Abo «Story Killers»-Interview über Cybersicherheit

«Natürlich sind wir in der Schweiz ein Ziel»

Nach der Aufdeckung der Geheimtruppe «Jorge», die anbot, mit Desinformation Demokratien zu destabilisieren: Der Schweizer Sicherheitsexperte Nicolas Mayencourt sagt, wo unser Land verwundbar ist.

Oliver Zihlmann

Publiziert: 15.02.2023, 18:00

Cybersicherheits-Experte Nicolas Mayencourt.

Foto: Christian Pfander (Tamedia)

Ein gehackter Top-Politiker, Angebote für Manipulationen von Wahlen gegen Geld, Armeen von falschen Profilen in den Sozialen Medien: Am Mittwoch Vormittag deckten Journalisten eine geheime Truppe um den Israeli «Jorge» auf. Sie bietet Politikern oder reichen Geschäftsleuten an, ganze Demokratien weltweit mit Desinformation zu destabilisieren. Die monatelange Undercover-Recherche des Journalistenkonsortiums, zu dem auch der Tamedia Recherchedesk und ihr Partner Paper Trail Media gehört, trägt den Namen «Story Killers». Sie zeigt, wie ehemalige israelischen Agenten mit einer beunruhigend mächtigen Software Facebook und Tw mit Fake-Profilen fluten und so Unruhen auslösen können – oder ganz gezielt in Mail- und Telegram-Konten von führenden Politikern gelangen und in deren Namen Nachrichten versenden.

Könnte auch die Schweiz ins Visier der Cyberkriminellen gelangen? Wir haben nachgefragt bei Nicolas Mayencourt, einem weltweit tätigen Spezialisten für Cybersicherheit.

Herr Mayencourt, die Welt erfährt gerade durch die Story-Killers-Recherchen, wie eine Truppe israelischer Ex-Agenten gegen Bezahlung offerierte, Politiker in beliebigen Ländern zu hacken oder Wahlen zu manipulieren. Sind solche Angriffe eine Gefahr für die Demokratie?

Ich kenne den vorliegenden Fall nicht, aber ich würde das sofort glauben. Sehen Sie: Dank dem Internet kann man heute von überall auf der Welt in lokale politische Systeme eingreifen. Man muss nicht mit Agenten vor Ort gehen, so wie früher. Manipulationen dieser Art geschehen in der Regel vollkommen anonym und bleiben oft unerkannt. Solche Aktivitäten sind zweifellos eine reale Gefahr für die Demokratie.

Wir haben solche Kampagnen bei den Russen gesehen, die in den US-Wahlkampf eingegriffen haben. Aber offenbar kann sich heute jeder mit genügend Geld solche Manipulationen einfach kaufen?

Absolut, und das ist inzwischen ein globales Problem. Denn heute haben auch nicht staatliche Gruppen dieses Geschäft entdeckt. Meinungen zu machen und zu manipulieren, ist heute eine Ware. Das war vor 20 Jahren noch nicht so. Gleichzeitig bestehen solche Gruppen oft aus Akteuren, die teilweise parallel noch für staatliche Stellen arbeiten. Die Grenzen sind also fliessend.

Ist auch die Schweiz ein Ziel für solche Gruppen?

Wir haben führende Industrien im Bereich Pharma und Elektronik und einen der grössten Finanzplätze der Welt. Als Rohstoff-Handelsmarkt sind wir global praktisch Nummer eins. Gleichzeitig sind wir eines der wichtigsten Gastgeberländer der Welt: für die UNO, die Sportverbände wie Fifa und IOK, für das World Economic Forum. Das sind alles sehr attraktive Ziele, auch für Einflussnahmen auf dem politischen Parkett. Mit anderen Worten: Natürlich sind wir ein Ziel.

Und können wir uns wehren?

Vorweg: Die Schweiz leidet hier an kognitiver Dissonanz. Zwei Rankings zeigen das eindrücklich. Einerseits sind wir beim globalen Innovationsindex die Nummer eins. Geht es um Patente oder kreative Erfindungen, ist die Schweiz Weltspitze, und darauf können wir auch zu Recht stolz sein.

Und was ist das zweite Ranking?

Das ist der «Global Cyber Security Index» der ITU (International Telecommunication Union), welche Teil der UNO ist. Er misst in 193 Ländern der Welt, wie cyber-sicher sie sind. Hier schneidet die Schweiz aber nicht mal in den Top Ten ab. Wir liegen derzeit auf Rang 42. Nach Tansania und knapp vor Ghana.

Der Unterschied zwischen unserer Innovationskraft und unserem mangelnden Cyberschutz ist also das Problem.

Genau. Alle unsere Innovationen landen letztlich als Daten auf unseren Servern. Die internationalen Organisationen treffen sich in unseren Sitzungszimmern und Konferenzsälen. Wenn wir da bei der Sicherheit nicht ebenfalls absolute Weltspitze sind, dann ist das, als würden wir eine Einladung schicken an Hacker und Spione. Wertvolle Ziele, geringer Schutz: Das zieht magisch an. Das Risiko, dass wir gehackt oder abgehört werden, steigt damit massiv.

«Viele Gemeinden haben teils völlig ungenügende Sicherheitsstandards und wenig Ressourcen.»

