AB-ND Prüfung 22-18
Datenbeschaffung durch Cyber NDB

Zusammenfassung:

Ausgangslage und Ablauf:

Von 2015 bis 2020 beschaffte der NDB in der Bearbeitung von möglichen Cyberangriffen auch Informationen, welche dem Fernmeldegeheimnis unterstehen. Diese Beschaffungsmassnahmen sind bewilligungspflichtig und nur mit Genehmigung des Bundesverwaltungsgerichts erlaubt.

Die AB-ND wurde im April 2021 vom damaligen Direktor NDB telefonisch über mögliche Unrechtmässigkeiten der Informationsbeschaffung im Ressort Cyber NDB sowie über die Einleitung einer internen Untersuchung des NDB informiert. Die AB-ND begleitete die interne Untersuchung des NDB betreffend diese Vorgänge und liess sich durch den NDB laufend über den Stand der Abklärungen informieren. Darüberhinausgehend erhielt die AB-ND weitere Hintergrundinformationen zum selben Sachverhalt.

Im Anschluss an diese interne Untersuchung leitete das VBS im Jahr 2022 eine durch den ehemaligen Bundesrichter Niklaus Oberholzer geleiteten Administrativuntersuchung ein. Die AB-ND verzichtete deshalb bis zu diesem Zeitpunkt auf eine eigene Prüfung.

Nach dem Abschluss der Administrativuntersuchung des VBS erachtete die AB-ND die Vorkommnisse im Ressort Cyber in Bezug auf die Rechtmässigkeit der Informationsbeschaffung als weitgehend abgeklärt.

Weiterhin offene Fragen wie bspw. Kontakte mit privaten Unternehmen und den mit diesen Unternehmen ausgetauschten Informationen wurden nach Meinung der AB-ND hingegen weder durch die interne Untersuchung des NDB noch durch die Administrativuntersuchung geklärt.

Im Juni 2022 startete die AB-ND deswegen eine Prüfung **mit Fokus auf die Beantwortung der zu den Vorgängen im Ressort Cyber NDB in den Jahren 2015 bis 2020 weiterhin noch ungeklärten Fragen. Darüber hinaus prüfte die AB-ND ebenfalls, ob die vom NDB eingeleiteten Massnahmen in Form von Anpassungen der Prozesse und der Organisation des Ressorts Cyber geeignet und ausreichend waren, um künftig die rechtmässige und zweckmässige Datenbeschaffung sicherzustellen.**

Die AB-ND analysierte dazu u.a. einen umfangreichen Datensatz, welcher weder in der internen Untersuchung des NDB noch in der Administrativuntersuchung des VBS untersucht worden war. Der NDB hatte diese Daten im Zuge der internen Untersuchung 2021 forensisch gesichert, entschied sich hauptsächlich aus personalrechtlichen Gründen jedoch gegen eine eigene Auswertung. Die AB-ND hingegen sah sich in ihrer Aufgabe als Aufsichtsbehörde als berechtigt, den Datensatz zu analysieren.

Die Prüfung der AB-ND behandelte Sachverhalte die Vorgänge im Bereich Cyber betreffend, die sich bis 2021 ereigneten sowie organisatorische Massnahmen im gleichen Bereich, die bis März 2023 getroffen wurden. Die Interviews mit den betroffenen Mitarbeitenden und Führungspersonen fanden bis Dezember 2022 statt. Zu einzelnen konkreten Fragen holte die AB-ND bis im Frühjahr 2024 gezielte Auskünfte ein. Abschliessend wurde der NDB zwischen Dezember 2024 und Januar 2025 Gelegenheit erteilt, zu den Prüfergebnissen Stellung zu nehmen.

