Gefahr im Cyberspace

Das Führungsforum Innovative Verwaltung befasste sich in einer Online-Veranstaltung mit dem Thema Cybercrime und beleuchtete die Arbeit des Bundeskriminalamtes.

Wie schnell man zum Opfer von Cyber-Kriminalität werden kann und welche Maßnahmen im Kampf gegen Hacker und Datendiebe von Polizei und Verwaltung gesetzt werden, war Inhalt eines Themenforums des *Führungsforums Innovative Verwaltung (FIV)* am 19. Jänner 2022.

Gemeindeamt erpresst. Gerald Wonner, Bürgermeister der Gemeinde Gössendorf bei Graz, berichtete als Betroffener davon, wie die Gemeinde-EDV am Wochenende vom 24. auf den 25. April 2021 gehackt wurde: „Innerhalb von zwei bis drei Stunden wurden alle unsere Daten verschlüsselt. Die Gemeindeserver sind lahmgelegen, E-Mails und Akten waren nicht mehr verfügbar.“ Vier Terabyte waren insgesamt betroffen; auch die Schließsysteme der Gemeindegebäude konnten nur noch manuell bedient werden.

Bald war klar, dass es sich um einen Erpressungsfall handelte: Die Hacker hatten ein Textfile mit Informationen im Netzwerk hinterlassen und stellten ihre Forderungen. Gegen Zahlung eines Betrages von 10.000 Euro in Kryptowährung würden sie die Daten wieder entschlüsseln. „Die Täter haben einen professionellen Support aufgezogen und waren quasi rund um die Uhr erreichbar. Sie haben auch gezeigt, dass sie in der Lage sind, die Daten wieder zugänglich zu machen“, schilderte Wonner.

Bei der Meldung der Straftat bei der Polizei stieß der Bürgermeister auf für ihn unklare Zuständigkeiten: An sich war für Gössendorf die Polizeiinspektion (PI) Hausmanstätten verantwortlich, Cyber-Kriminalfälle wurde aber von der benachbarten PI in Kalsdorf bearbeitet. Schließlich wurde auch das Landeskriminalamt Steiermark eingeschaltet. „Ein einheitlicher Ansprechpartner hätte die Sache am Anfang leichter gemacht“, sagte Wonner. Obwohl die Gemeinde Gössendorf in moderne Technik investiert und ihr Netzwerk mit einem professionellen IT-Betreuer abgesichert hatte, waren die Täter über genau diesen Netzwerk-Administrator auf eine geeignete Schwachstelle gestoßen:

Gerald Wonner: „E-Mails und Akten waren nicht mehr verfügbar.“

Über seine Zugangsrechte gelangten die Hacker unbemerkt ins System, verschafften sich über Wochen einen Überblick und bereiteten nach und nach ihren Angriff vor. „In den letzten vier Tagen vor der Verschlüsselung waren sie am aktivsten. Sie haben die Firewall ausgeschaltet, Trojaner in unterschiedlichsten Verzeichnissen platziert und konnten dann eigentlich auf Knopfdruck alles herunterfahren“, berichtete Wonner. In Abstimmung mit dem Gemeindevorstand entschloss sich der Bürgermeister schließlich dazu, auf die Erpressung einzugehen – über mehrere Monate waren nämlich keine Backups mehr erstellt worden. Viele Daten wären unwiederbringlich verloren gewesen. Die Geldforderung konnte auf 8.000 Euro heruntergehandelt werden, die Kryptowährung „Monero“ musste über einen Zwischenhändler in Belgien beschafft werden. Das Lösegeld, das rasch bereitstehen musste, bezahlte Wonner vorerst aus der eigenen Tasche: „Wenn die Hacker uns getäuscht hätten, wäre der Verlust bei mir hängen geblieben.“ Letztlich lieferten die Täter die Entschlüsselungs-Software und über das Wochenende konnten die Daten wieder zugänglich gemacht werden. „Rund zwei Wochen später waren wir wieder vollständig funktionstüchtig und online. Wir sind mit einem blauen Auge davongekommen.“

Den vorfinanzierten Betrag erhielt Wonner später aus der Gemeindekasse zurück. Wer hinter dem Cyber-Angriff steckte, ist bis heute ungeklärt. Inzwischen hat die Gemeinde das IT-Unternehmen gewechselt und ihre Daten zusätzlich mit Cloud-Lösungen gesichert. Über den Vorfall hat der Bürgermeister immer offen kommuniziert, lokale Medien berichteten über die gehackte Gemeinde. Diese Transparenz war ein wichtiges Kriterium für die Datenschutzbehörde, die den „Data Breach“ – also den Umstand, dass personenbezogene Daten trotz Schutzmaßnahmen in unbefugte Hände geraten waren – zu prüfen hatte. Da alle Betroffenen von der Gemeinde ausreichend über die Datenpanne informiert worden waren, stellte die Datenschutzbehörde schließlich ihr Prüfungsverfahren ein.

