«Die Cyberkriminellen arbeiten brutal

Hackerangriffe nehmen zu Digitalisierung und Homeoffice öffnen kriminellen Hackern Tür und Tor. IT-Sicherheitsexperten wie der Berner Sophus Siegenthaler sind darum immer gefragter.

Michael Bucher und **Andres Marti**

Sophus Siegenthaler sieht ein bisschen aus wie jemand, der sich als Hacker verkleidet hat. Der 37-jährige Informatiker trägt Vollbart, Sneakers und einen schwarzen Kapuzenpullover. Darauf angesprochen, meint er schmunzelnd: «Ich weiss, ich erfülle jedes Klischee.» Dazu passt folgende Pointe: Müssen Medien das Thema Hacker bebildern, so greifen sie häufig auf ein gewisses Agenturfoto zurück. Der abgebildete Typ im Hoodie, der im dunklen Zimmer Buchstabencodes auf dem Bildschirm studiert – das ist Sophus Siegenthaler.

Das Geschäftsmodell seiner Cyllective AG beschreibt Siegenthaler so: «Die Kunden bezahlen uns, damit wir ihre IT-Systeme angreifen und Sicherheitslücken finden, bevor es die Bösen tun.» Er bezeichnet sich als «ethischen» Hacker im Dienste eines Kunden. Wobei er den Begriff «Hacker» ablehnt, da damit im Allgemeinen eher Cyberkriminelle gemeint sind. IT-Security-Engineer sei die korrekte Bezeichnung seiner Tätigkeit.

Die Arbeitsstätte befindet sich im Untergeschoss eines ehemaligen Industriegebäudes im Berner Holligenquartier. Es sind Unternehmen jeglicher Grösse, die sich von Siegenthaler und seinem zehnköpfigen Team beraten lassen. Das Geschäft scheint gut zu laufen: Kürzlich ist das Team in einen grösseren Raum umgezogen.

Kriminelles Grundrauschen

Warum es Leute wie ihn braucht, demonstriert Siegenthaler auf einem Bildschirm an der Wand: Eine digitale Weltkarte zeigt die Anzahl Cyberangriffe auf sogenannte Honeypots in Echtzeit. Diese virtuellen «Honigtöpfe» täuschen Schwachstellen vor, um Angriffe zu provozieren, und dienen damit als Frühwarnsystem. 32'000 Attacken pro Minute registrieren die 19 Sensoren. Stellt man sich Internetkriminalität als Pyramide vor, wäre dies die erste Stufe. Die Fachleute nennen es das «Grundrauschen». Experten sind sich einig: Dieses Rauschen, es wird immer lauter.

Dass Internetkriminalität auch in der Schweiz boomt, zeigen die jüngsten Zahlen des Nationalen Zentrums für Cybersicherheit des Bundes. 2022 sind dort rund 34'000 Meldungen zu Cybervorfällen eingegangen – dreimal so viele wie noch 2020. Weil viele Firmen Angriffe nicht melden, dürfte die Dunkelziffer um ein Vielfaches höher sein.

Die Gemeinden Montreux VD und Rolle VD, Suisse Velo, die Emil Frey Gruppe, Comparis, die Spitalgruppe Hirslanden, das Rote Kreuz – sie alle wurden in letzter Zeit Opfer von Cyberattacken. Es ist bloss ein kleiner Ausschnitt einer langen Liste. Jüngstes Beispiel ist die Universität Zürich, die letzten Donnerstag einen gross angelegten Hackerangriff auf ihre IT-Infrastruktur publik machte. «Die organisierte Kriminalität findet heute hauptsächlich im virtuellen Raum statt», sagt Sophus Siegenthaler. Eine Bank überfalle heute praktisch niemand mehr. Zugenommen haben aber vor allem Erpressungen. Dabei infiltrieren Kriminelle Firmennetzwerke mittels sogenannter Trojaner und verschlüsseln anschliessend die Daten. Oft läuft die Erpressung mehrstufig ab: Es wird nicht nur der Betrieb lahmgelegt, sondern auch gedroht, die Daten – beispielsweise Kreditkartennummern von Kunden des Webshops – im Darknet zu veröffentlichen oder zu verkaufen. Der betroffenen Firma droht ein riesiger Rufschaden. Experten schätzen, dass 40 Prozent der Erpressten zahlen.