Ergebnis der Prüfung:

Konkret beantwortete die AB-ND bei dieser Prüfung folgenden Prüffragen:

1. Wurde der relevante Sachverhalt für die Beurteilung der Vorgänge im Ressort Cyber vollständig erfasst?
2. Wie stellt der NDB sicher, dass die Rechtmässigkeit bei der Analyse von Datenverkehr von Providern künftig gewährleistet ist?
3. Sind die vom NDB getroffenen organisatorischen Massnahmen und Kontrollen zweckmässig und wirksam, um solche Vorkommnisse in Zukunft verhindern zu können?

1. Wurde der relevante Sachverhalt für die Beurteilung der Vorgänge im Ressort Cyber vollständig erfasst?

Sowohl die interne Untersuchung als auch die Administrativuntersuchung kamen zum Schluss, dass die im Zuge der Analyse von Cyber-Vorfällen durch das Ressort Cyber bearbeiteten Daten praktisch ausschliesslich technischer Natur waren und kein allfälliger Personenbezug bestand. Das Ressort Cyber habe keinen Bedarf, nach Personendaten zu suchen; von Interesse seien technische Indikatoren und Vorgehensweisen, welche vollständig personenunabhängig seien. Die aus Cyberangriffen ausgewerteten Daten könnten nicht einer bestimmten Person zugeordnet werden.

Die Analyse der forensisch gesicherten Daten durch die AB-ND ergaben jedoch auch Treffer, die auf eine Bearbeitung von Personendaten und deren möglichen Austausch mit externen Stellen hindeuteten. Der Datensatz enthielt u.a. IP-Adressen[1], die aus rechtlicher Sicht als

[1] Eine IP-Adresse (Internet Protocol-Adresse) besteht aus einer Zahlenabfolge, die jedem Gerät zugewiesen wird, das mit einem Computernetzwerk oder dem Internet verbunden ist.

Personendaten zu qualifizieren sind. Personendaten sind gemäss Art. 5 lit. a des Datenschutzgesetzes (DSG)[2] alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Der Bundesrat hielt schon in der Botschaft zum DSG 1988 fest: «Ist der Aufwand für die Bestimmung der betroffenen Person derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, dann liegt keine Bestimmbarkeit vor.»[3] Der NDB verfügt über die Möglichkeit bspw. gemäss Art. 37 und 38 der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)[4], Auskünfte über die Identifikation der Benutzerschaft bei eindeutig oder nicht eindeutig in der Schweiz zugeteilten IP-Adressen einzuholen. Der Aufwand für die Bestimmung von betroffenen Personen, die eine IP-Adresse in der Schweiz benutzen, ist zumindest für einen Teil der bearbeiteten IP-Adressen für den NDB demnach nicht zu gross. IP-Adressen sind deshalb im Arbeitsumfeld des NDB aus Sicht der AB-ND als Personendaten zu qualifizieren.

Die AB-ND fand in ihren Prüfhandlungen ein paar wenige Hinweise, die auf eine mögliche Informationsweitergabe hindeuten könnten. Eine vertiefte und abschliessende Klärung dieser Frage war jedoch auch mit der Datenanalyse nicht möglich. Die AB-ND formulierte eine **Empfehlung**, die Risiken in der Zusammenarbeit mit externen Stellen im Cyber-Bereich zu überprüfen.

2. Wie stellt der NDB sicher, dass die Rechtmässigkeit bei der Analyse von Datenverkehr von Providern künftig gewährleistet ist?