Bundeskriminalamt. „Solche Vorfälle passieren leider wöchentlich, oft sogar mehrmals pro Woche“, bekannte Erhard Friessnik, Leiter des *Cybercrime-Competence-Center (C4)* im Bundeskriminalamt. Verschiedene Unternehmen und Institutionen seien in Österreich in letzter Zeit zu Opfern geworden. „Kaum ein anderes Kriminalitätsfeld boomt im Moment so wie Cybercrime.“ 2011 habe man in Österreich rund 5.000 Delikte an Cyber-Kriminalität verzeichnet, fünf Jahre später waren es bereits 30.000, 2020 wurden

FOTO: SISSI FURGLER FOTOGRAFIE

FIV

Vernetzung der Verwaltung

Das *Führungsforum Innovative Verwaltung (FIV)* ist ein 1999 gegründeter Verein mit mehr als 200 Mitgliedern aus allen Gebietskörperschaften. Es handelt sich um Führungskräfte von Bund, Ländern, Städten und Gemeinden sowie von öffentlichen Unternehmen, die sich überparteilich und unabhängig zusammengeschlossen haben.

In den Themenforen des *FIV* werden mit Hilfe von Expertinnen und Experten Themen mit Bedeutung für die Verwaltung wie die Digitalisierung, der demografische Wandel, die Ressourcenknappheit und andere Entwicklungen im öffentlichen Sektor behandelt. Innovationen durch zukunftsorientierte Technologien und moderne Managementmethoden sollen durch die Vernetzung im *FIV* vorangetrieben werden.

www.fiv.at

knapp 40.000 Cyber-Delikte registriert. „Dabei handelt es sich allerdings nur um die tatsächlich angezeigten Fälle, die Dunkelziffer ist deutlich höher“, meinte Friessnik. Allein 13.000 Fälle betrafen im Jahr 2020 Hackerangriffe und Erpressungen nach Datenverschlüsselungen mit sogenannter „Ransomware“, so wie im Fall von Gössendorf bei Graz. Die Corona-Pandemie habe das Cybercrime-Phänomen weiter vorangetrieben.

Cyber-Crime-Competence-Center. Bereits 2011 rüstete sich das Bundeskriminalamt mit der Einrichtung eines *Cyber-Crime-Competence-Centers (C4)* gegen die neuen Kriminalitätsformen. Seither wurde es mehrmals erweitert; im November 2021 übersiedelte es in neue Räumlichkeiten in Wien-Leopoldstadt, die auch eine personelle Erweiterung ermöglichen.

Das *C4* als Büro 5.2 des Bundeskriminalamtes ist in drei Referate gegliedert, eines davon für die elektronische Beweissicherung. „Im Computerbereich sucht die Forensik nicht nach Finger- oder Fußabdrücken, sondern nach Spuren auf Datenträgern, Servern oder Netzwerkgeräten“, schilderte Friessnik. Diese führe zum Teil zu einer hohen Komplexität der Ermittlungsarbeiten. Die Rückverfolgung von Fällen werde etwa durch sich anpassende Schad-Codes immer schwieriger.

Neben dem C4 als Zentralstelle gibt es in jedem Landeskriminalamt einen eigenen IT-Assistenzbereich (AB06), diesem nachgeordnet in den verschiedenen Bezirken IT-Ermittler, die auf die Polizeiinspektionen verteilt seien. „Wir versuchen mit dieser Struktur, möglichst viel Know-how bis in die einzelnen Polizeidienststellen zu bekommen.“ Im Zuge der laufenden Kriminaldienstreform sei es Ziel, weitere Bezirksbeamte in den Bundesländern „cyberfit“ zu machen. Bislang wurden 300 Bezirks-IT-Ermittler von Bediensteten des C4 ausgebildet, insgesamt ist eine Verdoppelung auf 600 geplant. „Dann wird es auch eine noch bessere Betreuung der Opfer geben können, die wir während des Falles laufend begleiten“, sagte der *C4*-Chef.

Internationale Vernetzung. Wesentlich sei bei der Bekämpfung der Cyber-Kriminalität die internationale Vernetzung. Das *C4* ist Ansprechstelle für Europol und Interpol, in den meisten

„Ransomware“: Kriminelle verlangen Lösegeld für verschlüsselte Daten. Nicht immer halten sie ihr Versprechen, die Daten wieder freizugeben.