Gibt es denn bekannte Fälle?

Eines der Probleme sind die Angriffe auf Gemeinden wie Neuenburg, bei denen Kriminelle Daten der Bevölkerung stehlen. Viele Gemeinden haben teils völlig ungenügende Sicherheitsstandards und wenig Ressourcen. Auch hier: wertvolle Ziele, wenig Schutz. Eine schlechte Kombination mit Blick auf Cyberkriminalität.

Warum?

Erstens haben die Gemeinden Schnittstellen zu den Servern des Bundes, und so besteht die Gefahr, dass auch der Bund in Mitleidenschaft gezogen wird. Oder der Bund ist von vornherein das eigentliche Ziel. Zweitens erbeuten die Kriminellen so extrem sensitive Daten von Zehntausenden Schweizern. Da sind AHV-Nummern drin, Pass-, Steuer- und sogar Gesundheitsdaten. Und das führt gleich zum nächsten Problem.

Nämlich?

Wenn die Kriminellen die Daten nicht mehr mit Erpressungen und Ähnlichem zu Geld machen können, dann erfolgt in der Regel eine Art Zweitverwertung. Die Daten aus der Schweiz werden dann einfach an staatliche Akteure weiterverkauft, die daran interessiert sind, etwa an gewisse Geheimdienste. Und die verfolgen dann mit den Schweizer Daten wieder ihre ganz eigenen Ziele.

Das bedeutet, wenn in der Schweiz Daten gehackt werden, dann kann man nicht ausschliessen, dass sie am Schluss auch bei Gruppen landen, die politische Ziele verfolgen wie jene in Israel.

Ja, solche Hacks verursachen mehrere Wellen von Schäden.

Es scheint erschreckend leicht zu sein, politische Einflusskampagnen wie jene der Israelis durchzuführen.

Mit dem Internet und den sozialen Medien wurde der Instrumentenkoffer für solche Kampagnen enorm erweitert. Gleichzeitig sind diese Instrumente erschreckend günstig geworden. Es ist inzwischen sehr einfach, vollständig automatisiert 100’000 Facebook- oder Linkedin-Konten zu erstellen, und einfach mal anzufangen, eine Meldung oder eben eine Desinformation zu verbreiten und damit Meinungen zu beeinflussen. Und gerade jetzt wird alles noch viel gefährlicher.

Inwiefern?

Schauen Sie, was Chat GPT und ähnliche künstliche Intelligenzen leisten. Sie können heute auf Knopfdruck 100’000 Texte mit Desinformationen innert Minuten raushauen. Und diese Texte sind gut geschrieben und scheinen von Menschen zu stammen. Noch vor ein paar Jahren hätte man dafür sehr viele Leute anstellen müssen. Und Chat GPT ist obendrein noch gratis und für jedermann verfügbar.

Müsste es dafür Kontrollen geben?

Absolut, aber daran denkt leider kaum wer. Eigentlich unverständlich, denn mit solchen Instrumenten kann man demokratische Prozesse in ganzen Staaten gezielt angreifen. Der Export von Waffen wie Panzern und Raketen ist regulatorisch streng geregelt und wird überwacht. Im Cyberbereich ist das viel komplizierter zu handhaben, da hier die Exportgüter digitaler Natur sind – sprich, sie sind physisch nicht wahrnehmbar. So können Cyberwaffen in Millisekunden praktisch ungehindert über die ganze Welt verschoben werden.

Werden Systeme mit künstlicher Intelligenz (KI) also künftig zur Bedrohung für die Demokratien?

KI wird immer bessere Botschaften versenden. Die Systeme werden bald Videos von Menschen simulieren können, bei denen wir nicht mehr bemerken, dass sie nicht echt sind. Wenn sie das dann skalieren und breitflächig zum Einsatz bringen, wird es brandgefährlich. Insbesondere, wenn das beide Seiten einer politischen Kampagne einsetzen.

Wie sähe so was konkret aus?

Ich kann mir gut vorstellen, dass wir 2035 politische Kampagnen sehen, die von künstlichen Intelligenzen gegen andere künstliche Intelligenzen geführt werden.

Für die Bürgerinnen und Bürger, die ja eigentlich wählen sollten, wird das Ganze zum unübersichtlichen Chaos und die Demokratie ad absurdum geführt.

Das klingt wie eine Dystopie.

Ja, es sind keine guten Aussichten. Aber wir müssen uns damit dringend als Gesellschaft auseinandersetzen. Ansonsten laufen wir Gefahr, in zehn Jahren zu Statisten degradiert zu werden. Ähnlich wie im Film «Matrix», wo die Menschen in einer von einer KI geschaffenen Traumwelt leben. Was ich sagen will: Wir erschaffen heute unsere Zukunft; morgen leben wir dann darin. Wir brauchen einen neuen Gesellschaftsvertrag, der unser Wirken im Cyberraum definiert und regelt. Genau so wie in der realen Welt.

Oliver Zihlmann ist Co-Leiter des Recherchedesks von Tamedia. Sein Schwerpunkt sind vertiefte Recherchen. Er ist Mitglied des International Consortium of Investigative Journalists und erhielt mit seinem Team den Zürcher Journalistenpreis. Mehr Infos