Verweis auf die Startseite

JOHANNES KEPLER UNIVERSITÄT LINZ

JKU/Kepler Tribune/Cyberwar

Cyberwar

Die Anzahl der Cyberattacken steigt – auch in Österreich. Entscheiden in Zukunft nicht mehr Kampfjets, Granaten und Drohnen über das Kriegsgeschehen, sondern Viren und Würmer?

Von Markus Sulzbacher

(c) iStock

Für den Experten liegen die Vorteile auf der Hand. Die Kriegsführung und die Spionage im digitalen Raum „kostet wenig, braucht kaum Personal, die Akteure können anonym agieren und die Maßnahmen sukzessive steigern“, erklärt Oberst Walter Unger vom Cyber-Verteidigungszentrum im Abwehramt des Bundesheeres. Es sind vor allem die vergleichsweise niedrigen Kosten, die diese Art der Auseinandersetzung attraktiv machen.

„Wir sind zum Schluss gekommen, dass ein gleichzeitiger Angriff auf die gesamte kritische Infrastruktur unseres Landes – von der Strom- und Wasserversorgung über Krankenhäuser, Behörden, die Flugsicherung bis hin zum Militär – mit relativ überschaubarem finanziellem Aufwand durchaus machbar wäre“, erklärt Unger. Mit einem Budget von zehn Millionen Euro könnte man Österreich digital weitgehend lahmlegen, wobei die meisten Kosten für Programmierer und IT-Experten anfallen würden, rechnet er vor. Ein hochmoderner Panzer oder ein Kampfjet ist für dieses Geld nicht zu bekommen.

Im Verteidigungsministerium in Wien geht man davon aus, dass großflächige Angriffe nur mehr eine Frage der Zeit sind. Solche Attacken könnten etwa zu einem Black-out, einem mehrtägigen Stromausfall führen, der auch verheerende Auswirkungen bis hin zu Todesfällen mit sich bringen könnte.

Dass ein derartiges Szenario nicht weit hergeholt ist, zeigte sich 2015 in der Ukraine. Eine Woche vor Weihnachten ging in einem Teil der Hauptstadt Kiew der Strom für einige Stunden aus, nachdem ein Kraftwerk Ziel einer Cyberattacke geworden war. Den Angreifern gelang es, eine ausgefeilte Schadsoftware auf Rechner eines Energieversorgers einzuschleusen und die gesamte Steuerung des Kraftwerks zu übernehmen. Der Angriff wurde von westlichen Beobachtern Russland zugeordnet und als Machtdemonstration gewertet.

Wie verwundbar die IT-Infrastruktur auch in Österreich ist, zeigte Anfang dieses Jahres der junge Wiener IT-Experte Christian Haschek auf. Er hat ganz Österreich auf Sicherheitslücken gescannt. Konkret hat er jede der rund 11,2 Millionen IP-Adressen, die dem Land zugewiesen sind, untersucht. Das Ergebnis zeigte gravierende Sicherheitsprobleme auf. Denn neben einfachen Webseiten entdeckte er auch Industriesteuerungen, Überwachungskameras und längst veraltete Server, die mit wenigen Klicks zugänglich sind. In einigen Häusern könne jedermann das Licht ein- oder ausschalten oder Musik abspielen, da deren Smart-Home- Steuerung über das Netz zugänglich war. Aber auch die Steuerung einer Kläranlage war über das Netz erreichbar. Jeder, der auf dieser Seite landete, konnte den Betrieb gehörig stören.

Angegriffen wird, „was irgendwie erreichbar ist“, betont Bundesheer-Experte Unger – auch das Bundesheer. Es gebe wöchentlich drei bis fünf Attacken, „die man ernst nehmen muss“, sagt Unger. Weitere hunderttausende Attacken mit der Absicht, Computer zu sabotieren oder Daten zu stehlen, werden mit herkömmlichen Methoden wie Firewalls abgewehrt.

