# Nationale NIS-Behörde

**Die Abteilung IV/10 Netz- und Informationssystemsicherheit im Innenministerium hat als nationale NIS-Behörde darauf zu achten, dass Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung die Vorgaben des Netz- und Informationssystemsicherheitsgesetzes umsetzen.**

Mit 1. Dezember 2021 wurde die Abteilung IV/10 Netz- und Informationssystemsicherheit (NIS) im Bundesministerium für Inneres eingerichtet. Die Abteilung erfüllt die Funktion der operativen NIS-Behörde für Österreich. Sie hat darauf zu achten, dass Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung die Vorgaben des Netz- und Informationsystemsicherheitsgesetzes (NISG) umsetzen. Weiters nimmt die Abteilung auf Basis der Regelungen im NISG eine koordinierende Rolle innerhalb der gesamtstaatlichen „Operativen Koordinierungsstruktur“ (OpKoord) und ihres Inneren Kreises (IKDOK) wahr und unterstützt die dem NISG unterworfenen Bereiche in der Cyber-Prävention. „Die zentrale Funktion der operativen NIS-Behörde für Österreich ist die behördliche Aufsicht über die Umsetzung der Vorgaben des Netz- und Informationssystemsicherheitsgesetzes (NISG) durch dessen Adressaten“, erläutert Gernot Goluch, der diesen Bereich innerhalb der Abteilung IV/10 verantwortet.

**Sicherheitsvorkehrungen.** Das NISG sieht vor, dass Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung verpflichtet sind, technische und organisatorische Sicherheitsvorkehrungen zu treffen und diese gegenüber der NIS-Behörde nachzuweisen, sowie schwere Sicherheitsvorfälle zeitnah zu melden. Neben einer Vielzahl anderer Aufgaben obliegt es den Mitarbeiterinnen und Mitarbeitern der Abteilung in diesem Zusammenhang, die Einhaltung der verpflichtenden Sicherheitsvorkehrungen bei den besagten Unternehmen und Organisationen in regelmäßigen Abständen zu überprüfen sowie eine Meldesammelstelle für Meldungen über Sicherheitsvorfälle zu betreiben.

**Qualifizierte Stellen.** Die Überprüfungen der verpflichtenden Sicherheitsvorkehrungen bei den betroffenen Unternehmen und Organisationen, genannt Audits, werden von „qualifizierten Stellen“ (QuaSten) durchgeführt. Mitarbeiterinnen und Mitarbeiter der Abteilung IV/10 sind in diesem Zusammenhang unter anderem dafür verantwortlich, auf Basis der Verordnung über qualifizierte Stellen (QuaSteV) die Qualifikationen der QuaSten sicherzustellen. Dazu zählen Erhebungen zur Qualifikation der Prüferinnen und Prüfer, sowie zu Prüfvorkehrungen, Sicherheitsvorkehrungen, Prüf- und Meldeprozessen.

Eine weitere zentrale Tätigkeit umfasst die Koordination und Kontrolle des gesamten Verfahrens, sowie die Dokumentation, Überprüfung und Bewertung der Ergebnisse der von den QuaSten durchgeführten Überprüfungen und Audits. Als Behörde obliegt es der Abteilung auch, Empfehlungen und im Bedarfsfall bescheidmäßige Anordnungen zur Umsetzung oder Anpassung von Sicherheitsvorkehrungen auszusprechen.

**Meldesammelstelle.** Die zentrale Tätigkeit in der Meldesammelstelle ist die Entgegennahme und Dokumentation von Pflichtmeldungen über Sicherheitsvorfälle bei Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen der öffentlichen Verwaltung sowie von freiwilligen Meldungen beliebiger Entitäten in Österreich. Im weiteren Verlauf werden Meldungen an relevante Empfänger verteilt, aufbereitet und in einem Dashboard visualisiert. Können aus eingegangenen Meldungen konkrete Gefahren für andere Unternehmen desselben oder eines anderen Sektors abgeleitet werden, werden in Zusammenarbeit mit dem IKDOK und der OpKoord Frühwarnungen erstellt und im Rahmen der gesetzlichen Möglichkeiten an potenziell betroffene Unternehmen und Organisationen verteilt. Gleichzeitig betreuen die Mitarbeiterinnen und Mitarbeiter der Meldesammelstelle auch den „Single Point of Contact“ als Anlaufstelle für NIS-Behörden anderer Mitgliedsstaaten der Europäischen Union. Diese Einrichtung spielt insbesondere im Zusammenhang mit der Kommunikation zwischen EU-Mitgliedstaaten bei grenzüberschreitenden Sicherheitsvorfällen eine entscheidende Rolle.

**Operative Koordinierungsstruktur.** „Der Schlüssel für nachhaltigen Erfolg bei der Erhöhung der Resilienz gegenüber Gefahren aus dem Cyber-Raum liegt in der Zusammenarbeit“, sagt Philipp Blauensteiner, geschäftsführender Leiter der Abteilung IV/10. Noch vor wenigen Jahren waren die Agenden zur Erhöhung der Cyber-Sicherheit auf eine Vielzahl von Ressorts und Organisationseinheiten verteilt, wobei ein Zusammenwirken nur rudimentär und punktuell zu beobachten war. Spätestens mit Inkrafttreten der ersten Österreichischen Strategie für Cyber-Sicherheit (ÖSCS) im Jahr 2013 fand hier ein grundlegendes Umdenken statt. Mit der Operativen Koordinierungsstruktur (OpKoord) versuchte man erstmalig, die Cyber-Sicherheitskräfte des Staates zu bündeln; ein Konzept, das sich als großer Erfolg herausstellen sollte.

