Marktkonzentration: Grossunternehmen drängen den Wettbewerb zurück *Seite 10*

Neue Zürcher Zeitung

NZZ – GEGRÜNDET 1780

Freitag, 3. Juli 2020 · Nr. 152 · 241. Jg. AZ 8021 Zürich · Fr. 4.90 · €4.90

KEYSTONE

Die dunkle Seite des Antifaschismus

Auch unter demokratischen Linken steht der Antifaschismus seit einigen Jahren wieder hoch im Kurs. Oft wird der Kreis der Faschismusverdächtigen auffällig weit gefasst. Ob diese nach wissenschaftlichen Kriterien wirklich faschistisch sind, ist dabei egal. Bis zum antidemokratischen und militanten Antifaschismus ist es dann bisweilen nicht mehr weit.

Feuilleton, Seite 27

Das Home-Office bleibt uns erhalten

85 Prozent der Firmen wollen das Modell auch nach der Pandemie anbieten

cei. · Bis Mitte Juni hiess es: Wer zu Hause arbeiten kann, soll das auch. Doch inzwischen hat der Bundesrat diese Empfehlung aufgehoben – und bisher auch nicht wieder eingeführt, obwohl die Covid-19-Fälle wieder dreistellig sind. Von einem normalen Arbeitsalltag wie vor der Krise kann jedoch weiterhin nicht gesprochen werden, wie eine Umfrage bei grossen Arbeitgebern aus diversen Branchen zeigt.

Die Abstands- und Hygieneregeln erlauben es nicht, dass man die Büroimmobilien wie vorher auslastet. Der Stromkonzern Axpo spricht von einer maximalen Belegungsquote von 35, die Beratungsfirma PwC von einer von 60 Prozent. Auch bei den Grossbanken UBS und Credit Suisse dürfte immer noch gut die Hälfte der Mitarbeiter von zu Hause aus arbeiten, und der Campus des Pharmakonzerns Novartis ist weitgehend verwaist. Der Suchmaschinenanbieter Google erlaubt seinen rund 4000 Mitarbeitern in Zürich sogar, bis Ende Jahr im Home-Office zu bleiben. Ganz anders dagegen der Finanzdienstleister Partners Group, bei dem die Zentrale fast wieder voll besetzt ist. Die Zusammenarbeit im Büro sei essenziell, heisst es bei der Zuger Firma. Eine Umfrage des sozialen Netzwerkes Xing bei über 1100 Personalverantwortlichen aus der Schweiz, Deutschland und Österreich bestätigt, was aus den meisten Branchen zu hören ist: Das Home-Office wird kein vorübergehendes Phänomen sein, sondern auch nach ausgestandener Pandemie zum betrieblichen Alltag gehören. 85 Prozent der Schweizer Umfrageteilnehmer jedenfalls äussern sich in diese Richtung. Man habe mit der flexiblen Home-Office-Regelung «sehr gute Erfahrungen» gemacht, sagt Axpo stellvertretend für viele Arbeitgeber – und gewiss auch für das Gros der Arbeitnehmer.

Wirtschaft, Seite 17

Haushoher Sieg des Kremls

Putin bedankt sich für das Resultat der Abstimmung über die Verfassungsänderungen

mac. Moskau · Mit einer überwältigenden Mehrheit von 78 Prozent bei einer Stimmbeteiligung von 65 Prozent haben die russischen Stimmberechtigten nach offiziellen Angaben die von Präsident Wladimir Putin eingebrachten Verfassungsänderungen gebilligt. Putin bedankte sich im Fernsehen für die Unterstützung und das Vertrauen, das ihm entgegengebracht worden sei. Sein Sprecher hatte zuvor gesagt, faktisch habe ein triumphales Referendum über das Vertrauen in Putin stattgefunden.

