PRO SENECTUTE
GEMEINSAM STÄRKER

Akzent

Magazin für Kultur und Gesellschaft

2|21
April

Digital unterwegs

Regionale KMU

Rotstift und Rotwein go digital

Cyberkriminalität

Der Dieb im Computer

Baseldytsch

Whatsäpple vor em Reeselikeel

Bildung und Kultur

Vortrag: Diagnose Demenz

Pro Senectute beider Basel
bb.prosenectute.ch

Liebe Leserin, lieber Leser

Es ist vor allem ein Moment, der sich mir eingeprägt hat: Die Sportlehrerin liegt im leeren Saal auf der roten Matte, sie macht eine Dehnübung und spricht dazu laut mit dem Laptop: «So ist es viel besser, Monika; einfach das Bein näher zum Gesäss ziehen – genau so!»

Was ich da sah, war ein Gymnastikkurs. Ein Gymnastikkurs übers Internet, möglich gemacht durch das Videoprogramm Zoom. Die Kursleiterin war vor Ort, die Teilnehmerinnen turnten zu Hause in der guten Stube mit. Alle zusammen im Laptop, jede für sich allein daheim. Und so wie an jenem Morgen im Akzent Forum fanden und finden seit Beginn der Coronapandemie landauf, landab solche Kurse, Sitzungen und Workshops statt.

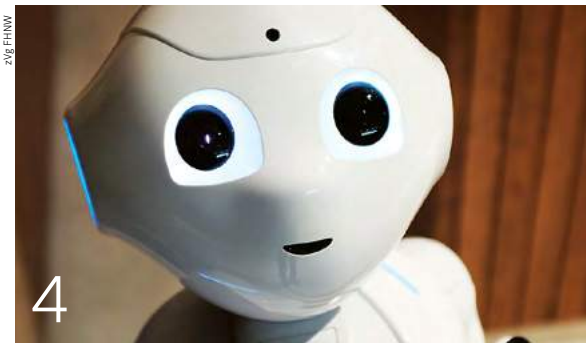
Die Digitalisierung wird oft – zu Recht – kritisch betrachtet. Sie treibt die Globalisierung voran und vernichtet Arbeitsplätze, sie macht uns zum überwachten, gläsernen Menschen, der sich vor der Cyberkriminalität fürchtet und in den sozialen Medien vereinsamt.

Aber gleichzeitig bietet die digitale Revolution auch zahlreiche Chancen. Sie schafft neue Geschäftsmodelle und vereinfacht bei KMU wie der Basler Rotstift AG und der Liestaler Traditionskellerei Siebe Dupf die Abläufe. Sie erleichtert der Zahnärztin Miriam Merz dank neuen Technologien die Zusammenarbeit mit dem Zahntechniker. Und sie macht im Smarthome die Steuerung der Heizung und des Lichts zum Kinderspiel. Mehr dazu im Schwerpunkt dieser Ausgabe.

Christine Valentin, Redaktionsleiterin

Inhalt

Titelfoto: Roboter Pepper, Foto: pio3/shutterstock.com



zVg FHNW

Was «fühlt» der Roboter?

jurgenfr/shutterstock.com

Gefährliche Tasten ...

Roland Schmid

Neue digitale Abläufe bei den KMU

bajour 21

Von analogen zu digitalen News

Marco Liechti von der Basler Kantonspolizei weiss, was man tun muss, um im Internet nicht übers Ohr gehauen zu werden.

Cyberkriminalität

Die Schattenseiten der Digitalisierung

Die digitale Revolution ist in vollem Gang. Sie weist ein enormes Potenzial auf. Doch auch Gefahren lauern. Marco Liechti, Ressortleiter Kriminalprävention bei der Basler Kantonspolizei, klärt über die Schattenseiten auf.

Text **Markus Sutter** · Foto **Claude Giger**

Marco Liechti berührt den grossen Bildschirm in einem Vorzeigeraum der Basler Kantonspolizei am Clarahofweg. Der Schirm ist voller Hinweise, Ratschläge und Warnungen vor den negativen Folgen der Digitalisierung: «Betrüger versuchen, Nutzer zur Eröffnung von Bankkonten zu bewegen» oder «Seien Sie wachsam, auch im Internet» lautet eine Kernbotschaft in einem kurzen Film. «Trauen Sie niemandem, den Sie nur aus dem Internet kennen.»

