ERLEBEN, WAS VERBINDET.

DEUTSCHE TELEKOM AG
DR. THOMAS KREMER
Mitglied des Vorstands

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
18(12)636

19.02.2016 - 18/2695

5410

Stellungnahme

für die Öffentliche Anhörung des Verteidigungsausschusses des Deutschen Bundestages am 22. Februar 2016

"Die Rolle der Bundeswehr im Cyberraum - Verfassungs-, Völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr"

Zunehmende Digitalisierung und die Folgen

Es gibt heutzutage keinen internationalen Konflikt mehr, der nicht auch virtuell, das heißt im Cyberraum ausgetragen wird: Von Propaganda und gezielter Desinformation bis hin zu Cyberangriffen auf Infrastrukturen, die die Lebensadern jeder Gesellschaft sind. Beispiele sind die Angriffe auf das Elektrizitätsnetz der Ukraine im Dezember oder die jüngsten Veröffentlichungen zum Angriff auf die iranischen Infrastrukturen. Wir stecken mitten in der Digitalisierung unserer Gesellschaft: Menschen, Maschinen und Geräte werden miteinander vernetzt und es entsteht eine Vielfalt an neuen Diensten und Nutzungsmöglichkeiten. Die Digitalisierung berührt alle Bereiche unseres Lebens: Arbeit, Freizeit, Bildung, Gesundheit, Sport, Glauben, Ethik. Nur ein Beispiel: Welches Wertegerüst gilt für selbstlernende Roboter, wer definiert es, wie sicher ist es? Solche Fragen sind heute keine Science Fiction mehr. Es ist letztendlich nur eine Frage der Zeit, bis ein ernsthafter Schaden durch Cyberangriffe auftritt, der auch eine konkrete Gefährdung für Leib und Leben bedeutet.

DEUTSCHE TELEKOM AG
Hausanschrift: Group Headquarters, Friedrich-Ebert-Allee 140, 53113 Bonn
Postanschrift: 53262 Bonn
Telefon: 0228 181-20101 | E-Mail: kremer@telekom.de | Internet: www.telekom.com
Konto: Postbank Saarbrücken, BLZ 590 100 66, Kto.-Nr. 166 095 662 | IBAN: DE0959010066 0166095662 | SWIFT-BIC: PBNKDEFF590
Aufsichtsrat: Prof. Dr. Ulrich Lehner (Vorsitzender) | Vorstand: Timotheus Höttges (Vorsitzender), Reinhard Clemens, Niek Jan van Damme, Thomas Dannenfeldt, Dr. Christian P. Illek, Dr. Thomas Kremer, Claudia Nemat
Handelsregister: Amtsgericht Bonn HRB 6794, Sitz der Gesellschaft Bonn | USt-IdNr. DE 123475223 | WEEE-Reg.-Nr. DE 50478376

Auswirkungen auf die Bundeswehr

Die Bundeswehr ist integraler Bestandteil unserer Gesellschaft. Auch sie ist von der fortschreitenden Digitalisierung unmittelbar betroffen. Im globalen Cyberraum verschwimmen nationalstaatliche Grenzen, Zeitzonen verlieren an Bedeutung und die Differenzierung von Freund und Feind wird zunehmend schwieriger, teilweise gar unmöglich.

Die Bundeswehr, die bisher hauptsächlich auf die Verteidigung der Landesgrenzen und damit die Sicherung der territorialen Integrität unseres Landes fokussiert war, muss sich auf die neue Bedrohungslage einstellen. Eine allein an nationalstaatlichen Grenzen orientierte „border control" – ohne digitale Landesverteidigung - reicht heute nicht mehr aus. Zugleich kann die Bundeswehr selbst Ziel von Cyberangriffen sein.

Gefahrenlage im Cyberraum

Die digitalen Bedrohungen umfassen gezielte Attacken auf staatliche Institutionen oder kritische nationale Infrastrukturen bis hin zu flächendeckenden Angriffen auf die infrastrukturellen Lebensadern ganzer Kontinente. Beispiele sind neben dem Cyberangriff auf den Deutschen Bundestag auch Angriffe auf Medien wie den französischen Fernsehsender TV5 und auf Infrastrukturen wie das ukrainische Stromnetz.

Die Deutsche Telekom identifiziert frühzeitig neue Angriffe auf ihre Infrastruktur und die dabei verwendeten Methoden. Unsere Sensoren im Netz – so genannte Honeypots - registrieren derzeit rund 4 Mio. automatisierte Angriffe auf die Deutsche Telekom pro Tag. Und wir stellen auch fest, dass individuelle Cyberattacken immer professioneller werden: Wir haben Fälle gesehen, in denen Angreifer in nur 6 Minuten die volle Kontrolle über ein System erhalten haben. Auch die Bürger erleben diese Gefahren immer konkreter: Laut einer aktuellen Umfrage von TNS Emnid im Auftrag der Deutschen Telekom ist fast jeder zweite Deutsche bereits Opfer von Cyberkriminalität geworden.

