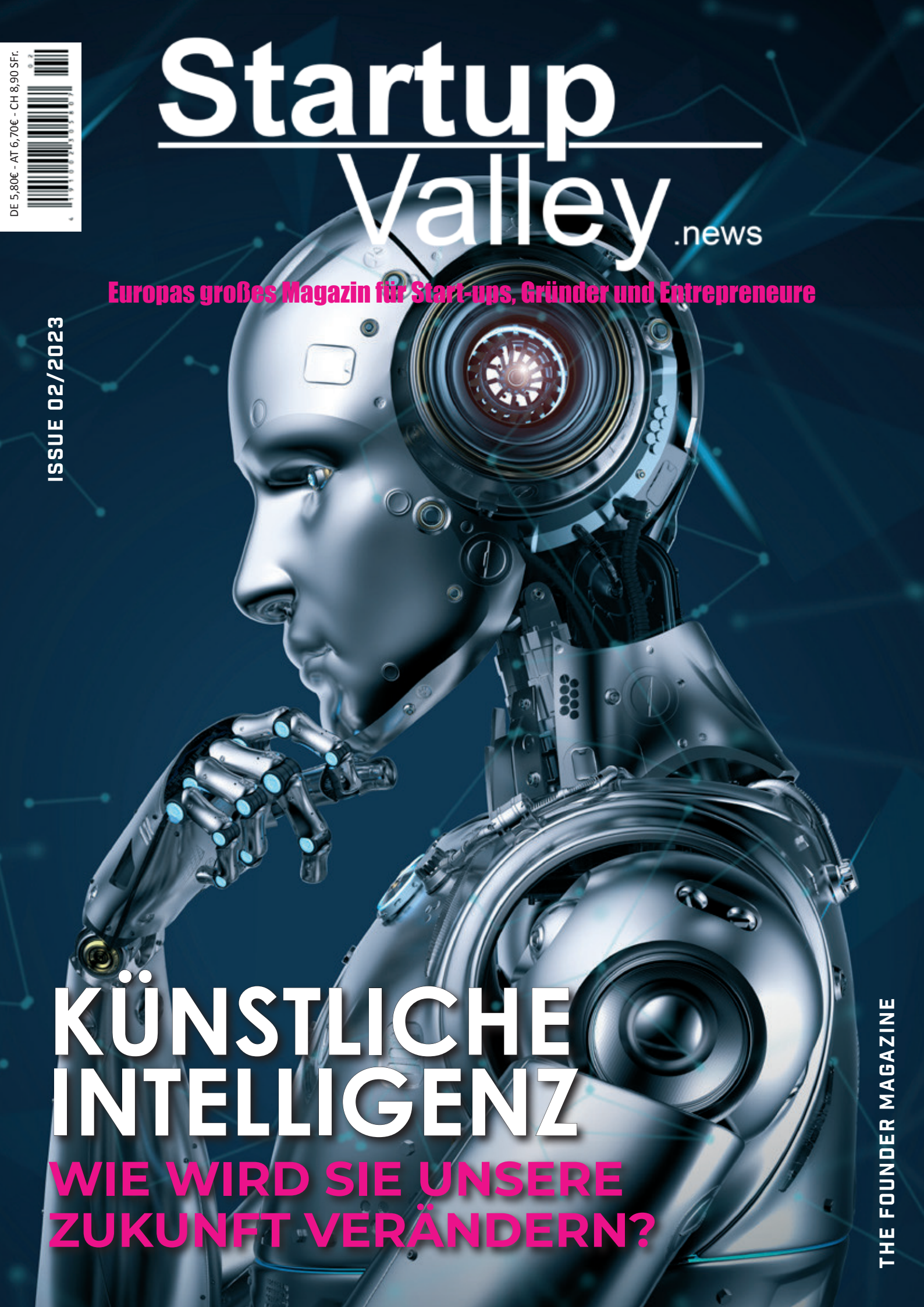
DE 5,80€ - AT 6,70€ - CH 8,90 SFr.