Wie viel Geld sich auf diese Weise erpressen lässt, zeigen die wenigen spektakulären Fälle, die an die Öffentlichkeit gelangen. Die Lösegeldforderungen orientieren sich dabei grob am Umsatz der betroffenen Firma, der ja meist ebenfalls irgendwo im Internet publiziert ist. Für die Entschlüsselung von über 3000 Media-Markt-Servern verlangten Kriminelle 50 Millionen Dollar. Ob der Konzern gezahlt hat, ist nicht bekannt.

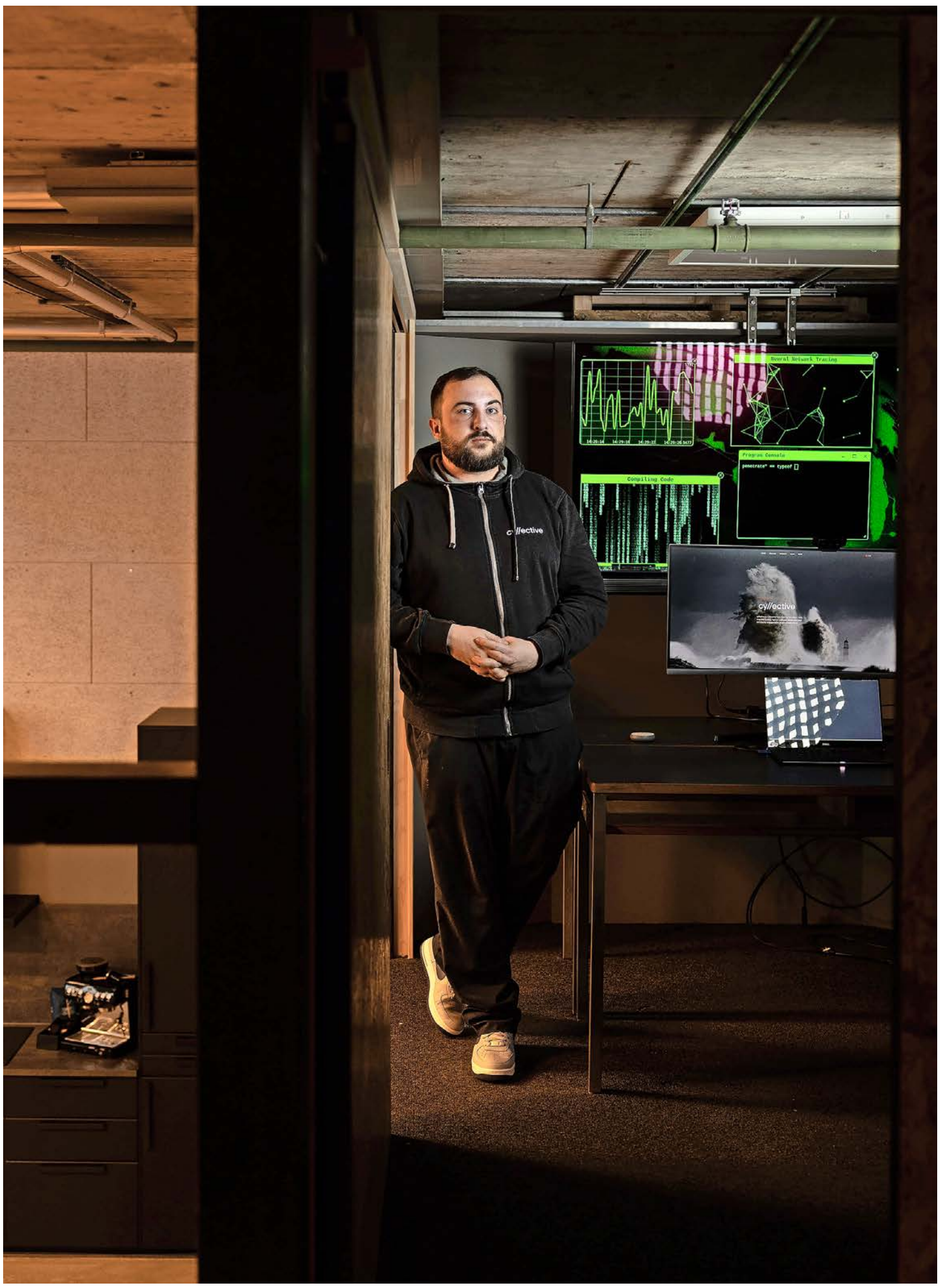
> «Die organisierte Kriminalität findet heute hauptsächlich im virtuellen Raum statt. Eine Bank überfällt praktisch niemand mehr.»
>
> **Sophus Siegenthaler**
> Cybersecurity-Experte

