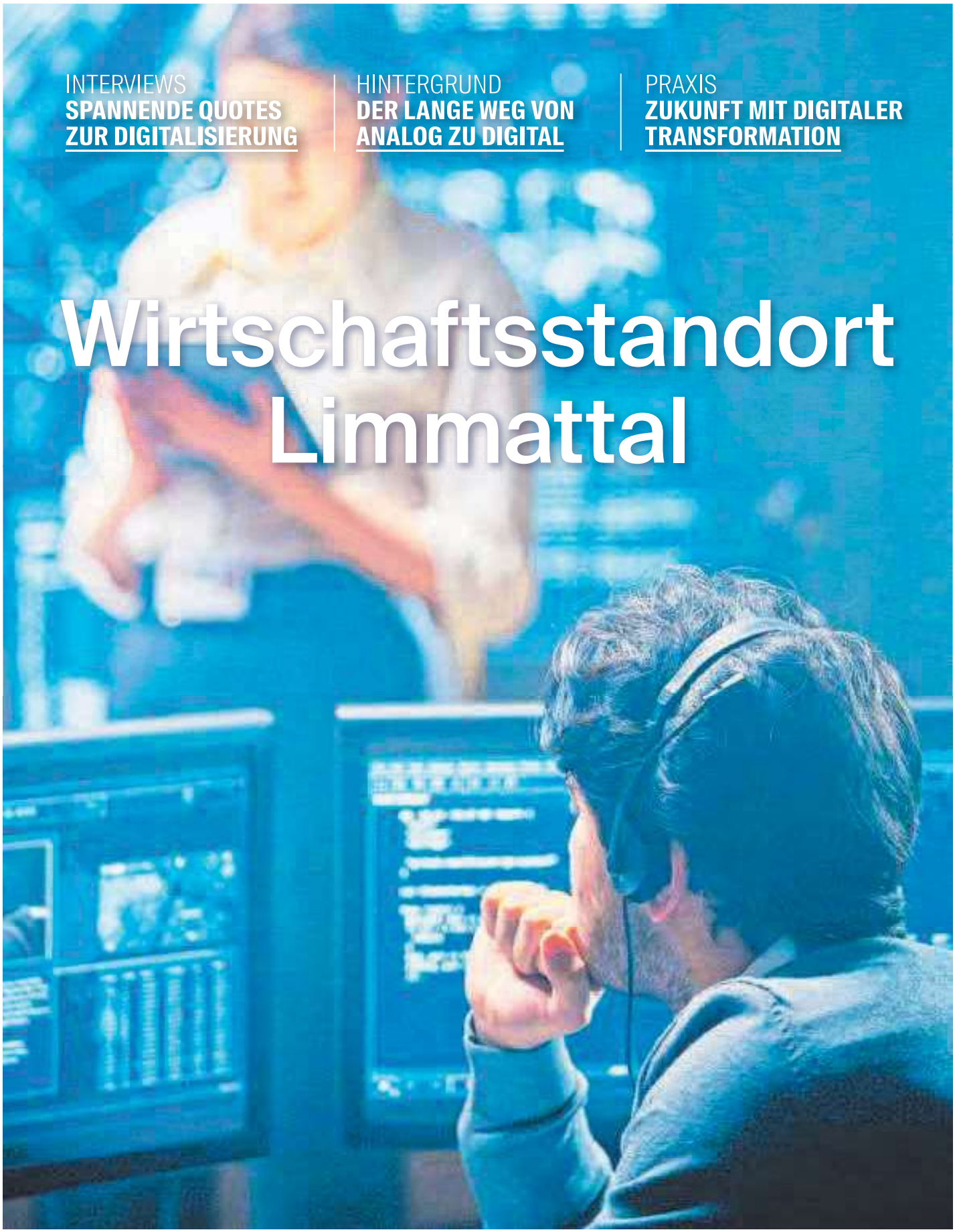
INTERVIEWS
SPANNENDE QUOTES ZUR DIGITALISIERUNG

HINTERGRUND
DER LANGE WEG VON ANALOG ZU DIGITAL

PRAXIS
ZUKUNFT MIT DIGITALER TRANSFORMATION

Wirtschaftsstandort Limmattal



Verlagsbeilage vom 15. Mai 2025

Limmattaler Zeitung

«Die grösste Gefahr bleibt der Mensch selbst»

Ivan Bütler ist Computerexperte und Dozent und führt ein Unternehmen für IT-Sicherheit. Welche Vorteile und Gefahren die Digitalisierung der Gesellschaft bietet, sagt er im Interview.

Thomas Pfann

Ivan Bütler, welches ist Ihr Spezialgebiet bei der IT Security?
Meine Aufgabe ist es, die IT-Systeme von Privatpersonen, Firmen oder Behörden auf ihre Sicherheit zu prüfen und etwelche Lücken und Fehler zu finden. Im Fachjargon nennt man uns «ethische Hacker» und greifen ein System an per Vereinbarung. Wir sind sowohl präventiv tätig und melden den Auftraggebern, wenn wir Sicherheitsmängel entdecken. Wir sind aber auch als «Feuerwehr» vor Ort, wenn Angriffe auf ein IT-System bereits erfolgt sind.

