Mehr Sicherheit durch klare Regeln

Mit dem Ende 2018 umgesetzten Netz- und Informationssystemsicherheitsgesetz soll ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und sichergestellt werden.

Das NIS-Gesetz ist ein erster wichtiger Schritt, um das Thema Cyber-Sicherheit in einen gesetzlichen Rahmen zu gießen“, sagt Mag. Gernot Goluch, Experte für Cyber-Sicherheit im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). Mit dem Netz- und Informationssystemsicherheitsgesetz (NISG) werden erstmalig in puncto Cyber-Sicherheit konkrete Vorgaben für bestimmte Bereiche der kritischen Infrastruktur getroffen. Gegenstand und Ziel des NISG sind die Festlegung von Maßnahmen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll. Das Gesetz richtet sich an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung. Die Adressaten des NISG sind verpflichtet, technische und organisatorische Sicherheitsvorkehrungen zu treffen und Sicherheitsvorfälle zu melden.

Wesentliche Dienste. Die Betreiber wesentlicher Dienste sind öffentliche oder private Einrichtungen aus den Bereichen Energie, Verkehr, Finanzmarktinfrastruktur, Bankwesen, Trinkwasserversorgung, Gesundheitswesen und digitale Infrastruktur. Das Bundeskanzleramt ermittelt für jeden Sektor diejenigen Betreiber mit einer Niederlassung in Österreich, die einen wesentlichen Dienst erbringen. Die Ermittlung erfolgt mittels Bescheid. Die betroffenen Unternehmen müssen mindestens alle drei Jahre nach Zustellung des Bescheids Sicherheitsvorkehrungen für die eigenen Netz- und Informationssysteme dem Bundesminister für Inneres nachweisen. „Das BMI ist ermächtigt, die Einhaltung der Anforderungen nachzuprüfen und an Ort und Stelle Einblick in die jeweiligen IKT-Systeme zu nehmen“, erklärt Goluch. Für operative Überprüfungen vor Ort sind Mitarbeiterinnen und Mitarbeiter des BVT, Abteilung 5 – Cyber-Sicherheit, zuständig.

Gernot Goluch: Betreiber wesentlicher Dienste müssen Cyber-Vorfälle melden.

Digitale Dienste. Bei den Anbietern digitaler Dienste handelt es sich um Unternehmen, die einen Online-Marktplatz, eine Online-Suchmaschine oder einen „Cloud-Computing-Dienst“ anbieten. „Unter Cloud-Computing-Diensten versteht man die Nutzung von IT-Infrastrukturen und IT-Dienstleistungen, die nicht auf lokalen Rechnern zur Verfügung stehen, sondern als Dienst gemietet werden und auf die über ein Netzwerk – beispielsweise das Internet – zugegriffen wird“, erläutert Goluch. Von der Regelung ausgenommen sind Kleinunternehmen, die weniger als 50 Mitarbeiterinnen und Mitarbeiter beschäftigen oder bei denen der jährliche Umsatz weniger als zehn Millionen Euro beträgt. Im Unterschied zu den Betreibern wesentlicher Dienste entfällt bei Anbietern digitaler Dienste die gesonderte Ermittlung durch Bescheid.

Meldepflicht. Bei Auftreten eines Sicherheitsvorfalles trifft die Betreiber wesentlicher und die Anbieter digitaler Dienste sowie die Einrichtungen der öffentlichen Verwaltung eine Meldepflicht. Die Unternehmen müssen die Meldung an das nationale oder – falls vorhanden – an das sektorspezifische Computer-Notfallteam („Computer Emergency Response Team“ – CERT) erstatten.

Das NISG schreibt vor, dass Meldungen zu Sicherheitsvorfällen unverzüglich zu erfolgen haben. In der Praxis würde das bedeuten, dass die betroffenen Unternehmen – nach kurzer Erstmeldung – die notwendigen Maßnahmen zur Abwehr oder Bekämpfung einer Cyber-Attacke einleiten können.

