Der Faktor Mensch

Technische Cybersicherheitsmaßnahmen nützen wenig, wenn das Gefahren-Bewusstsein bei den Mitarbeitenden fehlt. Mitarbeiter des Fachbereichs Prävention der NIS-Behörde im Bundesministerium für Inneres informieren über Gefahren und Sicherheitsmaßnahmen.

Die Frage, ob das eigene Unternehmen Ziel eines Cyberangriffes werden könnte, steht heute nicht mehr zur Diskussion, sondern die Frage, wann es passieren wird", sagt Philipp Blauensteiner, Leiter der Abteilung für Netz- und Informationssystemsicherheit (NIS) im Bundesministerium für Inneres. In seiner Abteilung ist die Funktion der nationalen Behörde für Netz- und Informationssystemsicherheit in Österreich angesiedelt.

Technische und organisatorische Cybersicherheit. Um Cybersicherheit in einem Unternehmen oder in einer Organisation sicherstellen zu können, sind Maßnahmen in mehreren Bereichen erforderlich. Grundlegendes Element jedes Sicherheitskonzepts ist die technische Cybersicherheit. Konzepte, wie Endpoint Protection oder Intrusion Detection- und Firewallsysteme werden in der Regel in Fachabteilungen umgesetzt, die finanziell und personell gut ausgerüstet sein müssen. Gleichzeitig ist die organisatorische Cybersicherheit von großer Bedeutung. Sie ist für die rasche Erkennung und die richtige Reaktion auf Sicherheitsvorfälle entscheidend. In diesem Zusammenhang sind entsprechende Prozesse zu implementieren und regelmäßig zu beüben. Dafür ist das größtmögliche Committment der Leitungsebene von Bedeutung. Doch können diese beiden Bereiche allein keinen ausreichenden Schutz bieten.

Der Faktor Mensch ist ein wesentliches Element bei der Sicherstellung von Cybersicherheit", sagt Andreas Wimmer, Referatsleiter in der Abteilung für Netz- und Informationssystemsicherheit. Technische und organisatorische Maßnahmen können ihre Wirkung nur entfalten, wenn sich die Anwender/-innen der Cyber-Gefahren bewusst sind und sich entsprechend verhalten. Sorglosigkeit aufgrund fehlenden Problembewusstseins, das ausschließliche Vertrauen auf technische Schutzmaßnahmen oder die Ablehnung von Mitverantwortung für die Sicherstellung von Cybersicherheit sind Themen, mit

Jede und jeder Mitarbeitende ist Teil der Cybersicherheit

denen sich Unternehmen und Organisationen auseinandersetzen müssen.

Awareness als Schlüssel zur Sicherstellung von Cybersicherheit wurde im Bundesministerium für Inneres früh erkannt. Auf Basis der „Österreichischen Strategie für Cybersicherheit" wurden Konzepte erarbeitet, wie Mitarbeiterinnen und Mitarbeiter von Unternehmen und Organisationen, die der Daseinsvorsorge der Bevölkerung dienen, bestmöglich für die Gefahren im Cyberraum sensibilisiert werden können. Der Fachbereich Prävention in der NIS-Behörde in Österreich wurde 2016 als Initiative des *Cyber-Security-Centers* im damaligen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung eingeführt. Zielgruppe waren die kritische Infrastruktur gemäß *APCIP (Austrian Program Critical Infrastructure Protection)* und die verfassungsmäßigen Einrichtungen in Österreich. Mit der Reformierung des Verfassungsschutzes und der damit verbundenen Einrichtung der Direktion Staatsschutz und Nachrichtendienst (DSN) wurde die Prävention als Teil der NIS-Behörde für Österreich in der Sektion IV (IT und Service) des BMI als eigenverantwortlicher Fachbereich auf neue Beine gestellt.

Fachbereich Prävention als Teil der NIS-Behörde. Das Hauptaugenmerk des Fachbereichs Prävention liegt auf den dem NIS-Gesetz (NISG) unterworfenen Einrichtungen, wie z. B. Betreibern wesentlicher Dienste oder Einrichtungen der öffentlichen Verwaltung. Darüber hinaus besteht weiterhin ein Angebot an die Unternehmen und Organisationen der kritischen Infrastruktur in Österreich. Neben den „klassischen" Kritis-Unternehmen gemäß APCIP bzw. NISG (z. B. Energieunternehmen, Verkehrsbetriebe, Gesundheitseinrichtungen, Finanzeinrichtungen) liegen staatliche Institutionen im Fokus der Maßnahmen (z. B. Parlament, Ministerien, Landesregierungen, Behörden, Rechnungshof). Der Fachbereich beteiligt sich mit Vorträgen und Workshops an Kampagnen zu Cybersicherheit (z. B. Schützenswertes Krankenhaus, Haus der Digitalisierung, Hostile Environment Awareness Training).

Ziel der Veranstaltungen des Fachbereichs Prävention ist es, in Vorträgen und Workshops die Awareness von Mitarbeiter/-innen zu erhöhen und die Resilienz gegenüber Cyber-Bedrohungen zu stärken. Die Basis bilden Themen wie Kennwortsicherheit, Verschlüsselung von Datenträgern und verschlüsselte Nutzung von Diensten sowie das sichere Löschen von Daten. Es wird die Funktionsweise unterschiedlicher Schadsoftware erläutert sowie typische Infektionswege, wie E-Mails mit manipulierten Anhängen oder Hyperlinks zu bösartigen Zielen dargestellt. Besonderes Augenmerk wird auf die Erkennung von Bedrohungen und das richtige Verhalten in diesen Fällen gelegt. Inhaltlich abgerundet wird das Thema mit einer Sensibilisierung für jeweils aktuelle Schadsoftware-Kampagnen, mit Informationen zum richtigen Umgang mit potenziell gefährlicher Hardware sowie mit Ausführungen zu Cybersicherheit auf Dienstreisen und bei der Nutzung mobiler Endgeräte.

„Umfassende Cybersicherheit entsteht aus dem kontinuierlichen Zusammenwirken zwischen den technischen Verantwortlichen und jeder und jedem einzelnen Mitarbeitenden in den betroffenen Unternehmen und Organisationen, unabhängig von Rang und Funktion", sagt Martin Merka, verantwortlicher Hauptreferent für den Fachbereich Prävention. *M. M.*

FOTO: VIDEOFLOW - STOCK.ADOBE.COM