Das Ausmass der Zustimmung in der Abstimmung, für die weder die Gesetzgebung über Referenden noch jene über Wahlen galt, weckte allerdings bei vielen Kritikern der Macht Zweifel. Sie sprachen von einer Zerstörung der Demokratie. Umfragen im Vorfeld der Volksbefragung hatten auf eine geringere Zustimmung hingedeutet, und Befragungen nach der Stimmabgabe in Moskau und St. Petersburg ergaben ein fast ausgeglichenes Bild. Zudem gab es zahlreiche Auffälligkeiten bei Ergebnissen einzelner Abstimmungslokale. Die siebentägige Dauer der Öffnung der Urnen, die Möglichkeit, zu Hause abzustimmen, und die Drangsalierung von Angestellten dürften sich im Resultat niedergeschlagen haben. Regionen in Süd- und Zentralrussland, im Nordkaukasus sowie in Teilen Sibiriens erzielten sehr hohe Zustimmungswerte. Die ganz im Norden Russlands gelegene autonome Region der Nenzen lehnte als einzige Provinz die Verfassungsänderungen ab.

Mit den Verfassungsänderungen kann Putin über 2024 hinaus regieren. Die präsidiale Macht wird gestärkt. In der Bevölkerung und der Elite ist die unterschwellige Unzufriedenheit aber grösser, als das Abstimmungsergebnis suggeriert. Der Kreml hat nicht viel Neues zu bieten, hat aber weitere Erwartungen geweckt.

Meinung & Debatte, Seite 9

Armee verschweigt Mängel bei der IT

Kontrolle deckt Sicherheitslücken auf

Nicht alle Systeme der Armee erfüllen die Vorgaben des Bundes für Cybersicherheit. Diese Sicherheitslücken wurden jedoch nicht vorschriftsgemäss gemeldet.

LUKAS MÄDER

Die Cyberexperten der Schweizer Armee verstecken sich hinter einem unscheinbaren Namen: Führungsunterstützungsbasis (FUB). Das ist jene Organisation, die für die hochsensible IT-Infrastruktur des Militärs zuständig ist – und deren Betrieb auch im Ernstfall sicherstellen muss. Zur FUB gehören auch die Cyberkrieger der Armee, die aktive Operationen im virtuellen Raum ausführen – zum Beispiel, um im Auftrag des Nachrichtendienstes Informationen zu beschaffen.

Doch ausgerechnet die Cyberspezialisten der Armee haben ein Problem mit der IT-Sicherheit. Nicht alle ihre Informatiksysteme erfüllen die minimalen Sicherheitsanforderungen, die in der Bundesverwaltung gelten. Dies hat die Eidgenössische Finanzkontrolle Ende letzten Jahres bei einer Prüfung entdeckt. Die Mängel waren so gravierend, dass die Finanzkontrolle nach der Entdeckung umgehend den Bundesrat informiert hat, wie ihr Direktor Michel Huissoud bestätigt. Das war am 13. Dezember 2019.

Die Bundesverwaltung kennt minimale Vorgaben im Bereich IT-Sicherheit, die alle Departemente und Ämter erfüllen müssen. Ist ihnen das nicht möglich, brauchen sie eine Ausnahmebewilligung. Zuständig dafür ist heute das neue Nationale Zentrum für Cybersicherheit (NCSC). Dieser sogenannte IKT-Grundschutz schreibt etwa vor, dass die Festplatten auf allen Rechnern verschlüsselt sein müssen zum Schutz gegen Diebstahl. Oder dass die Topologie der IT-Netzwerke inklusive ihrer Komponenten und Konfigurationen stets aktuell dokumentiert sein muss.

Unsicheres Protokoll verwendet

Diese Vorgaben hat die Armee nicht alle eingehalten und dafür auch keine Ausnahmebewilligung eingeholt. Das geht aus dem Bericht «Informatiksicherheit Bund 2019» hervor, den die NZZ gestützt auf das Öffentlichkeitsgesetz erhalten hat. Weil die bestehenden Lücken von Angreifern ausgenützt werden könnten, äussert sich die FUB nicht weiter dazu. Ein Defizit, das nach Informationen der NZZ Anfang 2020 noch bestand, war eine veraltete Version des Netzwerkprotokolls SMB. Dieses enthält Sicherheitslücken, die etwa von der Erpressungssoftware WannaCry ausgenützt werden. Im Mai 2017 befiel WannaCry über 200 000 Rechner in mindestens 150 Ländern.