Ein Fall, bei dem bezahlt wurde, ist jener um das US-Unternehmen Colonial. Fünf Millionen Dollar Lösegeld zahlte die Betreiberfirma der wichtigsten Pipeline in den USA vor zwei Jahren einer Hackerbande. Wegen des Angriffs war an etlichen Tankstellen der Sprit ausgegangen.

Verwaltung muss aufrüsten

Da kriminelle Hackerbanden meist opportunistisch vorgehen – Opfer werden alle, die sich nicht genug schützen –, müssen auch Verwaltungen wie jene im Kanton Bern immer mehr in digitale Sicherheit investieren. Erst recht, da bei den kantonalen Amtsstellen ab nächstem Monat im Austausch mit der Bevölkerung und Wirtschaft offiziell der Grundsatz gilt: «digital first». Geregelt wird die Digitalisierung der Direktionen von einem neuen Cybersecurity-Gesetz, welches derzeit in der Vernehmlassung ist.

Der Schutz sensibler Daten gehört zum Kerngeschäft der Bedag. Das Informatikunternehmen mit rund 450 Angestellten und einem Umsatz von knapp 100 Millionen Franken gehört zu 100 Prozent dem Kanton Bern. Praktisch alles, was die Kantonsverwaltung an Daten produziert, wird im Rechenzentrum der Bedag gespeichert. Darunter sind schützenswerte Daten wie Steu-



«Ich weiss, ich erfülle jedes Klischee»: Der «ethische Hacker» Sophus Siegenthaler trägt während der Arbeit im Kellergeschoss gerne einen dunklen Kapuzenpullover. Foto: Beat Mathys

Kleines Cybercrime-Glossar

Malware: Oberbegriff für Schadsoftware, wie Viren, Würmer, Trojaner. Die erste bekannte Malware war der Wurm «Creeper». Er verbreitete sich Anfang der 1970er-Jahre im Arpanet, einem Vorläufer des heutigen Internets.
Zombie: Ein Zombie (auch Bot genannt) ist ein durch Viren oder Trojaner infiziertes Gerät (PC, Telefon, Kamera etc), das ohne Wissen des Users von Kriminellen kontrolliert und ferngesteuert wird.
Botnet: Auch Zombiefarm genannt, ist ein Netzwerk mehrerer infizierter Rechner. Betreiber von Botnets versenden damit Spam- und Phishing-Mails. Solche Botnets können im Darknet gekauft oder gemietet werden.
DDoS-Attacke: Sogenannte Distributed-Denial-of-Service-Angriffe gibt es seit über zwanzig Jahren. Meist wird damit mit einem Botnet ein Server mit Datenanfragen überflutet, bis er zusammenbricht (Denial of Service: englisch für Dienstverweigerung).
Ransomware: Trojaner, welche Daten auf dem infizierten System verschlüsseln oder den Zugriff auf sie verhindern. Für die Entschlüsselung wird ein Lösegeld (Englisch: ransom) gefordert. Wird nicht bezahlt, sind sie Daten verloren – oder sie werden im Darknet veröffentlicht.
Social Engineering: Im Gegensatz zu technischen Angriffen zielt Social Engineering auf das menschliche Verhalten. Kriminelle versuchen dabei, das Vertrauen des Opfers zu gewinnen. Eine der bekanntesten Varianten ist das Phishing.
Phishing: Abgeleitet vom englischen Wort «fishing» für Angeln: Mit gefälschten Mails werden potenzielle Opfer dazu gebracht, infizierte Post zu öffnen oder persönliche Daten preiszugeben. Phishing ist für über 90 Prozent aller Cyberattacken verantwortlich.
CEO-Betrug: Massgeschneiderter Angriff (Spear-Phishing) auf die Finanzabteilung eines Unternehmens. Im Namen des Chefs oder Präsidenten der Firma wird verlangt, dass eine dringende Zahlung getätigt wird.