Gestützt auf die Erkenntnisse aus der internen Untersuchung ergriff der NDB am 20. Mai 2022 verschiedene Sofortmassnahmen. Nebst diesen Sofortmassnahmen überarbeitete der NDB noch während der internen Untersuchung seine Weisungen betreffend die nachrichtendienstlichen Tätigkeiten im Themengebiet Cyber im NDB vom 1. Oktober 2021 und setzte diese per 23. Mai 2022 in Kraft. Entgegen dem Inhalt der überarbeiteten Weisung nahm der NDB jedoch die Datenablage Netzwerkdaten Cyber, auf welcher die beschafften Daten aus Cyberangriffen gespeichert und bearbeitet wurden, bis heute nicht ausser Betrieb. Gemäss NDB könnte der Bereich Technische Analyse Cyber seine Arbeit ohne diese Infrastruktur gar nicht mehr, und das Ressort Cyber nur noch sehr eingeschränkt wahrnehmen. Die Ausserbetriebnahme sei nach wie vor die Absicht des NDB, vorerst müsse aber eine neue technische Lösung gefunden werden. Zu diesem Punkt warnte die AB-ND den NDB schon am 15. Dezember 2022 mit einem Schreiben. Sie informierte, dass die vom NDB kommunizierten Massnahmen weiterhin nicht umgesetzt wurden. Das für die Bearbeitung von Cyberdaten eingesetzte System sei nur eine

[2] SR 235.1
[3] BBl 1988 II 444
[4] SR 780.11

Übergangslösung, welche durch ein definitives System abgelöst werden solle. In diesem Zusammenhang **empfahl** die AB-ND dieses Thema nun dringend anzugehen.

Die Prüfhandlungen der AB-ND zeigten auf, dass die vom NDB getroffenen und gegen aussen kommunizierte Sofortmassnahmen nicht alle umgesetzt wurden. Der sowohl in der internen als auch in der Administrativuntersuchung kritisierten fehlenden engen Führung des Ressorts Cyber wurde erst 2024 mit geeigneten Führungsinstrumenten entgegengewirkt.

Der NDB installierte keine neuen Kontrollen. Ein Vieraugenprinzip ausserhalb von Cyber NDB fehlte weiterhin. Auch zu diesem Punkt formulierte die AB-ND eine **Empfehlung**.

Die AB-ND stellte fest, dass die Mitarbeitenden des NDB an kein spezielles Benutzerreglement gebunden sind, welches die Rechte und Pflichten im Umgang mit beruflichen Geräten regelt. Die AB-ND **empfahl** dem NDB insbesondere, die Trennung zwischen geschäftlichem und privatem Gebrauch klar zu regeln und die Mitarbeitenden darüber zu informieren, dass Geräte durch den NDB im Verdachtsfalls gesichert und untersucht werden können.

3. Sind die vom NDB getroffenen organisatorischen Massnahmen und Kontrollen zweckmässig und wirksam, um solche Vorkommnisse in Zukunft verhindern zu können?

Die Prüfung der Informationsbeschaffung mittels genehmigungspflichtigen Beschaffungsmassnahmen in allgemeiner Art und Weise stand nicht im Fokus dieser Prüfung. Aus den Prüfhandlungen im Bereich Cyber ergaben sich auch keine Hinweise, dass weiterhin unrechtmässig Informationen bei Providern beschafft werden.

Selbstauferlegte Massnahmen wie bspw. die zeitnahe Umsetzung der im Stichprobenbericht der Qualitätssicherungsstelle des NDB aufgeführten Punkte hielt der NDB nicht immer ein.

Angesichts der Tragweite der nach mehreren Jahren erkannten und aufgearbeiteten unrechtmässigen Informationsbeschaffung durch das Ressort Cyber erstaunte es, dass der NDB auf neue Kontrollen verzichtete und sich lediglich auf neue Prozesse abstützte. Neue Prozesse waren unbestrittenermassen nötig, der Kontrolle deren Einhaltung muss jedoch ausreichende Beachtung zukommen. Aus den Prüfhandlungen entstand nicht der Eindruck, dass die Führung des Ressorts Cyber bis zum Ende der Prüfhandlungen im Februar 2024 mögliche Missstände in einem durchaus schwierigen ND-Umfeld rechtzeitig erkannt hätte. Mittlerweile führte der NDB eine Transformation durch und konnte im Januar 2025 plausibel darlegen, dass die Führung des Ressorts Cyber verbessert wurde, deshalb entschied die AB-ND diesbezüglich keine Empfehlung auszusprechen.