Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 99 (2024)
Heft: 2

Artikel: Risiken im Cyberspace : diese Rolle spielt Russland
Autor: Goertz, Stefan
DOI: https://doi.org/10.5169/seals-1063031

Risiken im Cyberspace: Diese Rolle spielt Russland

In einer zunehmend vernetzten Welt steht der Westen vor einer wachsenden Bedrohung durch Cyberangriffe und Desinformationskampagnen. Die Strategien reichen von hochtechnisierten Spionageaktionen bis zur gezielten Beeinflussung der öffentlichen Meinung über die sozialen Medien.

Prof. Dr. Stefan Goertz, Bundespolizei, Hochschule des Bundes, Lübeck

Cyberangriffe sind nach aktuellen Angaben des deutschen Bundesministeriums des Innern und für Heimat (BMI) mittlerweile fester Bestandteil geheimdienstlicher Methoden der Spionage. Das digitale Zeitalter eröffnet auch für Spionage durch Cyberangriffe neue Möglichkeiten und Wege und stellt damit für die Spionageabwehr neue Herausforderungen. Seit Beginn des Ukrainekrieges stellen die Sicherheitsbehörden westlicher Staaten vermehrt Cyberangriffe gegen Parlamente, Behörden und westliche Wirtschaftsunternehmen fest, mutmasslich oder bestätigt ausgehend von russischen Akteuren. Diese russischen Cyberangriffe finden auf hohem technischem Niveau statt und gefährden daher massiv die Informationssicherheit in diesen Bereichen, so das deutsche BMI aktuell. Cyberangriffe können zur Spionage, im Kontext von Cyberangriffen zum Ausspähen von Daten, zur Einflussnahme beispielsweise durch Desinformation sowie zur Sabotage, also zum Stören von Abläufen, genutzt werden. Die Nachhaltigkeit und Zielauswahl von russischen Cyberangriffen gegen westliche Staaten zeigen klar den Versuch, westliche Staaten strategisch auszuspionieren.

Angriffe auf die Schweiz

Mitte Januar 2024 wurde bekannt, dass ein Cyberangriff auf mehrere Websites der Schweizer Bundesverwaltung diese lahmlegte, die pro-russische Gruppierung «No-Name» bekannte sich zu jenem Angriff. Als Begründung nannten die pro-russischen Hacker die Teilnahme des ukrainischen Präsidenten Wolodimir Selenski am Weltwirtschaftsforum in Davos. Bereits Mitte Juni 2023 waren nach Cyberangriffen der gleichen pro-russischen Hackergruppe in Zürich, Basel-Stadt, St. Gallen und weiteren Städten zahlreiche Websites der Behörden ausgefallen, was ein Ausmass darstellte, das europaweit im oberen Bereich lag.

Insgesamt 1149 Cybercrime-Vorfälle in der Schweiz wurden dem Nationalen Zentrum für Cybersicherheit (NCSC) allein bis Anfang November 2023 gemeldet. Das stellt das Hellfeld dar, die Dunkelziffer liegt im Bereich von Cybercrime und Cyberangriffen - auch im europäischen Vergleich - meistens noch deutlich höher.

Das Schweizer Bundesamt für Cybersicherheit (BACS) erklärt aktuell, dass Cyberangriffe in der Schweiz alle treffen können, auch Behörden. Bei solchen Cyberangriffen kann beispielsweise die Website offline gehen, aber auch das gesamte Netzwerk betroffen sein. Nebst finanziellen Schäden können auch vertrauliche Informationen in falsche Hände geraten, Systeme ausfallen und haftpflichtrechtliche Ansprüche aufgrund einer Datenschutzverletzung oder Reputationsschaden entstehen, erklärt das BACS.

Gefahr für Kritische Infrastrukturen

Nach Angaben von Microsoft aus dem Januar 2024 wurde der US-Konzern kürzlich von einer russischen, staatlich gesponserten Gruppe gehackt. Die russischen Hacker hätten sich Zugang zu E-Mails von ranghohen Managern des weltweit grössten Softwareherstellers verschafft. Die Attacke habe im November 2023 begonnen und sei Mitte Januar 2024 entdeckt worden. Hinter dem aktuellen Hack steht nach Angaben von Microsoft eine russische Gruppe, die unter den Namen Midnight Blizzard und Nobelium bekannt ist. Midnight Blizzard, auch bekannt als

Bilder: Wikimedia Commons

Der russische Präsident Putin in einem Studio von Russia Today.