Zusätzliche Details und Informationen zum Sicherheitsvorfall müssen nach den Erstmaßnahmen nachgemeldet werden. Die bei dem zuständigen Computer-Notfallteam einlangenden Pflichtmeldungen sind in weiterer Folge durch dieses unverzüglich an das BVT, Abteilung für Cybersicherheit (Abt. II/BVT/5.3 NIS), weiterzuleiten.

Computer-Notfallteams. Für die öffentliche Verwaltung besteht das „Government-CERT“ *(GovCERT)* als sektorspezifisches Computer-Notfallteam. Die anderen Bereiche müssen sich an das nationale Computer-Notfallteam *(CERT.at)* wenden. Bei *CERT.at* handelt es sich um einen Ansprechpartner für IT-Sicherheit auf nationaler Ebene. *CERT.at* ist mit anderen *CERTs* und *CSIRTs* (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur und IKT auch auf europäischer Ebene vernetzt. Es werden Warnungen, Tipps und Hilfestellungen für österreichische Unternehmen zur Verfügung gestellt. Neben der Funktion als Informationsdrehscheibe liegt der Schwerpunkt eines *CERT* darin, Erste Hilfe zu leisten und Notfallmaßnahmen bei IKT-Vorfällen einzuleiten.

Interministerielle Zusammenarbeit. Um Sicherheitsvorfällen entgegenzuwirken und auf diese reagieren zu können, ist eine enge Zusammenarbeit innerhalb des „IKDOK“ (Innerer Kreis der operativen Koordinierungsstruktur) sowie der „Opkoord“ (operative Koordinierungsstruktur) notwendig. Der „IKDOK“ setzt sich aus Vertreterinnen und Vertretern des Innenministeriums, des Verteidigungsministeriums, des Bundeskanzleramtes und des Außenministeriums zusammen. In der „Opkoord“ kommen anlassbezogen der „IKDOK“, die Computer-Notfallteams sowie Vertreter der Adressaten des NISG (z. B. Betreiber wesentlicher Dienste) zusam-

Fotos: Gernot Burkert

men. Beispielsweise bei einem groß angelegten Cyber-Angriff auf Sektoren der kritischen Infrastruktur, etwa auf Energie, Gesundheit oder Trinkwasserversorgung.

Cyber-Angriffe. Diese Zusammenarbeit hat beispielsweise 2017 im Zuge der internationalen „NotPetya"-Angriffswelle gut funktioniert. Während damals die Schäden, die die Schadsoftware „WannaCry" europaweit verursachte, noch nicht vollständig behoben werden konnten, startete am 27. Juni 2017 mit der Verschlüsselungssoftware (Ransomware) „NotPetya" eine neuerliche Welle von Cyber-Angriffen. Die Schadsoftware wurde in diesem Fall durch kompromittierte Softwareupdates einer legitimen Software verbreitet, die für das Verfassen von ukrainischen Steuererklärungen verwendet wurde. Europa- und weltweit wurden zahlreiche Unternehmen durch die Schadsoftware infiziert.

Bald stellte sich heraus, dass von der Infektion mit der Schadsoftware lediglich jene Unternehmen betroffen waren, die geschäftliche Verbindungen zur Ukraine unterhielten. Der Aufbau und die Funktion der Schadsoftware in diesem Fall deuteten vielmehr auf die gezielte Sabotage der Infrastruktur eines Landes (Ukraine) und weniger auf eine Bereicherungsabsicht der Täter hin.

„Wie bei WannaCry war bei NotPetya die Mehrzahl der Angriffsvektoren seit Monaten bekannt. Ein fehlendes Patchmanagement sowie ein mangelhaftes Update-Bewusstsein führten zu einer enormen Anzahl an Infektionen", erläutert Goluch.