Ein weiteres Problem der FUB sind die Netzwerkzugänge. Als der Bund Anfang 2016 den Cyberangriff auf den bundesnahen Betrieb Ruag bemerkte, zeigte sich rasch, dass niemand genau wusste, welche und wie viele Verbindungen es zwischen dem Netzwerk der Ruag und der Armee gab – durch die die Angreifer hätten eindringen können. Dieses Problem ist mit der Entflechtung der Ruag gelöst, bei der im April die aufwendige Einbindung des Schweizer Unternehmensteils in die Armee-Informatik abgeschlossen wurde.

Zu diesem Schnittstellenmanagement gehört aber auch die Anbindung externer Dienstleister. Geht es dabei um einen Zugang zu einem Waffensystem, besteht rasch ein Risiko für die Einsatzbereitschaft von Teilen der Armee. Wie die FUB mitteilt, sollen die laufenden Arbeiten zur vollständigen Dokumentation der Schnittstellen bis Ende 2020 abgeschlossen sein.

Nicht der erste Fall

Doch die Armee muss sich nicht nur vorwerfen lassen, dass ihre Systeme altbekannte Schwachstellen aufweisen. Sie hat diese Schwachstellen auch intern nicht gemeldet, wie dies die Departemente jährlich zu tun verpflichtet sind. Der Bericht «Informatiksicherheit Bund 2019» spricht von «relevanten Widersprüchen» zwischen der Prüfung der Finanzkontrolle und den Rückmeldungen des Verteidigungsdepartements im Rahmen des jährlichen Reportings. Konkret bedeutet dies: Das Verteidigungsdepartement hat nicht alle Lücken gemeldet. Diese falschen Angaben betreffen laut dem Bericht auch frühere Jahre.

Brisant ist die Frage nach den Gründen für diesen Widerspruch. Möglich sind zwei Erklärungen: Entweder die Armee kannte die Lücken gar nicht – was aus sicherheitstechnischer Sicht ein unangenehmes Szenario wäre. Oder aber die Armee hat die Information bewusst nicht weitergegeben – was ein Verstoss gegen die bundesrätliche Verordnung über die Bundesinformatik bedeutete.

Der Chef der Führungsunterstützungsbasis von 2018 bis Ende 2019 war der heutige Armeechef Thomas Süssli. Er selbst möchte zum Fall nichts sagen. Auch der Delegierte für Cybersicherheit, Florian Schütz, äussert sich zur Frage nach den Gründen nicht – vermutlich, um die Zusammenarbeit nicht zu belasten. In einer gemeinsamen schriftlichen Stellungnahme von Armee und Cyberdelegierten bleibt die Antwort unklar.

Die Prüfer der Finanzkontrolle waren dem Vernehmen nach jedoch überzeugt, dass die FUB die Sicherheitslücken bewusst nicht gemeldet hatte. So war dies zumindest auch in einer ersten Version des Berichts festgehalten. Dazu passt auch die in der Armee vorhandene Ansicht, dass zivile Stellen keine Aufsicht über die Waffensysteme von Luftwaffe oder Heer ausüben können. In dieser Logik muss sich die FUB auch nicht für Sicherheitsmängel rechtfertigen oder dafür gar eine Ausnahmebewilligung einholen – obwohl die Verordnungen des Bundesrats eigentlich klar sind.

Die FUB hat die Empfehlungen der Finanzkontrolle inzwischen akzeptiert, wie es auf Anfrage heisst. Sie will bis Ende 2021 die Vorgaben zur IT-Sicherheit erfüllen und wo nötig Ausnahmebewilligungen einholen.

Redaktion und Verlag: Neue Zürcher Zeitung, Falkenstrasse 11, Postfach, 8021 Zürich, Telefon: +41 44 258 11 11,
Leserservice/Abonnements: +41 44 258 10 00, www.nzz.ch
Wetter: 24, TV/Radio: 30, Traueranzeigen: 6, Impressum: 24

9 772297 322004 20152