Noch vor den Panzern sind die CYBERTRUPPEN in der Ukraine aufmarschiert. Hackergruppen, Aktivisten und Kriminelle reiten live auf offener Weltbühne Attacken, deren Konsequenzen noch nicht absehbar sind. Getroffen werden auch europäische Konzerne und Organisationen.

Antiquiert wirken die drei Festnetztelefone auf Wladimir Putins Schreibtisch. Der Kremlchef inszeniert sich nicht mit Hightech, das Internet ist ihm fremd. Dennoch befehligt Putin, der offiziell kein Smartphone nutzt, eine Cyberarmee unbekannter Stärke. Der einstige KGB-Mann ist ein Meister im Tarnen und Täuschen.

So war die Cybervorhut bereits Tage in der Ukraine, als sich die Bodentruppen noch nicht einmal stauten. Vor dem Aufmarsch attackierten sie massivst Banken und Behörden mit dem Ziel, die Gegenseite zu schwächen. Die Security-Spezialisten von Eset identifizierten eine Malware, die auf Hunderten Rechnern in fünf Organisationen Daten löschte.

Schnell eskalierte der Konflikt zu einem globalen Gefecht mit einer noch nie dagewesenen Gemengelage: Der ukrainische Digitalisierungsminister und Vizepremier Mychajlo Fedorow rekrutierte binnen kürzester Zeit eine Freiwilligenarmee von Hunderttausenden Nutzern, die mit gezielten Überlastungsangriffen (DDoS-Attacken) russische Behörden und Unternehmen angreifen. Historiker Yuval Harari spricht in seiner vielbeachteten TED-Rede von einer „neuen Form" des Krieges: „Menschen in Kalifornien oder Australien können mit in den Krieg ziehen, in dem sie Websites verteidigen oder attackieren."

Wie schnell es den Ukrainern gelang, Freiwillige zu versammeln, hat selbst erfahrene Cybersecurity-Experten wie Robert Herscovici vom österreichischen Unternehmen TCSS überrascht: „Neben dieser ‚IT Army of Ukraine' gibt es eine ganze Reihe von Telegram-Accounts, die weltweit rekrutieren. Die Ukrainer haben sogar Kampagnen in Russland gefahren, um Freiwillige zu finden. Sie haben Tausende Websites gebaut, um die Attacken zu befördern und zu monitoren."

Ob und wie weit die ukrainischen Streitkräfte diese Truppen noch kontrollieren können, ist selbst für Experten schwer auszumachen. Herscovici: „Jeder, der will, kann mithacken. Die Gefahr, dass diesem Hacktivismus, beabsichtigt oder nicht, ‚zivile' Infrastrukturen zum Opfer fallen, ist gegeben." Die Listen mit den Anzugreifenden – Unternehmen, Organisationen, Social-Media-Accounts Prominenter – werden laufend gepostet, Erfolge online gefeiert.

VON **BARBARA STEININGER**

Mitten im Aufmarsch stehen Hackergruppen. Das Kollektiv Anonymous hat sich auf die ukrainische Seite geschlagen und dem Vernehmen bereits das Satellitensteuerungssystem der russischen Raumfahrtbehörde angegriffen, was deren Chef Dmitry Rogozin bestritt, um direkt klarzustellen, dass „jeder Angriff eines Satelliten eine Kriegserklärung sei". Starts von Arianespace-Projekten vom Weltraumbahnhof Baikonur wurden storniert, ein unmittelbarer Kollateralschaden für Europa. Rhetorisch wird massivst aufgerüstet. Rogozin drohte: „Die Sanktionen könnten darin münden, dass die ISS unkontrolliert abstürzt."