Startup Valley .news

Europas großes Magazin für Start-ups, Gründer und Entrepreneure

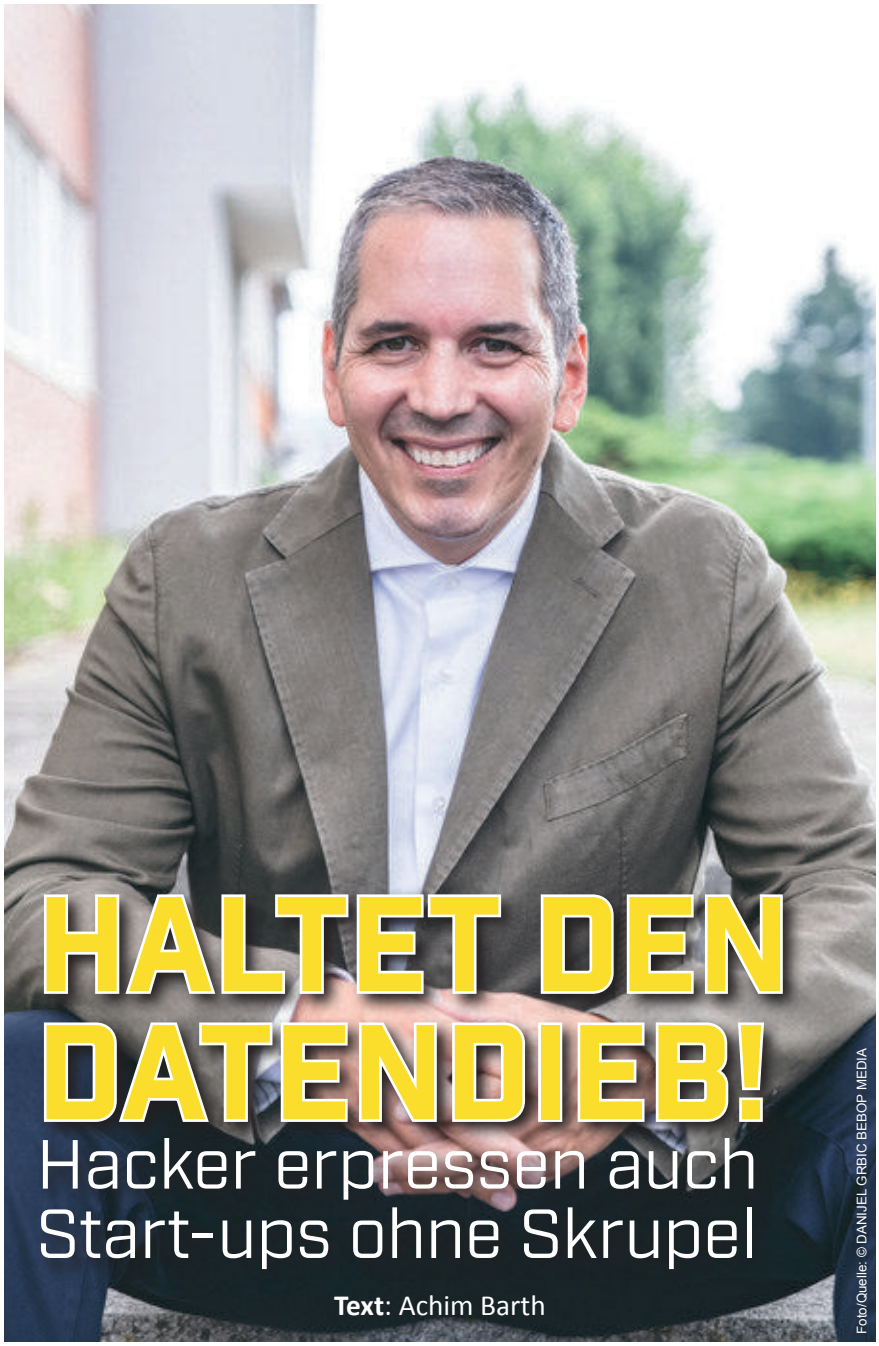
ISSUE 02/2023



KÜNSTLICHE INTELLIGENZ

WIE WIRD SIE UNSERE ZUKUNFT VERÄNDERN?

THE FOUNDER MAGAZINE



HALTET DEN DATENDIEB!

Hacker erpressen auch Start-ups ohne Skrupel

Text: Achim Barth

Foto/Quelle: © DANIJEL GRBIC BEBOP MEDIA

Hackerangriffe auf Start-ups nehmen zu. Wer Daten und Betriebsgeheimnisse schützen will, muss extrem auf der Hut sein. Wie können sich junge Unternehmen vor Attacken schützen? Mit welchen Methoden arbeiten Cyberkriminelle? Datenschutzexperte Achim Barth kennt die Schwachstellen und weiß, wie Start-ups sich so wenig angreifbar wie möglich machen.