APT29 oder Cozy Bear, steht nach Angaben von US-Behörden in Verbindung mit dem russischen Geheimdienst SVR. Ende des Jahres 2023 hatte die britische Regierung dem russischen Geheimdienst FSB vorgeworfen, sich mit Cyberangriffen auf Politiker, Journalisten und Nichtregierungsorganisationen in die britische Politik einzumischen.

Die Gefahr von Sabotage durch Cyberangriffe gilt vor allem für Kritische Infrastrukturen (KRITIS), beispielsweise für Energieversorgungsunternehmen. Bei einem erfolgreichen Cyberangriff besteht ein umfassender und schneller Zugriff auf grosse Datenmengen. Cyberspionageangriffe sind auch deswegen so gefährlich, weil sie von den Betroffenen oftmals nicht oder erst zu einem späteren Zeitpunkt erkannt werden.

Über 850 Cyberangriffe

Eine weltweite Welle von Cyberangriffen mit Erpressungssoftware legte zu Beginn des Jahres 2023 zahlreiche Unternehmen und öffentliche Einrichtungen in Europa und Nordamerika lahm. Nach Angaben des deutschen Bundesamtes für Sicherheit in der Informationstechnik könnten Hunderte deutsche Firmen betroffen sein. Der geographische Schwerpunkt der Cyberangriffe lag auf Frankreich, den USA, Deutschland und Kanada.

Die Firma Vulkan kooperiert nach Angaben westlicher Sicherheitsbehörden mit den wichtigsten russischen Geheimdiensten FSB, GRU und SWR. In den im Frühjahr 2023 medial ausgewerteten «Vulkan Files» werden Angriffsziele benannt, beispielsweise das «Lahmlegen von Kontrollsystemen von Eisenbahn-, Luft- und Schiffstransport» und die «Störung von Funktionen von Energieunternehmen und kritischer Infrastruktur». Mehrere westliche Geheim- und Nachrichtendienste halten die «Vulkan Files» für authentisch. Der Vorsitzende des Parlamentarischen Kontrollgremiums des Deutschen Bundestages, Konstantin von Notz, geht von «Hunderten solcher Cyberwaffen» aus, die gerade entwickelt würden. Die «Vulkan Files» legen zudem nahe, dass die als «Sandworm» weltweit bekannt gewordene Spezialeinheit 74455 des russischen Militärgeheimdienstes GRU mit der IT-Firma Vulkan kooperiert hat. «Sandworm» soll unter anderem verantwortlich sein für Angriffe auf ukrainische Firmen im Juni 2017. Die Schadsoftware geriet ausser Kontrolle und befiel weltweit Tausende Computer, auch in den USA und verursachte Schäden in dreistelliger Millionenhöhe.

Im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine zählte das CyberPeace-Institut in Genf für das Jahr 2022 mehr als 850 Cyberangriffe. Diese wurden demnach von pro-russischen Hackern gegen Ziele in der Ukraine und rund drei Dutzend westlichen Ländern ausgeführt. Pro-russische Hackernetzwerke würden durch immer stärkere Vernetzung immer unberechenbarer, erklärte die Chefanalystin des Instituts, Emma Raffray Anfang 2023. Bei den Flughäfen seien Websites vorübergehend gestört worden. Allein im September 2022 wurden an zwei Tagen fünf Cyberangriffe mit 18 Zielen in Deutschland registriert.

Seit Beginn der westlichen Unterstützung für die Ukraine mit Waffenlieferungen und Sanktionen gegen Russland gelten Cyberangriffe gegen Energieversorger oder militärische Einrichtungen als grosse Bedrohung für westliche Staaten.

Die Zentrale des russischen Geheimdienstes FSB in Moskau.

