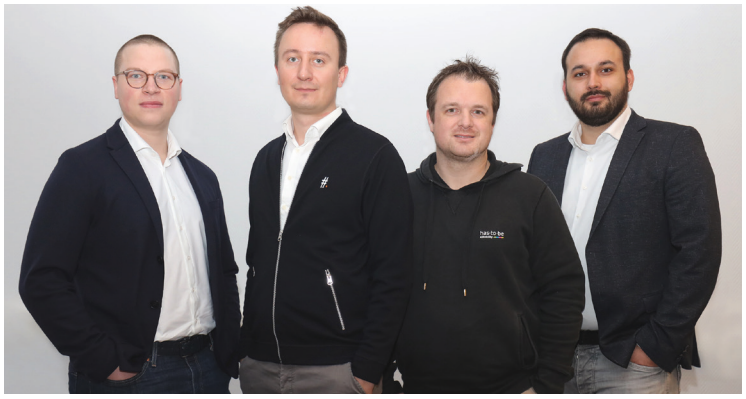
NIS-Gesetz: Strafen drohen

Bei nicht zeitgerechter Umsetzung drohen systemrelevanten Unternehmen Strafen von bis zu 100.000 Euro.

Bereits ab Anfang 2019 informierte der österreichische Staat rund 100 öffentliche und private Organisationen über ihren systemrelevanten Status. Diese Systemrelevanz bedingt, dass sie Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme treffen und darüber alle 3 Jahre Nachweise erbringen müssen. In Österreich ist die staatlich akkreditierte Zertifizierungsinstanz CIS als qualifizierte Stelle für NISG-Prüfungen zugelassen. Laut Geschäftsführer Klaus Veselko haben einige Unternehmen bereits vorbildlich gehandelt, andere lassen sich noch Zeit bei der Umsetzung. »Säumigen Organisationen drohen hohe Strafen. Zudem laufen bereits Verhandlungen, um künftig noch mehr Branchen in die Pflicht zu nehmen«, warnt Veselko. Das österreichische Netz- und Informationssystemsicherheitsgesetz (NISG) beruht auf der NIS-Richtlinie der EU und wurde bereits Ende 2018 in nationales Recht umgesetzt. Ab Anfang 2019 wurden sukzessive rund 100 Organisationen per Bescheid informiert, dass sie zur kritischen Infrastruktur Österreichs zählen. Sie stammen im Wesentlichen aus den Bereichen Energie, Verkehr, Bankwesen, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur. Diese Organisationen wurden nicht nur dazu verpflichtet, Sicherheitsvorfälle zu melden – sie haben auch Sicherheitsvorkehrungen zu treffen und müssen alle 3 Jahre ab Zustellung des Bescheides durch Überprüfung seitens qualifizierter Stellen Nachweise über diese Präventivmaßnahmen erbringen.
»Der Aufwand und die Komplexität der Umsetzung werden teilweise deutlich unterschätzt. Dadurch besteht die Gefahr, dass die Nachweise nicht zeitgerecht erbracht werden können«, so Veselko. »Von der Beauftragung der Auditoren bis zur Ausfertigung des Berichts und der Bestätigung muss man mit rund 4 bis 5 Monaten rechnen. Zudem sind oft noch umfangreiche interne Vorarbeiten in den Unternehmen notwendig.« Wie unter Abschnitt 7 des NIS-Gesetzes nachzulesen ist, drohen bei Verfehlungen bis zu 50.000 Euro Strafe, im Wiederholungsfall sogar bis zu 100.000 Euro. »Ich würde nicht empfehlen, die Sache auf die leichte Schulter zu nehmen«, so der Experte. Im Zuge der Sicherheitsüberprüfungen werden eine Reihe von Security-Checks wie etwa Schwachstellen-Scans durchgeführt, die Aufschluss darüber geben, ob Angreifer in ein System eindringen können. cb



Holler und Lew (hae.sh), Investor Klässner und Kirchmayr (hae.sh).

Millioneninvestment für Linzer hae.sh

Der Linzer Softwareschmiede gelang es, in einer Finanzierungsrunde 1,3 Mio. Euro zu generieren. Mit dem Geld will das Unternehmen schneller wachsen und in Produktentwicklung und den Ausbau des Teams investieren. hae.sh unterstützt Unternehmen dabei, ihre Kontrollprozesse zu modernisieren und zu perfektionieren. Der Fokus ist die Entwicklung einer leicht zu handhabenden Continuous Audit Application (Kontinuierliche Prüfungsanwendung) auf Blockchain-Basis. »Aufgrund rechtlicher Vorgaben ist es für Unternehmen und Wirtschaftsprüfer von elementarer Bedeutung über effiziente interne Kontroll- und Steuerungssysteme zu verfügen«, sagen Sebastian Holler, Nicolas Kirchmayr und Stefan Lew, die hae.sh 2020 gegründet haben. Die Finanzierungsrunde wird von Martin Klässner und Paul Achleitner angeführt. cb