Tatsächlich toben im Netz also viele derartige Auseinandersetzungen, die als „Cyberwar“ bezeichnet werden. Was die Kriegsführung im digitalen Raum von bisherigen Formen der Auseinandersetzung zwischen Staaten unterscheidet, ist, dass hier auch zu Friedenszeiten ständig „gekämpft“ wird. Und es kommen weitere Dimensionen wie Cyberspionage, Desinformationskampagnen und Einflussoperationen hinzu. Zudem ist nicht immer klar, wer hinter einem Angriff steckt oder wer das wirkliche Ziel ist. Weiters ist bei derartigen Attacken auch die Schwelle hoch, darauf militärisch zu reagieren. Wenn der Mailserver einer Partei gehackt und die E-Mails gestohlen wurden, wird man kaum mit einem massiven Raketenangriff darauf antworten.

Derzeit sieht es so aus, als könnten Cyberangriffe eine Alternative zu einem Angriff mit traditionellen Mitteln werden. Unter Experten gelten sie als Weg zur Vergeltung, ohne den Gegner frontal anzugreifen. „Man kann Schaden verursachen, ohne Menschen zu töten oder Dinge in die Luft zu sprengen“, sagte etwa James Lewis vom Zentrum für Strategische und Internationale Studien in Washington. Besonders die USA unter Präsident Donald Trump setzen derzeit auf diese Strategie, wie die aktuelle Krise am Persischen Golf zeigt.

Nach dem Abschuss einer US-Aufklärungsdrohne durch den Iran im Juni dieses Jahres führten die Vereinigten Staaten Cyberangriffe gegen iranische Ziele durch. Trump hatte zuerst einen militärischen Vergeltungsangriff erwogen, diesen dann aber kurzfristig abgebrochen. Wie die Zeitung „Washington Post“ berichtete, wies er stattdessen das US-Cyber-Kommando an, zur Vergeltung Cyberattacken gegen den Iran zu starten.

Einer der Angriffe galt demnach iranischen Computern, mit denen Starts von Raketen und Lenkwaffen überwacht werden. Unter Berufung auf zwei ehemalige Geheimdienstvertreter hieß es, die US-Cyberangriffe hätten zudem ein Spionagenetzwerk getroffen, das Schiffe in der Seestraße von Hormus beobachtete.

Dort waren zuvor zwei Tanker aus Norwegen und Japan angegriffen worden, wofür Washington den Iran verantwortlich machte.

Im September folgte ein Drohnenangriff auf Erdölförderanlagen in Saudi-Arabien, dessen Urheberschaft nicht restlos geklärt ist. Als Reaktion griffen die USA im Oktober Rechner im Iran an, die für die Verbreitung von „Propaganda“ verantwortlich waren, wie die Nachrichtenagentur Reuters meldete.

Der Iran wird von den USA seit Jahren immer wieder digital attackiert. So führte der US-Geheimdienst NSA, im Verbund mit israelischen Verbündeten, im Jahr 2010 einen „digitalen Angriff“ durch, der das iranische Atomprogramm zeitweise völlig zum Erliegen brachte. Mit Hilfe des Computerwurms „Stuxnet“ konnte der Betrieb tausender Zentrifugen in einer Urananreicherungsanlage gestoppt werden. Die Urananreicherung steht im Mittelpunkt des seit Jahren währenden Streits zwischen Teheran und der internationalen Gemeinschaft über das iranische Atomprogramm. Zwischen den USA und dem Iran haben sich die Spannungen auch deutlich zugespitzt, nachdem US-Präsident Trump das internationale Atomabkommen mit dem Iran 2018 einseitig aufgekündigt hatte.

Der erste Einsatz von Cyberwaffen soll aber weit länger zurückliegen. Vorbereitungen des US-Militärs für einen „Krieg durch Informationstechnologie“ wurden bereits Mitte der 1990er getroffen. Im Kosovo-Krieg kam die Technik laut damaligen Medienberichten erstmals zum praktischen Einsatz: So sollen US-Hacker die Radaranlagen der Serben gestört haben, um ungehindert Bombeneinsätze auf Belgrad fliegen zu können. Der Luftkrieg galt in Militärkreisen als Erfolg: Die NATO meldete nur zwei abgeschossene Jets.