Desinformationskampagnen

Die aktuellen russischen Desinformationskampagnen, die weltweit - gerichtet gegen westliche Staaten - angelegt sind, stellen kein neues Phänomen dar. Doch seit der völkerrechtswidrigen Annexion der Krim 2014 hat das System Putin die Intensität und Reichweite der Desinformationskampagnen drastisch erhöht. Dabei wird die «Informationskriegführung» als ein explizit anerkannter Bereich der russischen Militärdoktrin definiert und ist daher systematisch und finanziell gut ausgestattet. Für die Verbreitung von Desinformation wird neben herkömmlichen Kommunikationsmitteln wie staatsnahen oder staatseigenen Fernsehersendern oder Tageszeitungen auch Instant Messaging-Dienste wie Telegram, X (ehemals Twitter) und Facebook genutzt. Russische Trollfabriken sind für ihre Einflussnahme auf westliche Debatten in den Sozialen Medien bekannt.

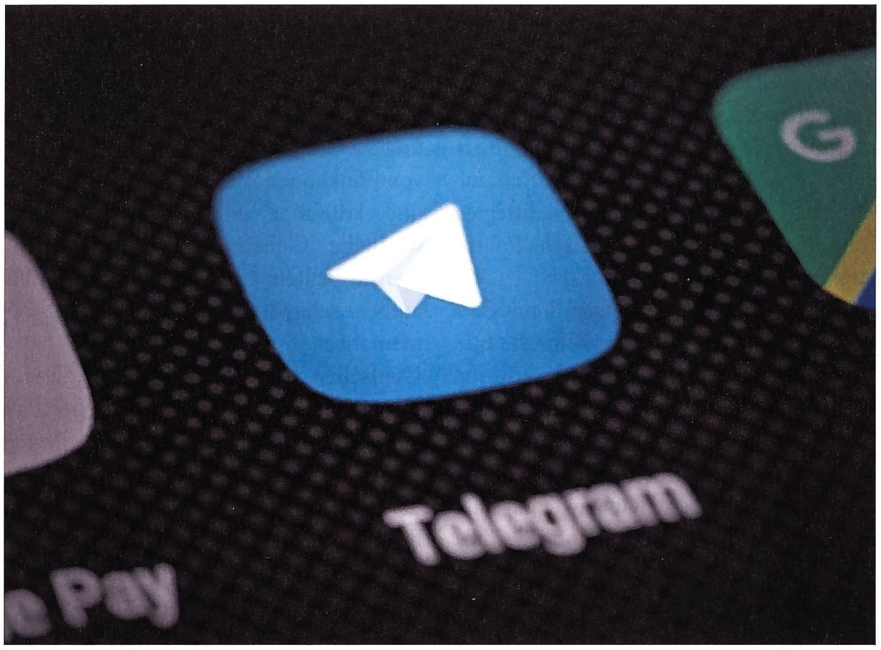
Falsche Narrative

Lutz Güllner, Leiter der Strategischen Kommunikation im Europäischen Auswärtigen Dienst (EAD), die sich um die Aufdeckung und Bekämpfung von ausländischer Desinformation beschäftigt, führt zu aktuellen russischen Desinformationskampagnen und deren Narrative aus, dass es sich um drei grosse Themenblöcke handele. Einerseits Falschinformationen zum Kriegsverlauf, beispielsweise falsche Verlust- oder Erfolgsmeldungen. Zweitens gehe es um die Frage Ursache und Wirkung. Wer ist der Aggressor? Wo kommt die Gefahr her? Hier würden Tatsachen entweder falsch oder verdreht dargestellt. Immer wieder werde die NATO oder «der Westen» als Aggressor genannt, gegen den sich Russland wehren müsse. Der dritte grosse Bereich beziehe sich schliesslich

auf die Ukraine selbst, deren Existenzrecht abgesprochen werde. Die politische Führung der Ukraine werde diskreditiert, eine gemeinsame Historie konstruiert. Russland spricht von Entnazifizierung und einer Friedensmission.

