die reserve

Aus der Truppe

Digitale Infanterie – Teil 2

Symbolbild: Einen größeren Cyber-Angriff, der einem anderen Staat anzurechnen ist, hat die Bundeswehr bislang nicht erlebt, dennoch ist es beruhigend, eine "Netz-Feuerwehr" zu haben. **(Foto: lizenzfrei/pexels.com)**

Von Sören Peters | 16.01.2018

Verteidigung und Angriff – das gibt es auch im Cyberraum. Die Bundeswehr spricht darüber nicht gern. Wir haben sie trotzdem gefragt – und einen Hacker ihrer geheimen „Abteilung Attacke“ getroffen.

Teil 1 hier lesen

Von Julia Egleder

Am Nachmittag läuft James Bond. Brigadegeneral Christian Leitges bedient sich des berühmtesten Filmagenten der Welt, um einen Punkt klar zu machen: Heutige Waffensysteme wie Schiffe sind vor Hackern nicht sicher. Der Filmausschnitt aus „Der Morgen stirbt nie“, 1997 veröffentlicht, zeigt die Kommandobrücke einer britischen Fregatte. Per Funk wirft die chinesische Küstenwache der Schiffsbesatzung vor, sich in chinesischen Gewässern zu befinden und fordert sie auf, einen chinesischen Hafen anzulaufen. Der Navigator des Schiffs dagegen ist sich sicher, sich in internationalen Gewässern aufzuhalten. „Können wir absolut sicher sein, was unsere Position betrifft?“ fragt der Kommandant. Der Navigator antwortet: „Ja, per Satellit exakt bestimmt.“ Doch in Wahrheit hat der Cyber-Terrorist

Gupta das GPS-Navigationssystem manipuliert. Sein Ziel ist es, die Chinesen gegen die Briten aufhetzen und zu einem Krieg anzustacheln.

Leitges lässt den Filmausschnitt unkommentiert. Doch es liegt nahe, was er mit der Vorführung bezweckt. Moderne Kriegsschiffe, sagt er, seien voller Computer. Vom Belüftungssystem über die Brandmeldeanlagen bis zu den Waffensystemen und zur Navigationsanlage – alles sei rechnerbasiert und vernetzt. Hackern gibt das ganz viel Angriffsfläche. Deshalb, sagt Leitges, sei es sehr wichtig, immer mit den neuesten Betriebssystemen zu arbeiten. Da seien Sicherheitslücken und Schwachstellen voriger Versionen behoben. Mit dem Aufspielen neuer Betriebssysteme sei die Bundeswehr bisher allerdings recht nachlässig. Das verwundert nicht: Aktualisierungen kosten Geld und Zeit. Das eine hatte die Bundeswehr lange zu wenig, das andere fehlt ihr noch heute.

Ein diffuses Gefühl der Unsicherheit

In den Pausen preisen Firmenvertreter die Vorteile ihrer IT-Lösungen an. Einer meint, was die Bundeswehr bisher im Cyberraum könne, sei lachhaft. Die Chinesen aber, weiß er, die hätten bereits ganze Cyberarmeen. Der Chef einer IT-Firma erklärt die Waffensysteme der Bundeswehr für unsicher. Das Problem, sagt er, beginne schon bei der Produktion. Hersteller könnten gar nicht überprüfen, ob sich alle Zulieferer an die Sicherheitsstandards bei der Produktion ihrer Kleinteile hielten. Für illoyale Mitarbeiter sei es leicht, Schadsoftware einzubauen, die dann wie ein feindlicher Spion im Waffensystem schlummere. Am Ende der Konferenz bleibt ein diffuses Unsicherheitsgefühl. Doch wie „heiß“ der Krieg im Netz tatsächlich ist und ob die Bundeswehr ihn schon führt, das war auf der Tagung in Koblenz nicht zu erfahren.

Vielleicht kann Oberstleutnant Marco Krempel mehr sagen. Während der Bundeswehrhacker der „Computer Netzwerk Operationen“ für den Angriff verantwortlich ist, ist Krempel für die Verteidigung der Bundeswehrrechner zuständig. Er führt eine Einheit mit dem sperrigen Namen „Cyber Security Operations Centre“ und ist damit für den Schutz von rund 200.000 Computern der Bundeswehr zuständig. Krempel ist praktisch der oberste Viren- und Trojanerjäger der Bundeswehr. Es sind seine Leute, die sich von Euskirchen aus aufmachen, wenn an einem Standort irgendwo im Land ein System ausfällt und der Administrator nicht mehr weiter weiß. Krempels derzeit rund 40 Mitarbeiter sind eine Art Quick Reaction Force für Computernetzwerke.

Rund 40 bis 60 Schadprogramme bearbeite sein Team mit anderen Bundeswehreinheiten pro Woche, sagt er. Meist versuchten sie es zunächst mit einer Ferndiagnose: Ist das System vielleicht nur überlastet? Oder handelt es sich um einen Sicherheitsvorfall oder gar einen Angriff? Ist letzteres der Fall, fahren sie los. „Wie die Feuerwehr“, sagt er. Vor Ort versuchen Krempels Leute dann in detektivischer Kleinarbeit herauszufinden, was in den Rechnern passiert ist. Sie fischen Schnipsel aus dem Arbeitsspeicher oder werten Daten aus Sensoren aus.