Die Gefahren der Datenspinne, die Tricks der Datendiebe und die Methoden der Cyberkriminellen bedrohen Firmen von allen Seiten. Die Zahl der Hackerangriffe auf Unternehmen steigt kontinuierlich. Betroffen sind nicht nur große Companys. Die meisten Kriminellen greifen breit an und nehmen alles mit, was sie erbeuten können. Start-ups sind oft reine, aber beliebte Zufallsopfer, weil kriminelle Profis kritische Schwachstellen in deren IT-Systemen, Servern oder Smartphones entdecken. Über Nacht wird die eigene Firmenwebseite so Teil eines kriminellen Botnetzes, zur Spamschleuder oder Werbeplattform für Onlinespiele. Kapern Hinterlistige den Mailserver, verschicken sie im Namen der jungen Marke feindliche Schadmails an alle Kontakte. Das beschädigt das junge Image und gefährdet die IT-Sicherheit der Kunden, Investoren, Lieferanten und Fans.

Phishing-Attacken können extremen Schaden anrichten

Phishing-Angriffe sind besonders gefährlich. Verbrecher wollen Auftragsdetails, E-Mail-Adressen oder andere sensible Firmeninterna „abfischen", um sie im Darknet zu Geld zu machen. Häufig werden Kundendaten gekapert, kopiert, zum Kauf angeboten oder für Straftaten missbraucht. Um an das Diebesgut zu gelangen und die Empfänger aus der Reserve zu locken, versenden sie täuschend echt aussehende Phishing-E-Mails. Diese wirken so authentisch, dass Nutzer den kriminellen Charakter nur mit vorheriger Schulung erkennen. Häufig imitieren die Betrüger die E-Mail-Struktur eines real existierenden Unternehmens und stellen im Text einen konkreten Bezug zum Start-up her.

Der Inhalt verbreitet dann Panik: Die Buchhaltung habe eine Rechnung nicht bezahlt. Das Kundenkonto werde gesperrt. Oder Lieferungen würden zurückgeschickt. Der Inhaber soll unter Druck geraten und Kreditkartendaten herausgeben. Überweist jemand pflichtbewusst Summe x, ist das Geld für immer weg. Manche Phishingmails enthalten Links oder Anhänge. Hier soll der Empfänger der Webadresse folgen oder den Zip-Ordner öffnen. Wer in die Falle tappt, landet unter Umständen auf einer gefälschten Seite, die Daten abgreift. Alternativ lädt der User unbemerkt Schadprogramme herunter. Nach einigen Tagen wird der Schädling aktiv und verschlüsselt alle Ordner.

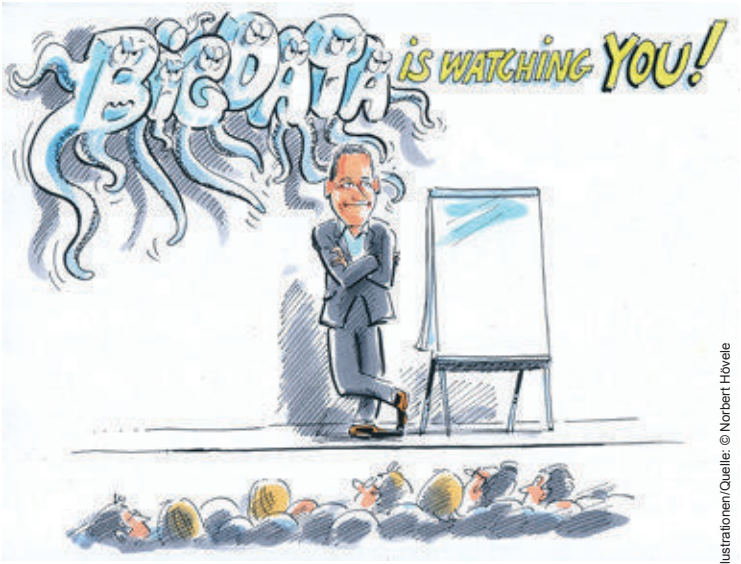
Das wieder in den Griff zu bekommen und alle Beteiligten zu beruhigen, kostet Zeit, Geld und Nerven. Dafür braucht es Profis. Besonders wenn Gründer zusätzlich erpresst werden, leidet der Ruf. Wenn Betrüger für die Entschlüsselung der Inhalte einen Geldbetrag in Kryptowährung fordern, ist so manche Firma aufgeschmissen. Das Ausmaß des Schadens kann ein junges Business in die Knie zwingen. Gehackte Organisationen haben keinen Zugriff auf Inhalte und Systeme, können nicht produzieren und sind

nicht mehr erreichbar. Deshalb ist es für moderne Unternehmen überlebenswichtig, sich konsequent vor solchen Attacken zu schützen.