effizient»

«Versuche, bei uns einzudringen, erfolgen permanent und nehmen stetig zu».

Dario Verrengia
Sicherheitsverantwortlicher bei Bedag

erunterlagen, Schulzeugnisse oder Betreibungen.

«Versuche, bei uns einzudringen, erfolgen permanent und nehmen stetig zu», sagt der Sicherheitsverantwortliche Dario Verrengia im Gespräch mit dieser Zeitung. Rund 150 Angriffe registriert die Bedag laut eigenen Angaben täglich. Die ungezählten Phishing-Mails – die meisten von Spamfilter und Firewall abgewehrt – nicht mitgezählt.

Hinter den Angriffen auf die Bedag steht jedoch in den wenigsten Fällen ein Mensch. «99 Prozent der Attacken laufen automatisiert ab», sagt Verrengia. Es sind Automaten, sogenannte Bots, die das Internet rund um die Uhr nach Schwachstellen durchsuchen. «Sie machen die Vorarbeit für die Hacker. Entdecken die Bots eine Schwachstelle, entscheiden die Hacker nach einer Kosten-Nutzen-Analyse, ob sich ein Angriff lohnt.» Es zeigt, wie hochprofessionell kriminelle Hackerbanden mittlerweile vorgehen.

Bislang habe man bei der Bedag einen «Breach» – also einen Einbruch oder Infizierung – verhindern können, sagt Verrengia. Unter dem Stichwort «Security Awareness» werden die Bedag-Angestellten darauf sensibilisiert, im Zweifelsfall lieber eine E-Mail zu viel zu melden. Denn nach wie vor gilt: «Das schwächste Glied in der Sicherheitskette ist der Mensch», so Dario Verrengia.

Hypervernetzte Gesellschaft

Dass die Internetkriminalität stetig zunimmt, ist für Roman Hüssy eine logische Folge der fortschreitenden Digitalisierung: «Immer mehr Menschen – und damit auch Kriminelle – haben Zugang zum Internet.» Gleichzeitig würden immer mehr verwundbare Geräte ans Internet angehängt: Kühlschränke, Babyphones, Videokameras.

Der IT-Sicherheits-Experte gründete vor 15 Jahren Abuse.ch – eine Plattform, die Malware und Botnets analysiert und von der IT-Sicherheitsbranche und Strafverfolgungsbehörden weltweit genutzt wird. In seinen Anfangszeiten wurde Hüssy selber einmal Ziel von Cyberkriminellen: 2008 verschickten sie an über 100'000 Schweizer Mailadressen eine fingierte Selbstmorddrohung in seinem Namen. Vermutlich aus Rache, weil er vor einem Trojaner gewarnt hatte, der Kriminellen Zugang zu Schweizer Bankkonten verschafft hätte.