Wo lauern heute die grössten Gefahren bei der Sicherheit im Umgang mit Computern und portablen Ausgabegeräten?
Die grösste Gefahr für alle Systeme und Geräte ist und bleibt der Mensch selbst. Ein falscher Klick auf ein E-Mail, auf einen Link oder einen Button und schon können Hacker ins System eindringen. Vorerst merkt man davon nichts, so dass sich die Angreifer und Cyberkriminelle etablieren und für ihre wahren Absichten bereit machen können.

Welche üblen Ziele verfolgen die Diebe meistens?
Oft versuchen sie, Zugriff auf Bankkonti zu erlangen. Sind diese Schranken einmal gefallen, können sie sich problemlos bereichern. Allerdings sind die Geldflüsse auch nach einem Angriff verfolgbar, was es für die Kriminellen nicht einfach macht. Sehr oft drohen Hacker mit Erpressung, wenn sie nach dem Eindringen ins System Daten verschlüsseln und nur bei Bezahlung eines Lösegelds wieder zugänglich machen. Wer von seinen Daten kein gutes Back-up gemacht hat, hat also richtig grosse Probleme.

Haben Sie Tipps, wie man sich im Alltag vor Cybercrime schützt?
Stets mit Verstand bei der Sache sein. Dubiose Angebote zum schnellen Geld, grosse Gewinne oder seltsame Forderungen nach Passwörtern oder Auskünften zur Person sind fast ausnahmslos versteckte Angriffe. Man sollte Geräte- und Betriebssystem-Updates immer sofort ausführen und am besten automatisieren. Keine unseriösen Apps installieren und regelmässig Passwörter ändern. Diese versteckt als Telefonnummer oder Adresse zu speichern, ist auch schlecht – Cyberkriminelle kennen diese Tricks. Ebenso wichtig ist die zweistufige Authentifizierung (2FA) beim Einloggen und das regelmässige Erstellen eines Back-ups.

Ivan Bütler ist Gaunern und Verbrechern im Internet auf der Spur. Bild: zvg

In Beruf und Geschäft muss man sich oft mit privaten Geräten auf Geschäftssysteme einloggen. Macht das Sinn?
Das kann schon ein Problem sein, wenn sich die Systeme privater Geräte mit denen der Firmensysteme verknüpfen. Tatsächlich kann man sich heute ohne eigenes Smartphone kaum mehr irgendwo einloggen. Ein Unternehmen muss sich gut überlegen, wie es die Zugriffsapplikation sicher gestaltet. Oft ist der Kostenfaktor relevant - aber «günstig» und Sicherheit vertragen sich nicht. Ein sicheres System kostet Geld.

Sind Smartphone- und Tabletnutzer je länger, je mehr überfordert mit den ständig ändernden Sicherheitsmassnahmen?
Es braucht ein gewisses Verständnis für den Gebrauch all dieser Geräte, klar. Das Leben ist mit dem Internet definitiv komplexer und vernetzter geworden. Grundsätzlich glaube ich, dass die mobilen Geräte vieles vereinfachen: Zugfahrpläne anschauen, Tickets kaufen, die gesamte Kommunikation mit Wort und Bild, die ständige Informationsverfügbarkeit – wenn alles einmal eingerichtet ist und funktioniert, können die elektronischen Begleiter unser Leben erleichtern.

Ist die Welt sicherer geworden mit der Digitalisierung – oder eher nicht?
Auf der einen Seite schon, bei Geräten, die sicherer funktionieren, oder bei technischen Prozessen, die sich besser kontrollieren und überwachen lassen. Grundsätzlich bietet die steigende Zahl an Geräten, die miteinander verbunden sind, mehr Angriffsfläche. Die Komplexität ist der Feind der Sicherheit, denn es braucht immer mehr Fachwissen, um dem Kalkül und den schlechten Absichten von Kriminellen folgen zu können. Die Digitalisierung erlaubt es ihnen, sich einfacher zu verstecken und anonym zu bleiben.

In welchem Bereich der Digitalisierung sehen Sie das grösste Entwicklungspotenzial?
Wie gesagt, die Digitalisierung macht unser Leben einfacher – und danach streben wir ganz allgemein. Vermutlich werden wir irgendwann unseren Körper mit einem Chip überwachen lassen können und so Krankheiten viel früher erkennen. Wenn es um die Gesundheit geht, sind viele Menschen für neue Möglichkeiten bereit, davon bin ich überzeugt. Bei der Kommunikation sind wir heute schon so weit, uns jederzeit auszutauschen. Übersetzungsprogramme gibt es schon, es werden aber solche in «Realtime» kommen, wo wir also in unserer Sprache sprechen und diese gleichzeitig in einer Fremdsprache weitergeben. Sprachen lernen, wie wir es heute machen, wird vielleicht überflüssig. Schliesslich kann die Digitalisierung auch zum verstärkten Individualismus führen, vom Leben in der Gesellschaft zu mehr Einzelgängern und Egozentrikern. Und bei autokratischen Regierungsformen mit einem ausgeprägten Überwachungssystem kann die Digitalisierung ein Mittel zur Machterhaltung sein.