Bewältigung von Angriffen. Für Österreich stellt das Auftreten von „NotPetya" eine Zäsur im Rahmen der staatlichen Reaktion auf derartige Schadsoftwarewellen dar. Diese Welle wurde von ihrem ersten Auftreten bis zur Bewältigung vom „IKDOK" koordiniert. Dabei zeigte sich, dass zur Erkennung und Bewältigung derartiger Bedrohungslagen ein zentrales staatliches Gremium von großer Bedeutung ist. Während einzelne Unternehmen oder branchenspezifische Gremien lediglich einen Ausschnitt der Situation beobachten können, war es dem Cyber-Security-Center im BVT gemeinsam mit dem IKDOK möglich, die Lage ganzheitlich zu erfassen und schnell entsprechende Schritte zu setzen (erster Hinweis um 15:16 Uhr, detailliertes Warnschreiben mit Lageeinschätzung und Handlungsempfehlungen um 18:05 Uhr).

Das NISG soll diese Kooperationen zusätzlich auf sichere rechtliche Beine stellen. Darüber hinaus regeln die datenschutzrechtlichen Bestimmungen, welche Informationen mit wem geteilt werden dürfen.

Ein wesentlicher Unterschied zur Vergangenheit liegt darin, dass die Betreiber wesentlicher Dienste nun dazu verpflichtet sind, Sicherheitsvorfälle zu melden. „Neben der Pflicht zur Meldung von Vorfällen wurde auch das Recht zur Meldung von Vorfällen im Gesetz verankert. Dieses Recht kann im Rahmen einer freiwilligen Meldung in Anspruch genommen werden und soll den Informationsaustausch im Bereich der Cyber-Sicherheit in Österreich verbessern", sagt der Cyberexperte.

„Eine fundierte Dokumentation von Cyber-Angriffen und Cyber-Vorfällen ist für das betroffene Unternehmen wie auch für die Allgemeinheit von großer Bedeutung", erläutert Goluch. Die Meldung von Sicherheitsvorfällen an Behörden sei unerlässlich, wenn es darum geht, ein klares Lagebild in puncto Cybersicherheit und Internetkriminalität für den Wirtschaftsstandort Österreich und die österreichische Gesellschaft zu zeichnen. „Nur so sind die zuständigen behördlichen Stellen in der Lage, bessere Unterstützungsmöglichkeiten für angegriffene Unternehmen zu schaffen."

Betreiber wesentlicher Dienste müssen alle drei Jahre einen Nachweis über Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme im Innenministerium einbringen.

Sanktionen. Sollten die vom NISG betroffenen Unternehmen gegen die Meldepflicht, die Umsetzung von Sicherheitsvorkehrungen oder die Mitwirkungspflicht verstoßen, müssen sie mit verwaltungsstrafrechtlichen Sanktionen rechnen. Der Bundesminister für Inneres kann die Umsetzung von Sicherheitsvorkehrungen bei Betreibern wesentlicher Dienste und Anbietern digitaler Dienste mittels Bescheid anordnen. Die Verwaltungsstrafen bei derartigen Verstößen können bis zu 50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro ausmachen. Zuständig für das Verwaltungsstrafverfahren ist die jeweilige Bezirksverwaltungsbehörde. „Es bleibt abzuwarten, wie sich der Schutz vor Cyber-Angriffen und die Vorsorge in puncto Cybersicherheit in Zukunft verbessert und ob sich die neu geschaffenen Strukturen, Möglichkeiten und Meldepflichten bewähren werden", sagt DI Philipp Blauensteiner, Leiter des Cyber Security Centers im BVT (II/BVT/5.1 CSC). Philipp Blauensteiner ist „Certified Information System Security Professional" (CISSP).

Gernot Goluch hat sein Studium an der Technischen Universität Wien absolviert. Er war in den letzten 13 Jahren in unterschiedlichen Funktionen und Bereichen der Informationssicherheitsbranche tätig. (Audits & Prüfungen, sichere Softwareentwicklung, Sicherheitsarchitekturen, Policies und Richtlinien, Schulungen etc.) Derzeit befasst sich Goluch in der Abteilung für Cyber-Sicherheit (Referat 5.3 NIS) im BVT mit den Aufgabenbereichen der operativen NIS-Behörde (u. a. Meldesammelstelle, Prüfung der Sicherheitsvorkehrungen, EU Single-Point-of-Contact). *Gernot Burkert*

FOTO: EGON WEISSHEIMER