Mit Angriffen konfrontiert, die auch private Computernutzer kennen

Ein wirklich spektakulärer Fall sei ihnen noch nicht untergekommen, sagt Krempel. Sie würden überwiegend mit Angriffen konfrontiert, die auch private Computernutzer kennen, etwa Schadsoftware, die sich durch das Öffnen von E-Mail-Anhängen auf dem Computer ausbreite. Wer die Angreifer sind, sei in den allermeisten Fällen unklar, vermutlich stünden hinter den meisten Attacken Kriminelle. Einen gut geplanten, konzertierten Angriff, der klar einem anderen Staat zuzurechnen sei, habe er noch nie erlebt. Grundsätzlich seien seine Mitarbeiter gut ausgebildet und die meisten Bundeswehrangehörigen für Cybergefahren sensibilisiert. Also kein Grund zur Panik? Krempel lächelt. Er wolle nicht übermütig klingen, erklärt er, könne aber selbstbewusst sagen, dass der Schutz der Bundeswehrrechner auf dem neuesten Stand sei. Aber, klar, absolute Sicherheit gebe es nicht.

Noch ein Allgemeinplatz, aber mit Blick auf die Waffensysteme der Bundeswehr klingt er beunruhigend. In einem Eurofighter beispielsweise sind zahlreiche Computer verbaut. Der Kampfjet ist ein fliegender Rechner. Kann er abstürzen, wenn er gehackt wird? „Nein“, sagt Michael Gerhards, der Leiter der deutschen Cybersecurity-Abteilung bei Airbus. Airbus ist eines der Unternehmen, die den Eurofighter entwickelt haben und noch immer bauen. Gerhards versichert, sensible Kommunikation zwischen den verschiedenen Rechnern des Eurofighters und seiner Umwelt werde verschlüsselt. Ein Zugriff aus dem Internet sei unmöglich, weil der Eurofighter ein in sich abgeschlossenes System sei. Und sollten doch einmal wichtige Computer ausfallen, würde er trotzdem nicht gleich vom Himmel fallen. Dann übernähmen andere Komponenten das Fliegen. „Redundanzen“, nennt Gerhards das.

Wer die Eurofighter-Netze angreifen will, muss also von Innen kommen. Ein Virus, ein Trojaner oder ein Computerwurm wie einst Stuxnet, mit dem vor sieben Jahren die Leittechnik iranischer Atomanlagen manipuliert wurde – das ist die größte Cyber-Gefahr für den Eurofighter. Dieser „Innentäter“ kann nur aus der Truppe kommen – oder beim Hersteller arbeiten. Das aber, sagt Gerhards, sei so gut wie ausgeschlossen. Jeder Airbus-Mitarbeiter an sensiblen Stellen des Produktionsprozesses sei sicherheitsüberprüft, und zwar nach strengen Maßgaben. Bewerber müssten zum Beispiel mehrere Bürgen angeben. Auch von Zulieferfirmen, die sensible Bauteile fertigen, verlange Airbus eine penible Sicherheitsüberprüfung der Mitarbeiter und der Produktion, berichtet Gerhards.

„Bei der Beschaffung hieß es in der Vergangenheit doch stets: Billig vor sicher“

Sind die Waffensysteme der Bundeswehr also vor feindlichen Netzattacken sicher? Thomas Reinhold, Experte für Cyberwar und IT-Sicherheit beim Hamburger Institut für Friedensforschung und Sicherheitspolitik, bezweifelt das. „Bei der Beschaffung hieß es in der Vergangenheit doch stets: Billig vor sicher“, sagt er. IT-Sicherheit habe in der Bundeswehr keine Priorität gehabt. Das allerdings hat sich inzwischen geändert. Die Aufstellung des Kommando CIR hat dazu geführt, dass bei neuen Rüstungsprojekten nun von Anfang an Cyber-Experten verstärkt auch die IT-Sicherheit der neuen Systeme im Blick haben.

Damit all die neuen Aufgaben im Cyberraum auch bewältigt werden können, sucht die Bundeswehr jetzt erst einmal Personal. Vor allem IT-Feldwebel werden gebraucht. An der Bundeswehruniversität in München entsteht ein Forschungsbereich „Cybersicherheit“ mit 13 neuen Professuren. Zulagen für besonders qualifiziertes Personal werden diskutiert, genauso wie von der Bundeswehr organisierte LAN-Partys. Auch Ludwig Leinhos ist solchen Plänen gegenüber aufgeschlossen. Er geht sogar noch weiter: „Wir müssen unsere Laufbahnen überdenken“, sagt er. Neben dem truppendienstlichen Weg soll es für IT-Experten auch einen fachlichen Weg geben, um in der Bundeswehr Karriere zu machen.

Die Cyberhacker der „Einheit Computer Netzwerk Operationen“ jedenfalls können sich über Bewerbermangel nicht beklagen, sagt deren Mitglied im Interview. Viele junge Leute wollten Hacken und gleichzeitig etwas für ihr Land tun. Wo außer bei uns könne man das tun?, fragt der Cyberkrieger. Es ist eine rhetorische Frage.

Mehr aus der .loyal erfahren? Hier Mitglied werden und das Magazin elf Mal im Jahr frei Haus geliefert bekommen.