Cyberangriffe können aber auch Angriffe mit klassischen militärischen Waffen begleiten. So wurde die israelische „Operation Orchard“ im September 2007 – damals wurde eine mutmaßliche Atomanlage in Syrien aus der Luft angegriffen – nach unbestätigten Berichten von einer digitalen Manipulation des Radarsystems begleitet, sodass auf dem Bildschirm nur ein leerer und friedlicher Luftraum zu sehen war. Die Syrer wurden von dem Angriff völlig überrascht.

Digital attackiert werden allerdings nicht nur Gegner der USA. Im Jahr 2007 kam es in dem kleinen baltischen Staat Estland zu Konfrontationen zwischen ethnischen Esten und der russischen Minderheit. In der Folge verübten Unbekannte von Russland aus massive Angriffe auf estnische Webseiten von Regierungsstellen, Parteien und Banken – für das digitale Vorzeigeland Estland ein besonderer Schock.

Die Angriffe auf Websites in Estland im April 2007 waren für sich genommen vergleichsweise harmlos, hatten aber weitreichende Konsequenzen. Die Attacken führten maßgeblich dazu, dass sich die NATO verstärkt mit dem Thema Cyberwar beschäftigte und weitere Staaten für den Krieg im Netz massiv aufrüsten. Die USA, Großbritannien, die Niederlande, Israel, China, Russland, Pakistan und Indien verfügen mittlerweile über enorme Kapazitäten und gelten in Sachen elektronischer Kriegsführung als Supermächte.

Auch das österreichische Bundesheer will seine diesbezüglichen Fähigkeiten in den kommenden Jahren massiv erweitern. So sollen defensive und offensive Cyberwaffen entwickelt und beschafft und ein „Trainingszentrum für den Kampf im Cyberspace“ errichtet werden. Zusätzlich soll Gerätschaft zur „Befähigung zur effektiven Störung der Waffen- und Kommunikationssysteme des Gegners“ angeschafft werden.

Im September 2018 beschuldigten NATO- Staaten Russland, hinter zahlreichen Hackerangriffen der letzten Jahre zu stecken – etwa dem Diebstahl von E-Mails der

US-Demokraten, deren Inhalte von Trump während des Präsidentschaftswahlkampfes geschickt genutzt wurden und dessen Wahl zum 45. US-Präsidenten vielleicht erst möglich gemacht haben. Zusätzlich drohte die NATO unverhohlen mit Gegenschlägen in Richtung Russland. Dafür stellten Großbritannien, Dänemark und die Vereinigten Staaten dem Bündnis offensive Cyberwaffen zur Verfügung.

Diese Aufrüstung wird von Netzaktivisten kritisiert. Die beste Verteidigung liege darin, sichere Systeme zu schaffen, Datenschutz auf allen Ebenen ernst zu nehmen und rigoros gegen Datenmissbrauch vorzugehen, sagt Thomas Lohninger von der Netz-NGO epicenter.works.

Obendrein begeben sich die Staaten in eine Zwickmühle: Um Angriffswerkzeuge zu bekommen, müssen sie Schwachstellen und Verwundbarkeiten von Betriebssystemen oder Programmen im Geheimen horten. Diese Sicherheitslücken werden von Dritten, meist Firmen mit zweifelhaftem Ruf, gekauft. Deren Geschäftsmodell verbietet es, die Öffentlichkeit über Lecks zu informieren, und eben diese geheim gehaltenen Lücken könnten von Kriminellen oder staatlichen Hackern entdeckt und für Angriffe ausgenutzt werden, was in der Vergangenheit bereits passiert ist.