Die Mehrheit der schädlichen Software stelle für Unternehmen allerdings keine grosse Gefahr dar. «Die grosse Masse an Malware bleibt in den Spamfiltern und Firewalls hängen». Grundsätzlich gelte die Regel: «Je zielgerichteter die Malware, desto komplexer und gefährlicher die Angriffe.»

Schweiz ist nur Mittelmass

Ein seit Jahren unentwegter Mahner ist Nicolas Mayencourt. Er ist Geschäftsführer und Gründer des IT-Sicherheitsunternehmens Dreamlab Technologies mit Sitz im Berner Monbijouquartier. Seine Firma erarbeitet seit 27 Jahren Sicherheitskonzepte und -lösungen für Kunden auf vier Kontinenten.

In der Schweiz werde zwar die Digitalisierung übergreifend vorangetrieben, jedoch bleibe dabei die Sicherheit der IT-Infrastruktur meist auf der Strecke, sagt Nicolas Mayencourt. «Das ist, als bauten wir eine Stadt auf Treibsand.» Er verweist auf die jüngsten Zahlen des «Global Cybersecurity Index» der Fernmeldeunion. Bei 182 Ländern rangiert die Schweiz dort auf Platz 42 – hinter Aserbaidschan und Tansania.

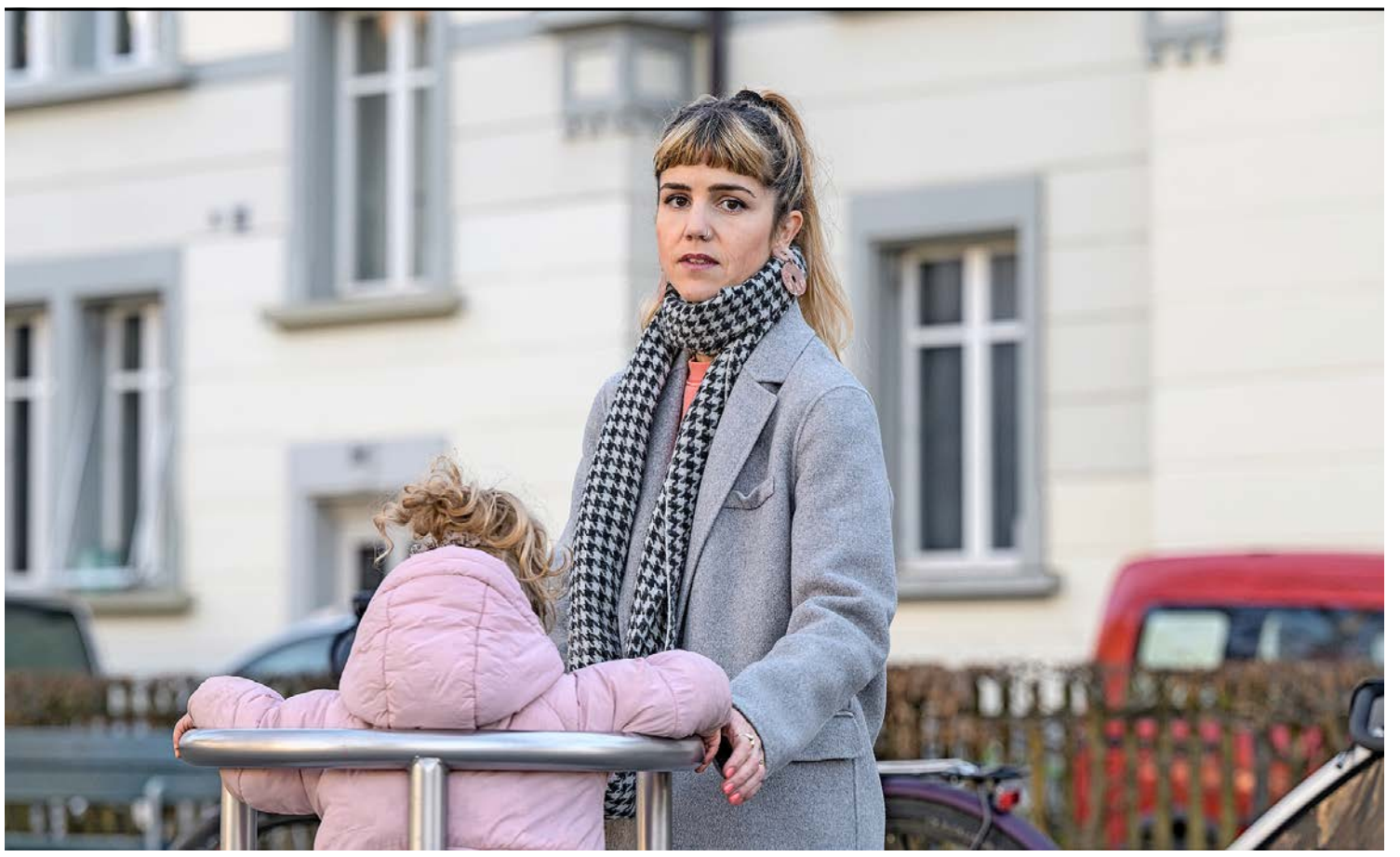
Das Thema werde immer dringlicher. Nicht zuletzt wegen der Corona-Pandemie. «Diese gab der Digitalisierung einen starken Schub. Gleichzeitig hat sich dadurch die Angriffsfläche explosionsartig vergrössert», hält Mayencourt fest. Dem stimmt auch Sophus Siegenthaler zu: Die Pandemie sei für die kriminelle Hackerszene wie ein «Dammbruch» gewesen.

