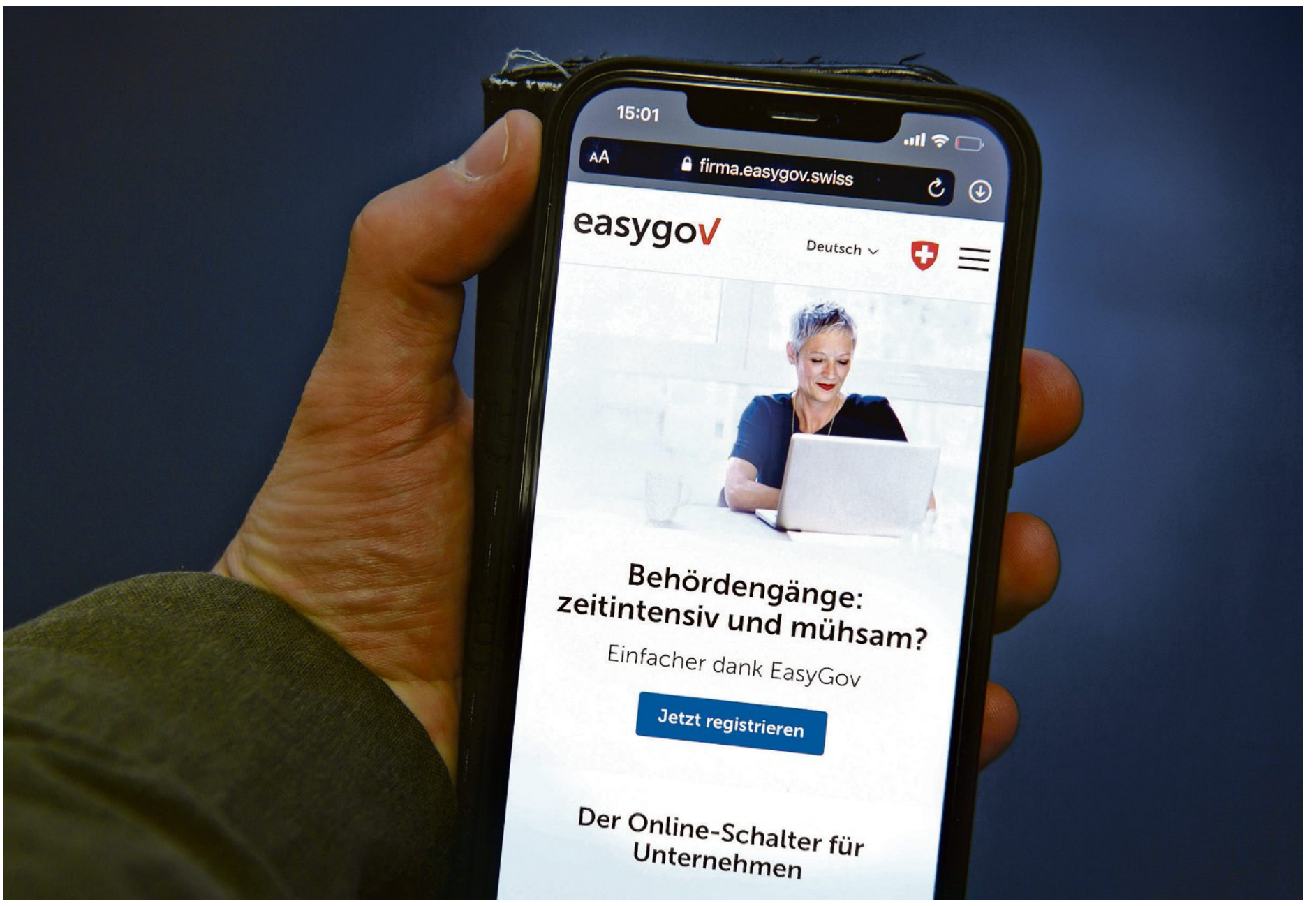
Der peinliche Datenklau

Hackerangriffe Unbekannte haben die Namen von 130’000 Firmen gestohlen, die beim Bund Wirtschaftshilfe beantragt haben. Es ist nur der letzte einer ganzen Reihe von Cyberangriffen. Die Bedrohung nimmt zu.



