Sicherheit erhöhen

Was wäre, wenn man einen Notruf der Polizei, Rettung oder Feuerwehr wählte, aber die Leitung tot wäre? Ein Totalausfall der Telekommunikation könnte zu unabsehbaren Folgen für die Menschen im Land führen.

Kriminelle drangen im Dezember 2019 mit einem Schadprogramm in das Netz des Telekommunikationsanbieters *A1* ein. Die Schadsoftware wurde vom *Computer Emergency Response Team (CERT)* von *A1* entdeckt. Die IT-Experten von *A1* hatten neben Meldungen an die NIS-Behörde im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) und die Datenschutzbehörde herauszufinden, worauf die Angreifer es abgesehen hatten. Mehr als 12.000 Server, rund 15.000 Computer sowie mehrere Tausend Applikationen mussten geschützt werden. Über die Netze von *A1* werden beispielsweise Transaktionen von Banken abgewickelt, das Gesundheitsnetz mit der E-Card sowie die Notrufnummern von Polizei, Rettung und Feuerwehr betrieben. Auch der reibungslose Betrieb von Unternehmen der kritischen Infrastruktur – die *A1*-Kunden sind – musste sichergestellt werden. Der Angriff wurde nach sechs Monaten beendet. Dazu wurden alle Kennwörter auf „Ungültig“ gesetzt, damit es für die Täter keine Möglichkeit mehr gab, sich zu verstecken.

„Gut, dass wir das NIS-Gesetz haben. Speziell die Möglichkeit der freiwilligen Meldung von Vorfällen ist ein wichtiger Punkt. Experten des BVT haben uns bei der Beurteilung der Lage und bei der Bewältigung des Angriffes unterstützt. Ein großer Spagat dabei ist das gleichzeitige Weiterarbeiten gewesen, um die Kommunikation im Land aufrecht erhalten zu können, und die Bekämpfung des Cyber-Angriffes“, schilderte Dr. Wolfgang Schwabl von *A1* beim „Sicherheitsforum Digitale Wirtschaft“ am 4. September 2020 im Innenministerium. „Wir haben den Angriff erfolgreich abgewehrt und viel gelernt über die Methoden der Angreifer. Dieses Wissen möchten wir gerne mit anderen großen Betreibern kritischer Infrastruktur teilen, um den österreichischen Wirtschaftsraum gemeinsam zu stärken und vor Cyber-Angriffen zu schützen.“

NIS-Gesetz. Der Cyber-Raum bietet eine Vielzahl von Chancen und Möglichkeiten. Um die Vorteile in einer globalisierten Welt zu nutzen, muss die dahinterstehende, digitale Infrastruktur zuverlässig funktionieren und hohe Sicherheit bieten. Die Gewährleistung von Cyber-Sicherheit ist eine der Prioritäten Österreichs und eine gemeinsame Herausforderung für Politik, Wirtschaft und Gesellschaft. Das mit Ende 2018 umgesetzte Netz- und Informationssystemsicherheitsgesetz (NISG) stellt einen wesentlichen Schritt zur Erhöhung der Cyber-Sicherheit dar. Die Betreiber wesentlicher Dienste (Energieversorgung, Gesundheitswesen, Bankwesen), digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen) und die öffentliche Verwaltung müssen aufgrund der Vorgaben des NISG fortlaufend technische und organisatorische Sicherheitsvorkehrungen treffen und Sicherheitsvorfälle melden. Diese Vorgaben betreffen auch die Informations- und Kommunikationstechnologie des Innenressorts.

Meldepflicht: Betreiber kritischer Infrastruktur müssen Sicherheitsvorfälle dem verantwortlichen Computer-Notfallteam melden.

Sicherheitsvorkehrungen im BMI. Mit dem NIS-Programm werden Sicherheitsvorkehrungen erarbeitet, die eine Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Netz- und Informationssysteme des BMI verhindern sollen. Ein eigenes Computer-Notfallteam (CSIRT-BMI) soll schnell auf Risiken und Sicherheitsvorfälle reagieren können. Die Zuverlässigkeit, Verfügbarkeit, Integrität und Vertraulichkeit der vom BMI betriebenen Systeme spielen für alle Organisationseinheiten des Ressorts eine wichtige Rolle.

IKT-Sicherheit. Eine gut funktionierende Informations- und Kommunikationstechnik (IKT) ist wichtiger Bestandteil einer jeden funktionierenden Infrastruktur. Durch technische Hilfsmittel lassen sich viele Aufgaben schnell und effizient erledigen – man denke an die elektronische Arbeitszeiterfassung oder an die Möglichkeit, mit einem dienstlichen Laptop (m-Baks) an jedem Ort der Welt und jederzeit in das BMI-Netzwerk einsteigen zu können – so als säße man am eigenen Arbeitsplatz.

Diese Vorteile bringen jedoch auch Risiken mit sich: Ungesicherte Netzwerke oder IKT-Infrastruktur können ein Einfallstor für Kriminelle und Hacker sein. Ein Ausfall aller IKT-Systeme im BMI hätte weitreichende Konsequenzen. Eine Abfrage im elektronischen kriminalpolizeilichen Informationssystem (EKIS) wäre nicht mehr möglich – was bedeuten würde, dass eine Polizistin oder ein Polizist bei einer Personenkontrolle einen flüchtigen Straftäter, der zur Fahndung ausgeschrieben ist, nicht mehr identifizieren könnte. Auch andere Behörden oder Institutionen hätten keinen Zugriff mehr auf wichtige Datenbanken, wie das zentrale Melderegister oder das Kfz-Zulassungsregister. Um solche weitreichenden Folgen so weit wie möglich ausschließen zu können, ist es erforderlich die IKT-Systeme zu schützen und diese widerstandsfähiger gegenüber Angriffen von Kriminellen und Cyber-Angriffen zu machen.