Fällen agieren die Täter vom Ausland aus, sodass grenzüberschreitende Polizeiarbeit unerlässlich ist. Erhard Friessnik berichtete über einen „Ransomware“-Fall, bei dem ein Unternehmen Opfer eines Hackerangriffs mit Datenverschlüsselung geworden sei. Kurz, bevor das Unternehmen das Lösegeld bezahlen wollte, fanden *C4*-Beamte über Europol heraus, dass dieselbe Tätergruppe bereits in der Schweiz aktiv war und die Daten nach Erhalt der geforderten Geldsumme nicht wiederhergestellt hatte. „Diese Information konnten wir noch rechtzeitig weitergeben. Leider halten sich die Täter nicht immer so korrekt an die abgemachte Vorgangsweise, wie das in Gössendorf der Fall war.“

Mit internationaler Expertise sei es in verschiedenen Fällen gelungen, die verschlüsselten Daten trotzdem wiederherzustellen. Wichtig seien für *C4*-Leiter Friessnik insbesondere Aufklärung und Prävention: „Der größte Angriffsvektor ist der Mensch.“ Mit der zunehmenden Verbreitung elektronischer Geräte im Alltag und der Verlagerung von Teilen des realen Lebens in die Cyber-Welt sei zwangsläufig auch mehr Cyber-Kriminalität verbunden. Es sei daher notwendig, Vorsicht im Internet walten zu lassen und die Sicherheitssysteme stets auf dem neuesten Stand zu halten.

Sicherheitsstrategien. DI Sandra Heissenberger, MBA, Chief Information Security Officer (CISO) der Stadt Wien, berichtete über Maßnahmen und Projekte der Wiener Stadtverwaltung im Umgang mit Cyber-Bedrohungen: „Als große Stadt sind wir leider ein beliebtes Ziel von Angriffen aller Art.“ Eine zuverlässige, robuste IKT-Infrastruktur sei eine Voraussetzung, um Bedrohungen wie Phishing-Mails, DDOS-Attacken oder Hackerangriffen begegnen zu können. „Als Betreiber von kritischer Infrastruktur haben wir hier eine besondere Verantwortung.“ Dazu komme eine vorausschauende IT-Strategie, die bei der Stadt Wien drei Bereiche umfasse: Safety, Security und Privacy. „Informationssicherheit ist die Basis für erfolgreiche Digitalisierung – sie schafft Vertrauen, bringt aber auch große Verantwortung mit sich“, betonte Heissenberger.

In Wien seien über 100 technische Systeme im Einsatz, um die Informationssicherheit zu gewährleisten; dazu komme ein umfassendes Regelwerk für jene Personen, die im IT-Bereich arbeiten: „Menschliches Fehlverhalten ist zu 60 Prozent der Auslöser von Sicherheitsproblemen.“ Die Stadt Wien verfügt über ein lokales *Computer Emergency Response Team (CERT)*, das eng mit der nationalen Koordinationsstelle *CERT.at* zusammenarbeitet. Dadurch

FOTO: ANDREY POPOV/STOCK.ADOBE.COM

wird es möglich, bei Bedarf sofort auf IT-Sicherheitsangriffe zu reagieren und gleichzeitig die Informationen mit den anderen Beteiligten im österreichischen *CERT*-Verbund zu teilen. „Aus strategischer Sicht" sei laut Heissenberger die Vernetzung mit den IT-Experten anderer Organisationen besonders wichtig, neben *CERT* etwa mit den Chief Information Security Officers anderer Bundesländer oder der Europäischen Agentur für Cyber-Sicherheit *ENISA*.

Schwachstellen finden. Um Schwachstellen im Internetauftritt der Stadt Wien herauszufinden, wurde ein „Bug Bounty Programme" gestartet: Interessierte werden offiziell zum „Hacken" eingeladen. Abgesichert durch klare Spielregeln können sich Teilnehmende, die einen Fehler („Bug") finden, eine Belohnung („Bounty") von bis zu 1.000 Euro verdienen. „Bei über 800 Anwendungen auf der Homepage kommt man trotz regelmäßiger Belastungstests einfach selbst nicht auf alles."

Neue Projekte. Zwei Wiener Projekte gehen neue Wege bei Cyber-Bedrohungen. So wurde eine eigene „Kompetenzstelle gegen Cybergewalt" geschaffen, bei der der *Wiener Frauennotruf*, der Verein *Wiener Frauenhäuser* und das Wiener *CERT* eng zusammenarbeiten. Laut Studien sind oft Frauen Opfer von Gewalt im virtuellen Raum, etwa durch Demütigungen oder Bedrohungen. Die Kompetenzstelle

Erhard Friessnik: „Die größte Angriffsfläche ist der Mensch."