Involviert sind längst auch Hackergruppen aus den Nachbarrepubliken. Die einen arbeiten für die Russen, die anderen für die Ukrainer. Herscovici: „Die allerwenigsten sind unpolitisch. Positionierung ist das Gebot der Stunde." Proukrainische Hacker griffen das Moskauer Institut für Atomenergie an, weißrussische Partisanen bremsten über eine Ramsomware-Attacke die eigene Staatsbahn aus und störten die Truppentransporte. „Dazu kommen neue Gruppen verschiedener Nationalitäten, die angekündigt haben, den Russen beizuspringen", sagt Herscovici. Der im Iran aufgewachsene israelische Cyberexperte und Securityvorstand von SentinelOne Morgan Wright beschreibt eine weitere Front. „Russland hat den Iran im Cyberbereich aufgerüstet. Die Iraner sind die Handlanger der Russen", sagt er dem Magazin „C-Tech".

KRIMINELLES TAGESGESCHÄFT. Daneben marodieren weiter „unpolitische" Ransomware-Banden durch das Netz. Eine Gruppe namens Hive erpresste zu Redaktionsschluss gerade den größten rumänischen Erdölkonzern Rompetrol. Und alles spielt sich live auf Telegram ab, jenem Messengerdienst, der zuletzt als Drehscheibe für Cybercrime und Coronaprotest genutzt wurde und jetzt die wichtigste Frontlinie darstellt – und laut Messungen von Checkpoint Security explosionsartig wächst. Betrieben von einem russischen Internetmilliardär, der in Dubai sitzt, und mit der Situation offensichtlich überfordert ist. Nicht einmal Experten können im Gefechtsnebel aus Rekrutierungsinitiativen und Desinformation die Lage beurteilen. „Cybermäßig stehen wir an einer absoluten Zeitenwende. Wir stehen erst am Anfang. Noch laufen sich alle warm", sagt Herscovici.

Der österreichische Security-Berater Ulrich Kallausch von Certitude Consulting wägt vorsichtig ab, ob er das Wort „Cyberkrieg" tatsächlich in Mund nehmen will: „Die Voraussetzungen für eine langfristige Bedrohungslage sind absolut gegeben." Kallausch warnt davor, die russischen Kapazitäten zu unterschätzen. „Auf Russland wurde gern etwas herabgeblickt, weil die US-Tech-Konzerne stark im europäischen Fokus sind. Russland ist Westeuropa im IT-Know-how ebenbürtig und kann sich eine eigene Cloud aufbauen. Russland hat viele und extrem gute Hacker, ganz nüchtern betrachtet."

Regierungsunterstützte russische Attacken laufen seit Jahren gegen private und öffentliche Einrichtungen im Westen. Kallausch: „Zu befürchten ist, dass Unternehmen, die sich aus Russland zurückziehen, verstärkt das Ziel von Angriffen sein werden." Diese Befürchtung teilen immer mehr Unternehmen in Österreich und wenden sich in diesen Tagen an Experten wie Kallausch, Herscovici und Kollegen.

Die neue Gefährdung kommt zur Unzeit. Im Zuge der Pandemie haben sich viele Organisationen tiefgreifender digitalisiert und die Sicherheit oft zu wenig mitbedacht. Unternehmen und Organisationen in Europa müssen ihre Cyberabwehr überprüfen. Sie sollten sich der Illusion, dass die Gefechte und das Chaos schnell vorbeigehen, nicht hingeben. „Russen sind geduldig, die können lange warten, bis sie Rache üben", warnt der Experte Morgan Wright: „In dem Land mit den meisten Schachspielern wird strategisch gedacht." T

HEIKLER NERV IM FINANZKREISLAUF. Vom Westen befürchtet werden russische Angriffe auf die drei Swift-Rechenzentren. Das Schweizer Zentrum steht bereits unter Polizeischutz.

IT-ARMEE UKRAINE. Allein am Hauptkanal haben sich 175.000 Nutzer registriert, die helfen wollen, die Ukraine digital zu verteidigen.

TELEGRAM. Von einem Russen gegründet, in Dubai operierend, ist der Messenger der Platz für Rekrutierung und Propaganda.

ANONYMOUS. Das Hackerkollektiv mit unbekannter Mitgliederzahl greift in Russland massiv an. Die Bandbreite reicht von Hackerscherzen (Putins Yacht) bis zu gefährlichen Angriffen auf die Satellitenstruktur.

FOTOS: ISTOCKPHOTO, LUKAS ILGNER. BEIGESTELLT (4)