E-Learning-Kooperation

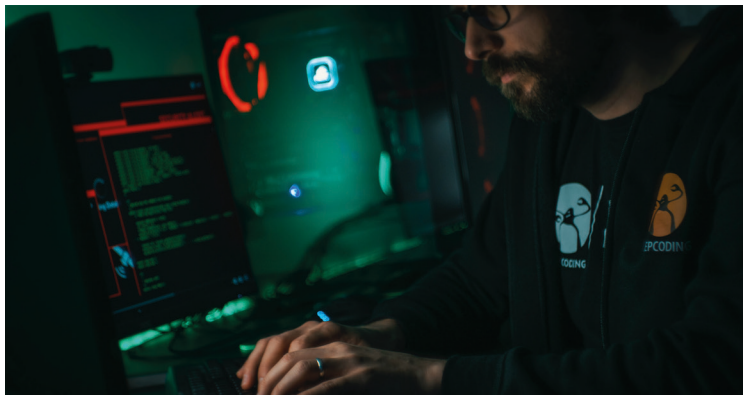
Der Verband Technischer Handel (VTH) aus Düsseldorf hat eine Kooperation mit dem Unternehmen QuickSpeech aus Gablitz bei Wien gestartet. »Durch kleine, leicht verdauliche Lernportionen wird den Mitgliedsunternehmen des VTH sowie seinen Mitarbeitern mit Hilfe von QuickSpeech ein einfacher und spielerischer Zugang zu Wissen ermöglich«, sagt Mario Ernst, Vorsitzender des VTH (Bild). Durch den Einsatz und Ausbau von Machine Learning passt sich die Software an die Bedürfnisse der Nutzer an. cb

Ausbildung für Startups

In puncto Wachstum zeigen internationale Startups Strategien, die heimischen Gründern fehlen. 9 von 10 scheitern bereits im ersten Jahr, weil sie ihr Produkt nicht am Markt etablieren können. Die Wiener Startup-Coachin Stephanie Biebel (Bild) bietet mit drei Partnern laut eigenen Angaben das erste Aus- und Weiterbildungsprogramm speziell für deutschsprachige Startups, das auf deren gesamten Lebenszyklus ausgelegt ist. Startpunkt für die mehrteilige »Growth Mastery« ist der 4. März. cb

Mehr Open Data

Die EU-Mitgliedsstaaten haben bei der Entwicklung von Open Data im Jahr 2021 weitere Fortschritte erzielt. Das ist das Ergebnis des »Open Data Maturity Reports 2021«, der zum siebten Mal in Folge den Reifegrad von Open Data in Europa misst. Der Bericht erfasst die Verbesserungen, die europäische Länder im vergangenen Jahr bei der Veröffentlichung und Wiederverwendung offener Daten erzielt haben, sowie die hierfür gesetzten Prioritäten. Österreich liegt demnach mit einem Reifegrad von 92 Prozent weit über dem EU-Schnitt, insbesondere durch einen hohen Reifegrad in der Kategorie »Policy« (96 Prozent – EU-Schnitt: 87 Prozent). Diese beschreibt unter anderem den regulatorischen Rahmen eines Landes für Open Data sowie die Strategie und Grad der Implementierung. Insgesamt verzeichnet die Studie einen europaweiten Reifegrad von 81 Prozent – eine Steigerung von 3 Prozentpunkten gegenüber dem Vorjahr. »Die EU hat die Bedeutung von Daten zur Verbesserung politischer und administrativer Entscheidungen erkannt und entsprechende Datenstrategien entwickelt. Die Studie zeigt, dass Österreich im Gegensatz zu anderen Staaten zwar beständige Fortschritte macht, wir uns auf diesen Lorbeeren aber nicht ausruhen sollten«, sagt Simon El Dib, Head of Capgemini Invent in Österreich (Bild). cb



Cyberattacken stiegen um 117 Prozent

Die Sicherheitsforscher von Check Point Research haben gemeldet, dass die Zahl von Angriffen auf Firmennetzwerke stark zugenommen hat. In Österreich um 117 Prozent, in Deutschland um 62 Prozent und in der Schweiz um 65 Prozent. Auf die Branchen bezogen, waren in Österreich die Bereiche Government/Military unter Dauerfeuer und verzeichneten einen Anstieg von 219 Prozent verglichen zum Jahr 2020. Danach kommen die Bereiche Finance/Banking mit 203 sowie Software Vendors mit 147 Prozent. Europa als Region sah einen Anstieg von 68 Prozent aller virtuellen Angriffe – in Prozent gemessen ist das der stärkste im Vergleich zu anderen Gegenden. »Ich gehe davon aus, dass all diese Zahlen 2022 steigen werden, da Hacker neue Methoden zur Durchführung von Attacken, insbesondere Ransomware-Angriffen, suchen werden. Ich empfehle der Öffentlichkeit, insbesondere im Bildungs-, Regierungs- und Gesundheitssektor, sich mit den Grundlagen des eigenen IT-Schutzes vertraut zu machen«, sagt Omer Dembinsky, Data Research Manager bei Check Point. cb