Einfallstor Homeoffice

So mussten etwa unzählige Firmen innert kürzester Zeit Mitarbeitende ins Homeoffice schicken, wo diese oft mit ihrem schlecht geschützten Privatgerät auf das Firmennetzwerk zugriffen. «Es musste alles schnell gehen», sagt Siegenthaler, «auf die Sicherheit hat dabei niemand gross geschaut.» Doch auch bei einer anderen direkten Folge der Pandemie rieben sich laut dem IT-Security-Experten Hackerbanden die Hände: «Online-Shopping hat in jener Zeit ebenfalls massiv zugenommen», sagt er, «und damit auch das Betrugspotenzial.»

Dreamlab-Gründer Mayencourt findet, es brauche verbindliche Mindeststandards an Cybersecurity in Verwaltungen auf allen Ebenen. «Auch die Schweizer Wirtschaft sollte in ihrem eigenen Interesse in die Pflicht genommen werden», sagt er. Cybersecurity müsse bei Firmen denselben Stellenwert erhalten wie das Controlling der Finanzen.

«Gerade bei KMU oder Gemeindeverwaltungen fehlt das Gefühl der eigenen Verletzlichkeit gegenüber Cyberkriminalität», sagt Mayencourt. Viele denken sich: Was gibt es für einen Hacker bei uns schon zu holen? Für Mayencourt eine fatale Einschätzung. Von gezielter und von langer Hand geplanter Wirtschaftsspionage dürften KMU und Gemeindeverwaltungen zwar in der Regel verschont bleiben, doch der weitaus grössere Teil der kriminellen Hackerbanden operiere komplett anders. «Sie arbeiten pragmatisch, professionell und brutal effizient. Sie schlagen dort zu, wo es am einfachsten etwas zu holen gibt.»



«Meine Tochter ist kein Roboter», sagt Fabia Dellsperger. Die Mutter kritisiert die neue Regel. Foto: Franziska Rothenbühler

Berner Eltern müssen ihre Kinder auf die Viertelstunde genau abholen

Stress wegen neuer Kita-Regel Die städtischen Kitas verlangen neu verbindliche Bring- und Abholzeiten. Doch ist das mit einem Kleinkind und je nach Job realistisch?