**Vertrauensaufbau.** Doch bevor es soweit war, musste aus der Vielzahl der einzelnen beteiligten Bereiche eine Einheit geschaffen werden. Dies stellte ei-

**IKDOK**

## Staatliches Gremium

Der Innere Kreis der Operativen Koordinierungsstrukturen (IKDOK) ist ein staatliches Gremium, das auf Basis des NISG wirkt. Dem Gremium gehören neben der Abteilung IV/10 eine Reihe weiterer staatlicher Akteure an. Dazu zählen die Direktion für Staatsschutz und Nachrichtendienst (BMI/DSN), das Cybercrime Competence Center (BMI/BK), das Bundeskanzleramt (BKA) mit dem GovCERT, das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) sowie das Abwehramt, das Heeres-Nachrichtenamt und das IKT & Cybersicherheitszentrum (alle BMLV).

**Sicherheitsvorkehrungen: Betreiber kritischer Infrastruktur sind verpflichtet, technische und organisatorische Sicherheitsvorkehrungen zu treffen sowie schwere Sicherheitsvorfälle der NIS-Behörde im BMI zu melden.**

ne unerwartet große Herausforderung dar, da die einzelnen Organisationen aus unterschiedlichen Denkschulen stammten. Das Spektrum reichte dabei vom nationalen Computer-Notfallteam (CERT) mit einer ausgeprägten „Need-to-Share"-Herangehensweise, bis hin zum damaligen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), wo das „Need-to-Know"-Prinzip im Mittelpunkt jedweden Handelns stand. Diese Welten in Gleichklang zu bringen, erforderte in einem ersten Schritt einen nachhaltigen Vertrauensaufbau.

**Gesamtstaatliches Cyber-Lagebild.** Heute stehen alle Beteiligten innerhalb der Operativen Koordinierung (OpKoord) und ihres Inneren Kreises (IKDOK), darunter Vertreterinnen und Vertreter der Abteilung IV/10, zur Erfüllung ihrer Aufgaben in permanentem Kontakt. Mit wöchentlichen Abstimmungsterminen und anlassbezogenen Ad-hoc-Treffen arbeiten sie gemeinsam an der Erhöhung der Cyber-Sicherheit in Österreich. Als zentrales Produkt dieser Zusammenarbeit erstellen die Mitarbeiterinnen und Mitarbeiter der Abteilung ein monatliches, gesamtstaatliches Cyber-Lagebild, das dem gesetzlich definierten Empfängerkreis unmittelbar zugutekommt. Dazu verarbeiten sie Informationen zu aktuellen Sicherheitsvorfällen, konkreten Angriffsmustern sowie Warnungen vor entdeckten Schwachstellen und analysieren und bewerten diese. Wird ein schwerwiegender Cyber-Angriff auf eine Organisation aus diesem Bereich gemeldet, übernimmt die OpKoord die Koordination der Bewältigung dieses Angriffs und unterstützt die betroffene Organisation. Kommt es, wie Anfang des Jahres 2020 im Zuge des Angriffs auf das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA), zur Ausrufung einer nationalen Cyber-Krise, werden dazu alle verfügbaren Kräfte auch physisch zusammengezogen.

**Cyber-Prävention.** „Cyber-Sicherheit ist niemals nur die Aufgabe anderer", ist einer der Grundsätze von Martin Merka, der den Bereich der Cyber-Prävention innerhalb der Abteilung IV/10 verantwortet. Cyber-Sicherheit im beruflichen Alltag entsteht im kontinuierlichen Zusammenwirken zwischen den technischen Verantwortlichen und jeder und jedem einzelnen Mitarbeitenden in den Unternehmen und Organisationen, unabhängig von Rang und Funktion. Um diese Verantwortung wahrnehmen zu können, ist ein Bewusstsein für Gefahren im Cyber-Raum zwingend notwendig. Man spricht in diesem Zusammenhang von Cyber-Awareness. Die Mitarbeiterinnen und Mitarbeiter der Cyber-Prävention verfolgen, in permanentem Austausch mit technischen Fachexpertinnen und Fachexperten sowie OpKoord und IKDOK, die aktuelle Cyber-Lage und leiten daraus Vorsichtsmaßnahmen und konkrete Handlungsempfehlungen ab. Diese fließen in Schulungskonzepte, Vortragsunterlagen und Publikationen ein, die von der Abteilung regelmäßig erstellt und fortwährend aktualisiert werden.

Auf Basis dieser Materialien bietet die Abteilung IV/10 berechtigten Unternehmen und Organisationen Vorträge und Workshops für deren Mitarbeiterinnen und Mitarbeiter – vorzugsweise Multiplikatoren in ihren jeweiligen Bereichen – an. Bei der Planung solcher Veranstaltungen werden Verantwortliche der jeweiligen Unternehmen einbezogen, was die Möglichkeit bietet, individuell auf die konkreten Bedürfnisse der einzelnen Bedarfsträger einzugehen und maßgeschneiderte Informationen anzubieten. *M. M.*

FOTO: EGON WEISSHEIMER