Die Instrumente russischer Desinformationskampagnen sind erstens die offiziellen Kanäle, Reden und Statements des russischen Präsidenten selbst, sowie seiner Minister und seines Kremlsprechers. Zweitens die russischen Staatsmedien, drittens die sogenannten Informationsportale, die häufig sehr eng mit russischen Behörden, auch mit den russischen Geheimdiensten verbunden sind. Und viertens gibt es einen klandestinen Bereich in den sozialen Medien, wo teilweise falsche Identitäten im Einsatz sind, deren Reichweite wiederum künstlich verstärkt werden.

Die Vizepräsidentin der Europäischen Kommission, Vera Jourova, macht sich aktuell Sorgen wegen der Wirkung russischer Desinformationskampagnen auf die Politik und die Zivilgesellschaft in der EU. Die tschechische Politikerin forderte die grossen Firmen Alphabet, Google, Microsoft, Meta Platforms und TikTok dazu auf, mehr gegen russische Desinformationskampagnen zu tun und sprach von einer «Multimillionen-Euro-Massenmanipulationswaffe» vor den anstehenden Europawahlen in Europa. Den Kurznachrichtendienst X bezeichnete sie als «Plattform mit dem grössten Anteil an Fehl- und Desinformationsbeiträgen».



Für die Verbreitung von Desinformation werden auch Instant Messaging-Dienste wie Telegram benutzt.

Fazit

Die zuständigen Behörden in Europa stellen seit Jahren – massiv verstärkt durch den Ukrainekrieg – fest und berichten transparent darüber, dass Cybercrime, Cyberangriffe und Desinformationskampagnen zu wesentlichen Bedrohungen für westliche Staaten, auch Wirtschaftsunternehmen, geworden sind. Im Kampf gegen den Westen, im neuen Ost-West-Konflikt des 21. Jahrhunderts, nutzt das System Putin Cyberangriffe sowie Desinformationskampagnen gegen westliche Staaten. Unsere europäische Demokratie benötigt starke Abwehrkräfte gegen Desinformationskampagnen, Fake News und Propaganda. Diese Abwehrkräfte müssen gestärkt und neue staatliche Akteure, Strategien und Mittel entwickelt werden.

Das Bundesamt für Cybersicherheit unterschiedet fünf Arten von Cyberangriffen

Cyberkriminalität
Cyberkriminalität umfasst Straftaten im Cyberraum, insbesondere Vermögensdelikte, wobei kriminelle Gruppen innovative Methoden entwickeln und sich professionalisieren. Oft ist das betroffene Opfer Ziel von Erpressungen

Cyberspionage
Cyberspionage, durchgeführt von staatlichen oder nichtstaatlichen Akteuren, zielt darauf ab, unerlaubt Informationen für politische, militärische oder wirtschaftliche Zwecke zu sammeln. Dabei sind Unternehmen und internationale Institutionen häufige Ziele. Die Schweiz ist aufgrund ihrer Innovationskraft besonders gefährdet.

Cybersabotage
Cybersabotage bezeichnet gezielte Angriffe, um das fehlerfreie Funktionieren von Informatik- und Kommunikationsmitteln (IKT) zu manipulieren, zu stören oder zu zerstören.

Die Motivation kann von Einzeltätern bis zu staatlichen Akteuren reichen mit dem Ziel, Organisationen oder eine Gesellschaft zu destabilisieren.

Cybersubversion
Bei Cybersubversion setzen staatliche oder politisch motivierte Akteure gezielte Cyberangriffe ein, um das politische System eines anderen Staates zu unterminieren, indem sie demokratische Prozesse, politische Institutionen und öffentliche Organisationen beeinträchtigen und mit Desinformationskampagnen kombinieren.

Cyberoperationen in bewaffneten Konflikten
Cyberoperationen in bewaffneten Konflikten sind eine weit verbreitete Praxis, da sie schwer zuzuordnen sind, vergleichsweise wenig kosten und es ermöglichen, Wirkung ohne physische Präsenz zu erzielen.

Die Bedeutung dieser Cybermittel wird voraussichtlich weiter zunehmen, was eine verstärkte Vorbereitung auf Cyberabwehr und Cyberdiplomatie erfordert.