Mühsam? Unbekannte haben dem Portal Easygov offenbar ohne allzu grosse Anstrengung die Namen von 130’000 Unternehmen entwendet. Foto: Keystone

Mathias Born, Hans Brandt und **Roland Gamp**

Die Messe Schweiz. Der Krankenkassen-Vergleichsdienst Comparis. Die Neuenburger Kantonalbank. Sie alle wurden kürzlich Opfer. Von «kriminellen Hackern», von Digital-Erpressern, der Cybermafia. Die Begrifflichkeiten sind noch nicht wirklich trennscharf definiert, doch eines ist klar: Die Angriffe aus dem Netz, die tatsächlich Konsequenzen für den Alltag einer Firma oder einer Verwaltungsstelle haben, nehmen zu.

«Die Schweiz hat dieses Jahr 30 Prozent mehr Cyberangriffe erlebt als noch letztes Jahr. Das zeigt, dass der Staat, aber auch viele Unternehmen zu wenig gut geschützt sind.» Franz Grüter ist SVP-Nationalrat, IT-Unternehmer und einer der wenigen Bundesparlamentarier mit fundiertem Wissen zum Thema. Kürzlich hat er in der «Rundschau» eine Art «Cyber-Wetterbericht» gefordert, in dem die aktuellsten Bedrohungslagen aufgeführt würden.

Dieser Wetterbericht, würde es ihn denn schon geben, hätte für gestern Donnerstag eine ziemlich schwarze Wolke angezeigt. «Kriminellen Hackern» sei es gelungen, mit einer automatisierten Abfrage die Namen von bis zu 130’000 Unternehmen von der Web-Plattform Easygov zu stehlen, teilte das Staatssekretariat für Wirtschaft (Seco) mit. All diese Unternehmen hätten letztes Jahr einen Covid-Kredit beantragt.

Die «Hacker» mussten offenbar nicht tief in die Trickkiste greifen. Die Daten waren nach aktuellem Wissensstand technisch ungeschützt. Die Kreditanträge wurden nicht im Hochsicherheitsbereich der Plattform Easygov.swiss erfasst, sondern in einem eiligst gezimmerten «Vorraum». Firmen, die einen Notkredit benötigten, erhielten von ihrer Bank den Weblink zum Erfassungstool. Dieses bot auch die Möglichkeit, Anträge anzupassen – etwa um Informationen zu ergänzen oder den Betrag zu erhöhen.

Datenklau «klar definiert»

Genau diese Funktion haben die Angreifer genutzt. Sie haben herausgefunden, dass die Plattform zuerst prüft, ob für die betreffende Firma bereits ein Antrag vorliegt. Dazu schickt sie die offizielle Identifikationsnummer des Unternehmens an eine technische Schnittstelle – eine API.

Die Angreifer haben daraufhin automatisiert die Identifikationsnummern der Schweizer Unternehmen durchprobiert – eine Fingerübung selbst für Programmieranfänger. Aus den Antworten des Servers können sie eine Liste der Firmen erstellen, die einen Antrag gestellt haben.

Betroffen sind alle Unternehmen, die einen Covid-Kredit beantragt und noch nicht zurückbezahlt haben. Neben den Firmennamen enthält die Liste auch die Information, ob ein Covid-Kredit gestellt wurde oder nicht. Dies teilt das Seco auf Nachfrage dieser Redaktion schriftlich mit. Der beantragte Kreditbetrag sei zwar Teil dieses Datensatzes gewesen, sei von den Hackern aber nicht abgefragt worden. Der gestohlene Datensatz sei somit «klar definierbar».

Ob die Hacker tatsächlich Schweizer Recht verletzt haben, müssen die Untersuchungen zeigen.

Vier von zehn Firmen zahlen Lösegeld

Die Angriffe von Hackerbanden auf Schweizer Firmen häufen sich markant. Die Dunkelziffer dürfte indes noch viel höher liegen, wie die Konsumentenzeitschrift «Beobachter» berichtet. Rund 40 Prozent der Betroffenen zahlen laut einem Experten Lösegeld. Kriminelle hätten letztes Jahr Daten von rund 2700 hiesigen Unternehmen geklaut und zum Verkauf ins Darknet gestellt, schreibt der «Beobachter». Die Zahlen im Bericht beziehen sich auf eine im Auftrag des Magazins erstellte Analyse des amerikanischen Cyberintelligence-Unternehmens Recorded Future. *(red)*

Warnten die Hacker selbst?