Mitarbeiter sensibilisieren. Der Faktor Mensch spielt bei Cyber-Kriminalität eine häufig unterschätzte Rolle. Die Abgelenktheit der Mitarbeiterinnen und Mitarbeiter oder die Selbstüberschätzung, multitaskingfähig zu sein, führen häufig zu Fehlentscheidungen, die für ein Computersystem oder Netzwerk eines Unternehmens weitreichende negative Folgen haben können. Denn solche Fehlentscheidungen ermöglichen es den Kriminellen, Zugang zu einem Unternehmen zu bekommen.

FOTO: GERD PACHAUER

„Die Mitarbeiterinnen und Mitarbeiter müssen deshalb laufend über neue Formen der Bedrohung durch Schadsoftware, über neue Phishing-Methoden und im verantwortungsbewussten Umgang mit dem Internet geschult werden. Darüber hinaus kann nicht oft genug betont werden, dass E-Mails von unbekannten Absendern mit diversen Dateianhängen nicht einfach geöffnet werden sollten – das gilt für den dienstlichen wie auch für den privaten Bereich gleichermaßen“, erläutert Mag. Gernot Goluch, Cyber-Sicherheitsexperte im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT).

Interministerielle Zusammenarbeit. Um Sicherheitsvorfällen entgegenzuwirken und auf diese reagieren zu können, ist eine enge Zusammenarbeit des inneren Kreis der operativen Koordinierungsstrukturen (IKDOK) sowie der „Opkoord“ (operative Koordinierungsstruktur) notwendig. Der „IKDOK“ setzt sich aus 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) zusammen. Beispielsweise bei einem groß angelegten Cyber-Angriff auf Sektoren der kritischen Infrastruktur, etwa auf Energie, Gesundheit oder Trinkwasserversorgung.

Cyber-Security-Center (CSC). Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung übernimmt mit dem CSC eine zentrale Rolle bei der Umsetzung der Vorgaben des NISG. Darunter fallen die Einrichtung und der Betrieb der operativen NIS-Behörde und der zentralen Anlaufstelle, die Leitung der „IKDOK“ und der „Opkoord“, Befugnisse und Datenverarbeitung einschließlich des Betriebs eines IoC-basierten Frühwarnsystems. Beim *Indicator of Compromise (IoC)* handelt es sich um Merkmale und Daten, die auf die Kompromittierung eines Computersystems oder Netzwerks hinweisen. Merkmale können beispielsweise Einträge in Logfiles, außergewöhnlicher Netzwerkverkehr, bestimmte Dateien, einzelne Prozesse, Registry-Einträge oder Aktivitäten unter einer Benutzerkennung sein. Die Kompromittierungsindikatoren lassen sich in eine strukturierte Form bringen und automatisiert auswerten.

Sicherheitsvorkehrungen im BMI: Ein eigenes Computer-Notfallteam (CSIRT-BMI) soll schnell auf Risiken und Sicherheitsvorfälle im BMI reagieren können.

FOTO: GERD PACHAUER

Meldeverpflichtung. Bei Auftreten eines Sicherheitsvorfalles trifft die Betreiber wesentlicher Dienste, die Anbieter digitaler Dienste aber auch die Einrichtungen der öffentlichen Verwaltung eine Meldepflicht. Und zwar an das verantwortliche Computer-Notfallteam (CERT). Das Government Computer Emergency Response Team (GovCERT) ist verantwortlich für die Entgegennahme von Meldungen über Risiken, Vorfälle und Sicherheitsvorfälle bei Einrichtungen der öffentlichen Verwaltung.

Bewältigung von Cyber-Angriffen. Österreichweit kommt es tagtäglich zu vielen Cyber-Angriffen. „Im BVT arbeiten Expertinnen und Experten des Cyber-Security-Centers täglich daran, die Sicherheit und Widerstandsfähigkeit von Betrieben und Einrichtungen kritischer Infrastruktur zu gewährleisten. Zur Bewältigung von Cyber-Krisen wurde ein Cyber-Krisenmanagement (CKM) eingerichtet, die Arbeitsweise orientiert sich dabei am staatlichen Krisen- und Katastrophenschutzmanagement“, sagt DI Philipp Blauensteiner, Leiter des Cyber-Security-Centers im BVT. *Gernot Burkert*

NIS-Behörde: NIS@bvt.gv.at.

FACHKONFERENZ

Personenschutz und Unternehmenssicherheit

In der Burg Deutschlandsberg in der Steiermark findet am 23. und 24. März 2021 die erste Fachkonferenz „Personenschutz und Unternehmenssicherheit“ statt. Zielgruppe sind Führungskräfte Personenschutz, Leiter Unternehmenssicherheit/Sicherheitsverantwortliche, Private Sicherheitsdienstleister/-Unternehmen.

In der Konferenz geht es unter anderem um Kommunikative Deeskalation, Politik und Medien, Covid-19: Die Pandemie unter dem Blickwinkel strategischer Entscheidungen, Korruption und Sicherheit – fahrlässig vernachlässigt? Psychische und physische Auswirkungen einer Geiselnahme für die Geisel und deren familiäres und soziales Umfeld.

Vortragende sind unter anderem: Martin Kreutner, Dekan Emeritus der International Anti-Corruption Academy (IACA), Michael Novotny, Jagdkommando, Dr. Clemens Wissiak, Facharzt für Unfallchirurgie & Orthopädie, Thomas Greis, Bundesministerium für Inneres, Thomas Lay, Sicherheitsexperte, Michael Fleischhacker, Journalist, Markus Schimpl, Sicherheitsberater und Personenschutzexperte. Anmeldeschluss ist der 31.12.2020. Weitere Informationen: *www.ichrettemich.com*.