Es ist eine Neuerung, die für Ärger sorgt: Mitte Januar informierten die städtischen Kindertagesstätten in Bern darüber, dass die flexiblen Zeiten fürs Bringen und Abholen der Kinder abgeschafft werden. Während bisher am Morgen und Abend jeweils ein Zeitfenster von rund zwei Stunden für die Übergabe galt, müssen die Eltern künftig auf die Viertelstunde genau angeben, wann sie den Nachwuchs bringen und wieder abholen.

Bei einigen der betroffenen Eltern kommt das gar nicht gut an. «Meine Tochter ist kein Roboter, sondern ein Kind am Anfang seiner Trotzphase», sagt etwa Fabia Dellsperger. Deshalb gelinge es oft nicht, pünktlich aus dem Haus zu kommen. «Manchmal macht die Tochter mit, manchmal gar nicht», berichtet die Mutter.

Eltern wehren sich mit Protestbrief

Auch aus beruflichen Gründen sei die neue Regelung nicht praktikabel. «Es kann sein, dass wir spontan auf einen Kunden reagieren müssen», so Dellsperger, die Mitinhaberin einer Werbeagentur ist. Jede Woche sei anders. «Eigentlich wäre es die Aufgabe der Kitas, die Vereinbarkeit von Familie und Beruf zu ermöglichen, doch das ist das Gegenteil davon.» Mit anderen Eltern hat sie sich deshalb mit einem Brief gegen die Änderungen gewehrt.

Dellsperger vermutet hinter der neuen Regelung vor allem eine Sparmassnahme. Damit liegt sie teils richtig. Weil die Ressourcen knapp sind, möchte die Stadt Bern während der Randzeiten nur so viele ausgebildete Betreuende aufbieten, wie aufgrund der anwesenden Kinder nötig sind. «Wir versuchen lediglich, unsere Planung zu optimieren», verteidigt die Leiterin der Kitas Stadt Bern, Renata Rotem, das Vorgehen. Sie betont zudem, dass man bei Verspätungen kulant sei und die deklarierten Bring- und Abholzeiten nicht in Stein gemeisselt seien. Sie liessen sich jederzeit ändern.

Hintergrund der neuen Regel ist laut Renata Rotem die neue kantonale Verordnung über den Betrieb von Kitas. Diese lege den Betreuungsschlüssel genauer fest als früher. Während der Kernzeiten sei klar, wie viele Kinder auf einer Gruppe seien. «Doch während der Bring- und Abholzeiten ist das eine dynamische Sache», erklärt Rotem. Ab sechs Kindern braucht es zwei ausgebildete Betreuungspersonen, ab 15 Kindern müssen drei anwesend sein und jeweils eine weitere für die nächsten sieben Kinder. Und das immer ab dem ersten zusätzlichen Kind.

Allerdings geht es laut Rotem nicht in erster Linie ums Sparen – sondern auch darum, sparsam mit dem knappen Personal umzugehen. In den 13 städtischen Kitas seien derzeit sieben Stellen unbesetzt, schweizweit seien es rund 1000. «Der Fachkräftemangel ist längst in der Kita angekommen.» Eine der Kitas könne keine zusätzlichen Kinder mehr aufnehmen, solange die Stelle nicht besetzt sei.

Private Kitas ziehen nicht nach

Obwohl die städtischen Kitas so viele Fachpersonen Betreuung (Fabe) ausbildeten wie möglich, würden diese vom Markt rasch absorbiert. Die Fabe könnten nämlich auch in Tagesschulen arbeiten und sogar auf der Basisstufe unterrichten. Angesichts des grossen Lehrpersonenmangels ist Letzteres eine attraktive Option. «In der Schule werden die Fabes viel besser bezahlt als in den Kitas», sagt Rotem.

«Eigentlich wäre es Aufgabe der Kitas, die Vereinbarkeit von Familie und Beruf zu ermöglichen, doch das ist das Gegenteil.»

Fabia Dellsperger
Mutter, Mitinhaberin einer Werbeagentur

Verbindliche Zeiten beim Bringen und Abholen der Kinder? Was die städtischen Kitas nun einführen, ist für die meisten privaten Anbieter in Bern zurzeit kein Thema. Die von dieser Zeitung angefragten Kitaketten Pop e Poppa, Kibe Plus sowie Kitas Murifeld wollen alle an ihrem bisherigen Modell festhalten.