Das Seco bezeichnet die Datensammler als «kriminelle Hacker». Ob diese aber tatsächlich Schweizer Recht verletzt haben, müssen die weiteren Untersuchungen zeigen. Automatisierte Abfragen werden oft gemacht und sind nicht illegal: «Wer eine technische Schnittstelle ungeschützt zur Verfügung stellt, muss damit rechnen, dass diese auch benutzt wird», sagt Nicolas Mayencourt, Inhaber der Sicherheitsfirma Dreamlab. «Solange keine Sicherheitsvorkehrungen umgangen werden müssen, kann man nicht einmal von Hacking sprechen.» Auch dass die Daten in hoher Kadenz angefragt worden seien, lasse sich nicht den Angreifern anlasten: «Es ist Sache des Schnittstellenanbieters, die Anzahl Zugriffe zu limitieren.»

Ob es eine offene Schnittstelle braucht, hängt von den Anwendungen ab. Sollte allein der eigene Server Anfragen machen? Dann hätte sich die Schnittstelle einfach absichern lassen. Mussten auch andere Systeme, etwa der Banken die Infos anfordern? In dem Fall wäre die offene Schnittstelle in der Krise eine pragmatische Lösung. Sie hätte aber längst abgesichert werden müssen.

Es könne leider passieren, dass eine Schnittstelle fälschlicherweise öffentlich zugänglich sei, sagt Anwalt Martin Steiger, der sich auf Digitalthemen spezialisiert hat. «Ich hoffe, dass die Verantwortlichen aus dem Vorfall lernen und dass die IT-Sicherheit dadurch verbessert werden kann.» Die Betroffenen versuchten in solchen Fällen oft, die «kriminellen Hacker» in den Vordergrund zu rücken. «Ob aber wirklich eine Straftat vorliegt, müsste auf dem Rechtsweg geprüft werden.»

Sollten die Namen auf der Liste publik werden, so sähen sich unzählige Firmen mit Problemen konfrontiert. Denn viele Unternehmerinnen und Unternehmer haben sich die Covid-Kredite mit falschen Angaben erschlichen – oder die Gelder anschliessend zweckentfremdet. Zahlen des Seco zeigen: Derzeit sind dazu 1137 Strafanzeigen offen. Dabei geht es um eine mutmassliche Deliktsumme von über 152 Millionen Franken. Bekannt wurden bisher nur die allerwenigsten Fälle. So zeigten Recherchen dieser Zeitung, wie der Betreiber einer Hausarztkette trotz falscher Angaben über 3,5 Millionen Franken erhielt. Er wurde in der Folge wegen Betrugs, Urkundenfälschung und weiterer Delikte verurteilt.

Insgesamt konnten die Strafbehörden bisher 265 Missbrauchsfälle abschliessen. Die Namen der fehlbaren Firmen blieben geheim. Was sich mit einer Veröffentlichung der gehackten Liste ändern könnte. Denn so liesse sich einfach prüfen, wer sich nicht an die Regeln hielt. Covid-Kredite durften nämlich nur Firmen beantragen, die besonders von der Pandemie betroffen waren und nicht schon vorher finanzielle Schwierigkeiten hatten.

Wer hinter der Hackerattacke steckt, ist noch unklar. Auf die Frage, ob die Hacker mit dem Seco oder einer anderen betroffenen Stelle Kontakt aufgenommen haben, antwortet die Medienstelle: «Das Seco hat die Meldung von einer externen Person erhalten und geantwortet, dass der Hinweis sehr ernst genommen wird. Weitere Kontakte gab es nicht.» Das deutet darauf hin, dass die Hacker selbst das Seco informiert haben könnten. Die Meldung ging demnach am Dienstag ein – die problematische Schnittstelle sei noch am gleichen Tag geschlossen worden.

Für freundliche Attacken

Erich Herzog von Economiesuisse betont, wie wichtig Cybersecurity sei. Was es für ein Unternehmen bedeute, wenn bekannt werde, dass es einen Antrag für einen Covid-Kredit gestellt habe, sei sehr individuell, so Herzog. «Das hängt auch davon ab, wie ein Unternehmen in der Öffentlichkeit wahrgenommen wird.»

SVP-Nationalrat Grüter fordert, abzuklären, ob alle Sorgfaltspflichten eingehalten wurden. Das nationale Cybersicherheitszentrum habe betont, dass viele IT-Einrichtungen der öffentlichen Hand Schwachstellen hätten. «Viele der Leute sind überfordert, haben zu wenig Kenntnisse. Sie brauchen Unterstützung von Spezialisten, zum Beispiel mit freundlichen Hackerattacken, um Sicherheitssysteme zu testen.»