So stammt die Schadsoftware „Wanna Cry“ ursprünglich von der NSA. Die Software nutzte eine Schwachstelle im Microsoft- Betriebssystem Windows aus, die der US-Geheimdienst entdeckt und jahrelang für eigene Spionageangriffe genutzt hatte. Die Cyberwaffe mit dem Namen „EternalBlue“ geriet 2016 in die Hände einer Hackergruppe, danach schwappten Angriffswellen mit der Software durch das Netz, die weltweit Millionen Rechner trafen. Kriminelle hatten „EternalBlue“ zu einem Verschlüsselungstrojaner weiterentwickelt. Dieser soll die Anwender mit manipulierten E-Mails dazu animieren, auf einen infizierten Dateianhang zu klicken und damit eine flächendeckende Verschlüsselung aller Daten auf den Computern im Netzwerk auszulösen. Für das Passwort, mit dem die Daten wieder entschlüsselt werden können, wird Lösegeld in Form von Bitcoins verlangt. Neben Privatpersonen und Banken wurden auch Krankenhäuser Opfer dieser Erpressung.

Auch Spionagesoftware für Smartphones benötigt Sicherheitslücken, um das Gerät in Echtzeit zu überwachen. Derartige Programme können unter anderem Standortdaten, Chat-Verläufe, Fotos oder Gespräche übertragen. Dass derartige Software auch von staatlichen Behörden eingesetzt wird, sieht René Mayrhofer, Institutsvorstand für Netzwerke und Sicherheit der Johannes Kepler Universität Linz, äußerst kritisch. Die Risiken sind höher als deren Nutzen, sagt der Sicherheitsexperte. Dass Sicherheitslücken bewusst verheimlicht werden, damit sie von Strafverfolgern genutzt werden können, sieht er als fahrlässig an. Das Risiko, dass derartige Schwachstellen auch von Kriminellen gefunden und ausgenutzt werden, ist hoch. Er wirft die Frage auf, ob derartige Software, die darauf baut, mit Steuergeld gekauft werden soll. Immerhin beliefern große Anbieter derartiger Programme auch Diktaturen oder Autokraten, die damit Journalisten oder Oppositionelle überwachen.

Mayrhofer hält diese Form der polizeilichen Ermittlungen nicht für besonders zukunftsträchtig. Mobile Betriebssysteme wie Googles Android werden immer mehr mit starken Schutzmechanismen ausgestattet, die Angriffe und Manipulationen von Handys enorm erschweren sollen. Mit jedem Android-Update werden Lücken geschlossen und so die Möglichkeit zu absoluter Kontrolle über ein Smartphone verhindert.

Johannes Sametinger vom JKU-Institut für Wirtschaftsinformatik streicht heraus, dass kritische Infrastrukturen künftig so entworfen und gebaut werden müssen, dass

sie Angriffen nicht nur besser standhalten, sondern im Ernstfall auch Fallback-Strategien zur Verfügung haben. „Gut vorstellbar ist das beispielsweise anhand eines Herzschrittmachers“, erklärt Sametinger. „Kein Patient, der ein solches Gerät implantiert hat, kann ruhig schlafen, wenn er jederzeit potentiell damit rechnen muss, dass Unberechtigte die Kontrolle über das Gerät übernehmen können. Wenn also Schwachstellen solcher Geräte bekannt werden oder es sogar zu Angriffen kommen sollte, dann ist es besser, auf Komfort zu verzichten und beispielsweise durch Abdrehen von Kommunikationskanälen die Sicherheit zu erhöhen, weil dadurch Angriffe verhindert werden können.“ Auch in Flugzeugen sollte das Netz der Passagiere physisch vom Netz der Flugzeugsteuerung getrennt sein. Eine weitere Maßnahme, um Angriffspunkte in einem möglichen Cyberwar zu entschärfen, wäre es, im Ernstfall kritische Infrastrukturen wie das Stromnetz physisch vom Internet zu trennen.

NEWS 13.12.2019

Wissen

Erschienen in Ausgabe 4/2019

Zurück zur Übersicht

JOHANNES KEPLER UNIVERSITÄT
Altenberger Straße 69
4040 Linz, Österreich

T: +43 732 2468 0
F: +43 732 2468 4929
info@jku.at