Marco Liechti, Feldweibel 1 und Ressortleiter Kriminalprävention bei der Basler Kantonspolizei, weiss, wovon er spricht. Und er weiss, warum er so spricht. Trotz grosser Aufklärungsarbeit gibt es immer wieder Unvorsichtige und Gutgläubige, denen man ein X für ein U vormachen kann. Eine verliebte Frau tut sich manchmal schwer, sich selbst einzugestehen, dass der um sie werbende Traummann auf einer Datingplattform in dieser Vollkommenheit letztlich nur virtuell existiert. Die Warnzeichen hingegen, dass er es ganz real vor allem auf ihr Portemonnaie abgesehen hat, übersieht sie. Dabei sind sie offensichtlich. Der Traummann lässt sich beim realen Treffen im Café nie persönlich blicken, weil verflixterweise immer etwas dazwischen kommt … Der Betrüger nützt die Anonymität des Netzes, das Nähe vortäuscht, schamlos aus. Deshalb rät

Marco Liechti: Wer immer wieder abgewimmelt oder vertröstet wird, wenn der Zeitpunkt des persönlichen Kennenlernens naht, sollte vorsichtig sein, vor allem wenn Geldforderungen ins Gespräch kommen.
Marco Liechti gehört einem Dreierteam der Basel Polizei an, das seit Jahren Firmen, Vereine und Institutionen aller Art sowie Einzelpersonen sensibilisiert und berät. Gerade Klein- und Mittelbetriebe (KMU) drohen in ernsthafte Schwierigkeiten zu kommen, wenn wichtige Daten von Kriminellen blockiert werden. Das Erpressungspotenzial ist gross. Einzig die Schulen zählen nicht zu Liechtis Klientel. Die Informationsarbeit über die Schattenseiten der Digitalisierung wird in diesem Bereich von der Jugend- und Präventionspolizei übernommen.

Zunehmende Cyberkriminalität

Vor Gefahren wie Einbruchdiebstählen oder Gewalt zu warnen, ist nichts Neues für den Kriminalbeamten Marco Liechti, der ursprünglich Koch gelernt hat. Später hat er sich in seiner Polizeiarbeit unter anderem Kenntnisse im Entschärfen von Bomben erworben. Mit dem Aufkommen der Computertechnologie sei aber ein zusätzlicher Gefahrenherd dazugekommen. «Die Cyberkriminalität hat in den letzten Jahren stark zugenommen», konstatiert der Ressortleiter der Kriminalprävention.
Delikte im und mithilfe des Internets sind eine Zeiterscheinung, gegen welche die Polizei ihre Kräfte in Zukunft verstärken will. Im Kanton Basel-Stadt befindet sich eine neue Abteilung Cybercrime im Aufbau. Und in Baselland gibt es ein Kompetenzzentrum dieses Namens. Zum Pflichtenheft zählen unter anderem die Identifizierung und forensische Sicherung von digitalen Spuren.
Eine typische Form von Cyberkriminalität stellt laut Liechti das sogenannte Phishing dar. Phishing ist ein Kunstwort und bedeutet «Passwörter fischen». Cyberkriminelle verwenden dabei Köder in Form von betrügerischen E-Mails oder SMS, um potenzielle Opfer auf gefälschte Websites zu locken. Hier sollen die arglosen Empfänger der Nachrichten dann ihre persönlichen Informationen wie Benutzernamen, Passwörter oder Bankdaten eingeben. Immer wieder gelingt es den Betrügern mit diesem Trick, ganze Bankkonten zu leeren.
Kriminelle werden laufend erfinderischer und versuchen, menschliche Schwächen auszunützen. So wissen sie etwa, dass das Misstrauen weniger gross ist, wenn einem Geld versprochen wird, als wenn man einen Geldbetrag bezahlen soll. «Im Moment sind SMS im Umlauf, die angeblich von der Eidgenössischen Steuerverwaltung stammen. Sie geben vor, dass die letzte Rechnung zweimal bezahlt wurde und ein Beitrag zurückerstattet wird», warnt etwa das nationale Zentrum für Cybersicherheit. Immer wieder gibt es Menschen, die dieser Versuchung nicht widerstehen können. Doch Liechti warnt: «Klicken Sie gar nicht erst auf den Link. Das SMS sollte man umgehend löschen.»

