Helpline bei Cybercrime

Die Zahl der Cybercrime-Delikte stieg in Wien 2017 etwa um ein Drittel gegenüber 2016. Da viele Unternehmen betroffen waren, richtete die Wirtschaftskammer Wien eine Hotline ein.

Etwa ein Drittel aller in Österreich 2017 angezeigten Fälle von Cyber-Kriminalität (16.804) betraf Wien (5.596). Stark von Cybercrime betroffen waren Unternehmen. Daher richtete die Wirtschaftskammer Wien eine Cybercrime-Security-Helpline ein. Die Hotline 0800 888 133 ist 24 Stunden am Tag besetzt ist. Acht zertifizierte Unternehmen bieten Firmen im Schadensfall Hilfe und vermitteln Spezialisten.

Angriffe auf Unternehmen erfolgen laut Harald Wenisch, IT-Sicherheitsexperte und Sprecher der IT Security Experts Group der Wirtschaftskammer, häufig über E-Mails, Webbrowser, das Netzwerk, Social Engineering und Datenträger wie USB-Sticks. Unternehmen werden immer öfter von Ransomware bedroht, einer Schadsoftware, die Daten verschlüsselt und für deren Entschlüsselung die Kriminellen ein „Lösegeld“ (Ransome) verlangen. Weitere „Angriffswerkzeuge“ seien laut Wenisch Betrug und Phishing. Klein- und Mittelbetriebe und Unternehmensbereiche wie die Personalabteilung und der Vertrieb seien davon besonders betroffen. Mitarbeiter seien gewohnt, unterschiedliche

Leopold Löschl, Martin Puaschitz, Martin Heimhilcher und Harald Wenisch präsentieren die neue Cybersecurity-Hotline der Wirtschaftskammer Wien.

Beilagen zu öffnen und auf Links zu klicken, da sie regelmäßig E-Mails von fremden Personen erhielten. Laut Mag. Leopold Löschl, Leiter des Cybercrime-Competence-Centers (C4) im Bundeskriminalamt, werden die Täter „immer einfallsreicher und professioneller“. Phishing-Mails zum Beispiel waren früher aufgrund von Sprach- und Rechtschreibfehlern leicht zu erkennen. Heute seien Mails zum „Abfischen“ von Daten professioneller. Kriminelle versuchen, ihre Opfer in Stress zu versetzen, indem sie etwa Mails kurz vor Büroschluss verschicken.

Anzeigen und sensibilisieren. Martin Puaschitz, Obmann der Fachgruppe UBIT Wien – Unternehmensberatung, Buchhaltung und Informationstechnologie, rät, alle Vorfälle anzuzeigen. Firmen würden das oft nur dann tun, wenn eine Versicherung eine Anzeige fordert. Die Anzeigenmotivation sei nicht sehr hoch, bestätigt C4-Leiter Leopold Löschl. Er rät, jeden Cybercrime-Fall bei der Polizei anzuzeigen. Puaschitz empfiehlt, Mitarbeiter für Cyber-Sicherheit zu sensibilisieren. Software, Antivirenprogramme und Firewalls sollten immer auf dem letzten Stand sein.

Hilfe bei Entschlüsselungsprogrammen bietet die Webseite *www.nomoreransom.org*. Sie ist von Europol in Kooperation mit dem Bundeskriminalamt sowie privaten und exekutiven Partnern entstanden und unterstützt Opfer digitaler Erpressungen bei der Wiederherstellung ihrer Daten.

Die Cybercrime-Meldestelle im Bundeskriminalamt ist unter *against-cybercrime@bmi.gv.at* erreichbar. Weitere Sicherheitstipps gibt es unter *www.bundeskriminalamt.at*.

CYBERCRIME-BEKÄMPFUNG

Kompetenzen bündeln

Dr. Philipp Amann, Direktor der Cyber-Security-Abteilung von EUROPOL, referierte am 28. Mai 2018 im Kabinett des Bundesministeriums für Inneres vor wichtigen Entscheidungsträgern und Experten über seine Erfahrungen und Einschätzungen zu aktuellen Bedrohungslagen.

Enge Zusammenarbeit. Kabinettschef Ing. Mag. Reinhard Teufel betonte einleitend die Notwendigkeit einer engeren Zusammenarbeit aller im Bereich Cybersecurity tätigen Akteure. Die digitale Revolution habe alle Lebensbereiche erfasst und stelle nicht nur das Innenministerium vor große Herausforderungen. „Die Bevölkerung hat nur eine eingeschränkte Möglichkeit zum Selbstschutz in einer digitalisierten

Impulsveranstaltung zu Cybersecurity: Kabinettschef Reinhard Teufel, Europol-Abteilungsleiter Philipp Amann.

Welt. Sie erwartet sich daher vom Staat professionelle Sicherheitslösungen“, sagte Teufel. Die österreichische Bundesregierung habe die Themen Cybercrime und Cybersecurity zu Schwerpunkten erklärt. Ziele seien die Verbesserung der Rahmenbedingungen, die Schließung digitaler Sicherheitslücken sowie die Förderung digitaler Freiheit und Selbstbestimmung. Der Kabinettschef zitierte dabei aus dem Regierungsprogramm: „In Österreich sind die Kompetenzen im Bereich der digitalen Sicherheit zu bündeln und eine Strategie zur digitalen Sicherheit zu erarbeiten.“ Dazu bedürfe es aber sowohl entsprechender Expertise als auch organisatorischer Strukturen, sagte Teufel, der Amanns Vortrag als wichtige Impulsveranstaltung auf dem Weg dorthin wertete.

Die Ausführungen des EUROPOL-Vertreters fanden großen Anklang im Auditorium. Die Anwesenden nutzten die Gelegenheit für einen fruchtbaren Erfahrungsaustauch und kamen überein, die Kontakte zueinander zu vertiefen, um dem komplexen und vielschichtigen Thema Cyber-Kriminalität wirksamer zu begegnen.

Fotos: BMI, Florian Wieser