Wie können Start-ups sich vor Datendieben schützen?

Als Erstes müssen Start-ups ihre Hausaufgaben machen und die DSGVO einhalten. Und sei es nur, um keine Abmahnung oder Bußgelder zu riskieren. Viele Aufsteiger haben erst einmal andere Sorgen: Produktentwicklung, Vertrieb, Marketing. Der Datenschutz fällt da immer unter den Tisch. Doch wer die DSGVO sofort richtig umsetzt, ist automatisch besser vor Cyberkriminellen geschützt. Die Systeme sind auf dem neuesten Stand und das Team ist für einen bewussten Umgang sensibilisiert.

Illustrationen/Quelle: © Norbert Hövele



Illustrationen/Quelle: © Norbert Hövele

Die DSGVO deckt jedoch nicht alles ab. Auch alle anderen Informationen wie Patente, Pläne oder Lösungen sind schützenswert. Jeder Selbstständige sollte sein Business systematisch absichern: Dazu gehören: Zutrittskontrolle (wie sichere ich meine Produktions-, Verkaufs-, Büro- und Serverräume?), Zugangskontrolle (wie sichere ich meine digitalen Systeme?), Zugriffskontrolle (wie stelle ich sicher, dass Kollegen nur bestimmte Daten sehen?) und Trennungskontrolle (wie garantiere ich, dass Kundeninformationen nicht vermischt werden?). Konkret beginnt das zum Beispiel mit abschließbaren Türen, gesicherten Diensthandys und seriöser Software. Weiter geht es damit, dass Unternehmen ein gutes Antivirusprogramm einsetzen, das Malware erkennt und entfernt. Unternehmen sollten ihre Dienste mit der Zwei-Faktor-Authentifizierung absichern. Ein einfacherer wirksamer Tipp ist auch, alle technischen Systeme immer auf dem neuesten Stand zu halten. Wer Erpressern das Leben schwer machen will, nutzt stets die jüngste Version des Betriebssystems und Browsers. Auch Sicherheitsupdates sollten Kollegen sofort installieren.

Tipps zu Verhalten und Technik

Neben diesen und weiteren IT-Grundlagen steht und fällt der Schutz mit dem Verhalten der Mitarbeiter. Wer täglich E-Mails, Apps, Messenger und andere digitale Systeme nutzt, macht schnell Fehler. Das nutzen Kriminelle gezielt aus. Daher ist es so wichtig, dass Teams wissen, was wie zu tun ist: E-Mail-Absendern nicht blauäugig vertrauen, Apps nur aus offiziellen Stores herunterladen, nur auf gesicherten Webseiten surfen, VPN-Tunnel und verschlüsselte Netzwerke nutzen, alte Daten konsequent löschen und neue mit starken Passwörtern sichern, die nicht auf Zetteln am Bildschirm kleben. Da sich Technik und Hackermethoden rasant weiterentwickeln, sollten sich Inhaber am besten jährlich in Sachen IT-Sicherheit und Datenschutz weiterbilden.

Trotz aller Vorsichtsmaßnahmen: Absoluten Schutz vor Datendieben gibt es nicht. Backup-Systeme können dafür sorgen, dass Start-ups im Ernstfall weich landen. Sie retten bei Angriffen ebenso wie bei Wasserschäden, technischen Defekten oder menschlichen Fehlern. Chefs sollten das System jedoch regelmäßig testen. Wer nicht ausprobiert, ob sich die Daten jederzeit einspielen lassen, steht vor einem Problem. Zu guter Letzt empfiehlt es sich, ein klares Notfallkonzept vorzubereiten. Was ist zu tun, wenn Systeme längere Zeit nicht verfügbar sind? Der Strom ausfällt? Oder die Büros nicht betreten werden können? Diese Überlegungen sparen im Ernstfall jede Menge Ärger. ■

Achim Barth

Achim Barth, Datenschutzbeauftragter und Meldestellenexperte: Zielgerichtet, sachkundig und immer up to date begleitet der mehrfach zertifizierte Datenschutzprofi Unternehmen bei der Umsetzung des Datenschutzes und Hinweisgebergesetzes.