Anzeige erstatten

Und wenn doch etwas passiert, weil man unvorsichtig war? «Erstatten Sie in jedem Fall Anzeige», empfiehlt der Fachmann. Auch wenn die Täterschaft nicht gefunden wird, liefert eine Anzeige der Polizei oft wertvolle Erkenntnisse über das Vorgehen der Kriminellen. Sie sind für die weitere Polizeiarbeit wichtig. Dass man sich bei heiklen Sexgeschichten schämt und finanziellen Forderungen lieber nachkommt, als in der Öffentlichkeit blossgestellt zu werden, kann Marco Liechti verstehen. Dennoch sollte man sich auch in solchen Fällen überwinden und die Polizei kontaktieren.
Immer mehr Menschen wissen inzwischen, dass sie ihre elektronischen Hilfsmittel gut sichern soll(t)en, um nicht selbst ein Opfer der Digitalisierung zu werden. Bei der Anwendung, etwa der Installation von Programmen oder Virenschutz, ist die Polizei aber kein «Freund und Helfer». «Nein», betont Liechti auf die entsprechende Frage, «wir klären die Menschen nur auf, was sie tun müssen, damit sie nicht übers Ohr gehauen werden.» Wer wissen will, mit welchen Massnahmen respektive Handgriffen man seinen Computer oder das Smartphone konkret sichert, ist zum Beispiel bei den Angeboten von Pro Senectute im Bereich der digitalen Medien besser aufgehoben. ■

«Im Moment sind SMS im Umlauf, die angeblich von der Eidgenössischen Steuerverwaltung stammen. Sie geben vor, dass die letzte Rechnung zweimal bezahlt wurde und ein Beitrag zurückerstattet wird. Klicken Sie gar nicht erst auf den Link. Das SMS sollte man umgehend löschen.»

Fünf Schritte für Ihre digitale Sicherheit

Die Schweizerische Kriminalprävention – eine interkantonale Fachstelle – zeigt unter dem Titel «5 Schritte für Ihre digitale Sicherheit», wie man sich erfolgreich vor Betrügern schützt. Denn bei einem erfolgreichen Angriff können Kriminelle elektronische Geräte wie Computer, Tablets und Smartphones hacken und ihren Besitzern so einen grossen Schaden zufügen. Nach dem Eindringen ins System lassen sich Daten verändern, löschen und Informationen missbräuchlich verwenden. Immer wieder kommt es etwa vor, dass auf Kosten der Besitzerinnen und Besitzer im Internet eingekauft wird.

So schützen Sie sich vor Missbräuchen

1

Daten sichern

Damit wichtige Texte, Dokumente, E-Mails oder Fotos nicht verloren gehen (auch durch Fehlmanipulationen oder einen Defekt der Festplatte), sollten Sie die Daten regelmässig auf einer externen Festplatte, DVD, CD, einem Stick oder online in einer Cloud – einem virtuellen Datenspeicher im Internet – speichern.

2

Mit Virenschutz und Firewall überwachen

Jedes digitale Gerät hat zahlreiche Eingangstüren und kann schutzlos unter Umständen innert kürzester Zeit durch Schadsoftware infiziert werden. Diese öffnet unberechtigten Dritten Tür und Tor der Geräte für Missbrauch. Verwenden Sie deshalb ein Virenschutzprogramm.

3

Mit Updates vorbeugen

Die Hersteller von Programmen und Apps kümmern sich in der Regel zuverlässig um die Sicherheit ihrer Software. Laden Sie deshalb die nötigen Programme und Apps immer von der Herstellerseite herunter. Aktivieren Sie zudem die automatische Updatefunktion für das Betriebssystem des Geräts. Verwenden Sie für den Zugang ins Internet zudem nur die aktuelle Version eines Webbrowsers wie Firefox, Safari oder Edge.

4

Onlinezugänge schützen

Gehen Sie mit Passwörtern vorsichtig um, und vermeiden Sie alles, was sich leicht herausfinden lässt; also keine Namen von Kindern oder Geburtstagsdaten verwenden. Ein sicheres Passwort zu erstellen, ist nicht so schwer.
Merken Sie sich einen Satz, zum Beispiel: **I**ch **b**in **z**um **4. M**al **V**ater **g**eworden.
Daraus wird dann das komplexe Passwort **Ibz4.MVg**, das (nur) Sie sich gut merken können.

5

Aufpassen – wachsam sein

Seien Sie beim Surfen im Internet stets wachsam, und überlegen Sie gut, wem Sie Ihre persönlichen Informationen preisgeben. Auch Misstrauen ist angezeigt: Finanzinstitute, Telekommunikationsanbieter und sonstige Dienstleistungsunternehmen fragen nie nach einem Passwort, weder per Telefon noch per E-Mail oder SMS. Holen Sie sich bei Unsicherheit Unterstützung bei einer Fachperson.