«Für viele berufstätige Eltern ist es schwer genug, ihren Arbeitsalltag zu planen – da wollen wir ihnen mit fixen Bring- und Abholzeiten das Leben nicht noch schwerer machen», sagt Lucien Brahier, Geschäftsführer von Kibe Plus. Die Kette betreibt in Berns Agglomeration 13 Kitas und bietet morgens und abends jeweils Zeitfenster von ungefähr zwei Stunden an.

Ähnlich tönt es bei Pia Aeschimann von den Kitas Murifeld. «Natürlich wären für uns als Unternehmen verbindliche Bring- und Abholzeiten auch einfacher», sagt sie. Letztlich gehe es aber um ein Dienstleistungsangebot, bei dem eine gewisse Flexibilität erwartet werden könne. Für sie spricht zudem noch etwas anders gegen fixe Zeiten: «Das Abholen der Kinder ist schon so oft mit Stress verbunden.» Komme noch eine zeitlich enge Vorgabe dazu, erhöhe das den Stress und die Belastung noch mehr, so die Kitaleiterin. «Die Leidtragenden sind am Ende meist die Kinder.»

Ein Franken pro Minute Verspätung

Bei einigen wenigen Kitas gehören fixe Bring- und Abholzeiten derweil zum Geschäftsmodell. So bietet etwa die schweizweit tätige Kette Strampolino, die auch in Bern einen Standort betreibt, unter anderem ein minutengenaues Reservationssystem an. Das heisst: Eltern können ganz spezifische Betreuungszeitfenster buchen und auch die Betreuungstage kurzfristig wechseln. Abgerechnet wird dabei nicht pauschal nach Tagestarifen, sondern nach Minute. Holt man sein Kind verspätet ab, kostet dies nach einer Kulanzzeit von einer Viertelstunde extra – pro Minute einen Franken. Laut der Strampolino-Geschäftsleitung ist die Nachfrage nach diesem besonders flexiblen Modell in den vergangenen Jahren stark gestiegen.

Gehen die städtischen Kitas mit ihrer Massnahme zu weit? Aude Spang, bei der Gewerkschaft Unia zuständig für Gleichstellungsthemen, hat sowohl für die Kitas wie für die Eltern Verständnis. «Die Kinderbetreuung ist für beide Seiten prekär», sagt sie. Weil Kitas zu wenig Ressourcen hätten, seien sie auf eine möglichst hohe Planbarkeit angewiesen. Doch für die Eltern bedeute es weniger Flexibilität.

Aber gerade für Eltern mit Präsenzzeiten, wenig Zeitautonomie und kurzfristigen Arbeitseinsätzen erzeugten fixe Bring- und Abholzeiten in Kitas noch mehr Druck, so Spang. Höher qualifizierte Elternteile, die auch während der Arbeit weitgehend selbst über ihre Zeit verfügen könnten, hätten die Möglichkeit, sich das Bringen und Abholen der Kinder besser zu organisieren.

Wie flexibel müssen Arbeitgebende sein?

Die Unternehmerin Sarah Steiner nimmt allerdings auch die Arbeitgebenden in die Pflicht. Steiner hat in Zürich selbst eine Kita gegründet und berät Firmen dabei, wie sie ihren Mitarbeitenden die Vereinbarkeit von Beruf und Familie ermöglichen können. «Auch innerhalb der immer flexibleren Arbeitswelt muss man sich gewisse Rahmen stecken und die Firmenkultur danach richten», sagt sie. Bereits mit kleinen Dingen wie etwa familienfreundlichen Sitzungszeiten könnten Arbeitgebende viel zur Vereinbarkeit beitragen. Von fixen Bring- und Abholzeiten in der Kita hält aber auch sie nichts.

Naomi Jones und **Christoph Albrecht**