Sandra Heissenberger: „Vernetzung mit IT-Experten ist wichtig."

analysiert den Fall und bietet – erforderlichenfalls unter Einschaltung der Strafverfolgungsbehörden – durch Beistellung technischer Hilfsmittel Unterstützung. Beispielsweise können IT-Experten dabei helfen, gelöschte Daten wie Fotos oder Videos wiederherzustellen, damit sie bedrohten Frauen, die Agressionshandlungen zur Anzeige bringen wollen, als Beweismittel zur Verfügung stehen. Der Start des Kompetenzzentrums ging mit einer Informationsoffensive zu Cyber-Kriminalität einher; 2022 soll die Kooperation mit weiteren Gewaltschutzorganisationen ausgebaut werden.

Cybercrime-Erstberatung. Im ersten Quartal 2022 startet auch eine neue „Cybercrime-Erstberatung" als Anlaufstelle der Stadt: Bei Fragen zu vermuteter Cyber-Kriminalität wird potenziellen Opfern Beratung als Entscheidungshilfe für weitere Schritte angeboten. „Oft geht es nur um eine erste Einordnung des geschilderten Falles und darum, ein echtes Delikt von einem rein technischen Problem zu unterscheiden", sagte Heissenberger. Ein niederschwellig eingerichteter, telefonisch erreichbarer Kontaktpunkt wie in Wien sei auch ein kommendes Ziel des Bundeskriminalamts, ergänzte Erhard Friessnik nach dem Vortrag. Bislang sei die Meldestelle des *C4* nur per E-Mail erreichbar.

Diskussion. Eine an die Referate anschließende Diskussion befasste sich unter anderem mit der Notwendigkeit von Schulungen über IT-Sicherheit zur Bewusstseinsbildung, mit staatlichen Vorgaben bei Hackerangriffen, dem Umgang mit Medien und Ressourcen und den aktuellen Möglichkeiten, sich gegen Cyber-Angriffe versichern zu lassen.

Sektionschef Dr. Mathias Vogl, Leiter der Rechtssektion im Bundesministerium für Inneres und Moderator der Veranstaltung, verwies auf die laufenden Aktivitäten des Innenressorts zur Bekämpfung von „Hass im Netz". Aufgrund umfangreicher Schulungen bei der Polizei und der systematischen Erfassung von Motiven bei vorsätzlichen Straftaten seien im sicherheitsbehördlichen Bereich wichtige strategische Maßnahmen gegen „Hate-Crime" gesetzt worden. *Gregor Wenda*

Gemeinsames Vorgehen

Nach der Eröffnung der neuen Räume des *Cybercrime Competence Centers (C4)* im November 2021 wurde ein weiteres wichtiges Thema begonnen. Um innerhalb der DACH-Region Deutschland, Österreich und Schweiz gestärkt gegen Cybercrime vorzugehen, unterzeichneten der Direktor des Bundeskriminalamtes, General Mag. Andreas Holzer, MA, die Vizepräsidentin des Bundeskriminalamtes Wiesbaden, Martina Link, und der Vizedirektor des Bundesamtes für Polizei der Schweizerischen Eidgenossenschaft (fedpol), Yanis Callandret eine Vereinbarung, die sie im gemeinsamen Kampf gegen Cybercrime einigt.

Gemeinsam gegen Cybercrime: Yanis Callandret, Fedpol, Martina Link, BKA Wiesbaden, Andreas Holzer, BK Wien.

Gemeinsame Absichtserklärung. Die Erklärung soll die wechselseitige Beziehung nicht nur vertiefen, sondern auch weiterentwickeln. „Die gemeinsame Absichtserklärung, die uns im Kampf gegen Cybercrime eint, war ein wichtiger Schritt in die richtige Richtung. Wir müssen unser Wissen bündeln und Erfahrungen austauschen, wenn wir effektiv gegen Cybercrime vorgehen wollen", erklärte BK-Direktor Holzer.

Ziel der Vereinbarung ist, die Kooperation beim Wissens- und Erfahrungsaustausch zu fördern und zu intensivieren, ebenso soll bei der Aus- und Fortbildung sowie der fachspezifischen Forschung die Zusammenarbeit ausgebaut und forciert werden. Erreicht werden soll dieses Bestreben durch koordiniertes und gemeinsames Vorgehen unter der Einbindung von Wissenschaft und Wirtschaft sowie der Nutzung bereits bestehender Instrumente, wie zum Beispiel der *Joint Cybercrime Action Task Force (J-CAT)*.

FOTOS: BK/ARMIN HALM, GERD PACHAUER, STADT WIEN