen, den TLS-Proxy erfolgreich zu etablieren. Der Bundesrechnungshof bewertet es insbesondere kritisch, dass von den 52 Nutzern der NdB, die die Sicherheitsanforderungen nicht erfüllen, weiterhin 45 den TLS-Proxy nicht verwenden. Diese Nutzer gefährden nicht nur ihre eigenen Netze, sondern die NdB insgesamt und deren Nutzer.

Das BMI hätte spätestens nach den Hinweisen des Bundesrechnungshofes im Jahr 2022 sicherstellen müssen, dass insbesondere die Nutzer, die die Sicherheitsanforderungen der NdB nicht erfüllen, den TLS-Proxy schnellstmöglich einsetzen – vor allem, weil diese noch nicht in die Grundschutzzone wechseln und die NdB weiter gefährden. Dies wiegt umso schwerer, da das BSI die Bedrohungslage im Cyberraum als so hoch wie nie einschätzt.

Ein TLS-Proxy ist ein geeignetes Werkzeug, um Schadsoftware zu erkennen und damit die Sicherheit der NdB insgesamt zu steigern. Je mehr Nutzer ihn verwenden, desto besser sind die NdB insgesamt und deren Nutzer vor Angriffen aus dem Internet geschützt. Die weiteren Investitionen, um die Kapazität des TLS-Proxy zu erweitern, sind jedoch nur dann gerechtfertigt und sachgerecht, wenn sie um geeignete Maßnahmen ergänzt werden, die seinen Einsatz durch die Nutzer sicherstellen.

4.3 Stellungnahme

Das BMI hat die Feststellungen des Bundesrechnungshofes zum TLS-Proxy grundsätzlich geteilt. Allerdings lasse der technische Aufbau der NdB bisher nur eine begrenzte Anzahl Nutzer für den TLS-Proxy zu.

Zugleich hat das BMI darauf hingewiesen, dass die Nutzer, die die Sicherheitsanforderungen nicht einhalten, die NdB unterschiedlich gefährdeten. In Einzelfällen wären bereits geringe Abweichungen mit niedrigem Gefährdungspotenzial ausschlaggebend. Auch würden einzelne Nutzer eigene, zum TLS-Proxy vergleichbare Lösungen einsetzen. Insgesamt bestehe in den NdB bereits ein hohes Maß an Sicherheit. Dennoch wolle die BDBOS den TLS-Proxy bis Sommer 2025 erneuern und dessen Kapazitäten erweitern. Perspektivisch sollen alle Nutzer den TLS-Proxy einsetzen. Dies würde die Sicherheit der NdB weiter verbessern.

Schließlich hat das BMI eingeräumt, dass in der Grundschutzzone viele Dienste fehlen. Es plane für Ende 2024 ein Pilotprojekt, um künftig benötigte Dienste in der Grundschutzzone bereitzustellen. Darüber hinaus arbeite es bereits an einer Nachfolgelösung für die NdB. Diese werde leistungsfähiger sein und viele der heutigen Sicherheitsprobleme lösen.

4.4 Abschließende Würdigung

Der Bundesrechnungshof hält an seiner Kritik fest. Die NdB und deren Sicherheit haben eine hohe Bedeutung für den Bund. Für Nutzer, die sich nicht in der Lage sehen, die Sicherheitsanforderungen der NdB zu erfüllen, hat das BMI die Grundschutzzone errichtet und ihnen bis zum Wechsel dorthin den TLS-Proxy angeboten. Die meisten dieser Nutzer nutzen aber bisher weder den TLS-Proxy, noch haben Sie die NdB zugunsten der Grundschutzzone verlassen.

Dem Bundesrechnungshof ist bewusst, dass die Nutzer, die die Sicherheitsanforderungen nicht erfüllen, die NdB unterschiedlich gefährden. Diese stellen dennoch insgesamt eine Gefährdung für die NdB dar. Mehrere dieser Nutzer gehören zudem zu Nutzergruppen, deren IT in der Vergangenheit erhebliche Mängel aufwies. Dennoch nutzen auch diese den TLS-Proxy größtenteils nicht. Dies ist und bleibt riskant.

Das BMI hat mit dem TLS-Proxy eine zentrale Lösung entwickelt und diese inzwischen allen Nutzern angeboten. Perspektivisch sollen alle Nutzer den TLS-Proxy einsetzen. Es ist daher für den Bund nicht wirtschaftlich, wenn einzelne Behörden und Einrichtungen eigene, zum TLS-Proxy vergleichbare Lösungen beschafft haben. Ob insbesondere jene Nutzer, die die Sicherheit der NdB erheblich gefährden, solche Eigenlösungen einsetzen, lässt das BMI in seiner Stellungnahme offen.

Zwar hat das BMI angekündigt, viele der heutigen Sicherheitsprobleme in der Zukunft lösen zu wollen. Es ließ aber offen, bis wann es fehlende Dienste in der Grundschutzzone bereitstellen und die geplante Nachfolgelösung der NdB aufbauen will. Angesichts des unklaren Zeithorizonts sollte das BMI die Sicherheit der NdB in der aktuellen Struktur sicherstellen.

Das BMI sollte angesichts der Bedrohungslage gemeinsam mit den übrigen Bundesministerien die Ursachen für die geringe Nutzung des TLS-Proxy ermitteln und beseitigen. Zudem sollten das BMI und die Bundesministerien verbindlich festlegen, welche Nutzer wann den TLS-Proxy einsetzen müssen. Dabei hat das BMI darauf hinzuwirken, dass insbesondere solche Nutzer den TLS-Proxy schnellstmöglich verwenden, die die Sicherheitsanforderungen nicht erfüllen und gleichzeitig die Sicherheit der NdB am meisten gefährden. Die BDBOS hat zugleich die technische Umsetzung sicherzustellen.