Weitere Fakten sind:

- Der geschätzte weltweite Schaden durch Cyberkriminalität betrug in 2014 laut den Experten von McAfee (Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies June 2014) bis zu 575 Mrd. USD.
- 51 Mrd. Euro beträgt nach aktuellen Schätzungen der jährliche Schaden für die deutsche Wirtschaft (Repräsentative Umfrage unter Unternehmen ab 10 Mitarbeitern im Auftrag des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. Bitkom, April 2015).
- Die durchschnittlichen Kosten pro Schadensfall betrugen für Großunternehmen 360.000 Euro, für kleine und mittelständische Unternehmen 41.000 Euro (Bitkom).
- 51% aller Unternehmen sind Opfer von digitaler Wirtschaftsspionage (Bitkom).
- 92% aller deutschen Unternehmen waren schon Opfer von Cyberangriffen, davon 61% aus dem Mittelstand (Bitkom).
- Die Zahl der Angriffe auf Industriesteuerungssysteme oder Smart Home Devices steigt stark an. Sogar Fernseher oder Haushaltsgeräte im privaten Umfeld werden zu neuen Zielen. Das wird durch aktuelle Medienberichte über Vorfälle in den USA deutlich, wo vernetzte TV-Geräte und sogar ein Kühlschrank für globale Cyberangriffe und den Versand von infizierten SPAM-Mails genutzt wurden.

Zum Vorgehen der Angreifer

Cybercrime ist ein florierendes illegales Geschäft mit hohen Margen und einem niedrigen Strafverfolgungsrisiko. Die Täter haben die Fähigkeit, hohe Summen in Cyber-Werkzeuge und Vorgehensweisen zu investieren. Oftmals ist das aber gar nicht nötig. Viele Unternehmen des Mittelstands machen es den Tätern zudem leicht: IT-Sicherheit wird bei den Investitionen oft vernachlässigt. Die besondere Schwierigkeit im Cyberraum ist darüber hinaus, dass weder Angriffsziel noch Angriffsart valide Schlussfolgerungen auf den tatsächlichen Angreifer zulassen. Als Angreifer können wir nur bestimmte IP-Adressen

identifizieren, ohne zu wissen, ob der Angriff tatsächlich von diesem System erfolgt oder ob es sich nur um ein Werkzeug handelt, das selbst von einem Command-and-Control-Server gesteuert wird. Diese Techniken sind dabei selbstverständlich nicht nur Kriminellen vorbehalten, sondern werden auch zum Beispiel von Geheimdiensten verwendet.

Für Cyberangriffe werden entweder spezifische Programme verwendet oder bestehende Sicherheitslücken in IT Systemen, insbesondere Software, ausgenutzt, mit der ein Angreifer zunächst einmal unbemerkt in die Systeme seines Zielobjektes eindringt. Dort kann er an sensible Informationen gelangen oder komplette Systeme so kompromittieren, dass sie nicht mehr funktionieren. Hinzu kommt: Das Tarnen, Täuschen und oft auch spurlose Verschwinden ist in der globalisierten digitalen Welt um ein Vielfaches einfacher als in der analogen.

Wiederverwendbare Cyberwaffen

Häufig wird die für Angriffe verwendete Software leicht verändert und von unterschiedlichen Tätergruppen gegen neue Ziele eingesetzt. Es gibt inzwischen sogar digitale Marktplätze im Netz, auf denen je nach Bedarf die gewünschten Schadsoftwaremodule gekauft und dann gegen ein gewünschtes Ziel in Stellung gebracht werden können. Primär wird das nach unserer Kenntnis von der organisierten Kriminalität bei Angriffen auf Unternehmen genutzt. Aber auch militärische Cyberwaffen werden von klassischen Tätergruppen wiederverwendet. Ein Beispiel dafür ist die Schadsoftware STUXNET. Mutmaßlich für Angriffe auf das iranische Atomprogramm entwickelt, wurde sie nach der Entdeckung durch Cyberkriminelle abgeändert und für deren Zwecke eingesetzt. Das macht deutlich, dass selbst hochentwickelte Cyberwaffen, die ursprünglich für militärische Zwecke entwickelt worden sind, einmal angewandt, kaum mehr zu kontrollieren sind.

Herausforderungen für die Bundeswehr

Anders als bei der konventionellen Kriegsführung stehen im Cyberraum bisher vor allem zivile Ziele im Fokus. Daher müssen sich Betreiber von kritischer Infrastruktur besonders

gegen virtuelle Angriffe schützen. Hierzu bedarf es einschlägiger Expertise und eines detaillierten Verständnisses, wie und mit welchen Methoden Cyberangriffe ausgeführt werden. Nur wer die Strategien und Methoden des digitalen Angreifers kennt, kann sich wirksam verteidigen. Die Bundeswehr steht dabei vor ähnlichen Herausforderungen wie die Wirtschaft.

Im Ergebnis kommt es für die Bundeswehr wie für zivile Unternehmen darauf an, die Angriffsflächen im Cyberraum zu minimieren, die eigenen Systeme zu härten und auf die Abwehr zukünftiger Angriffe zu fokussieren. Es werden neue Security-Kompetenzen bei Soldaten und Mitarbeitern ziviler Unternehmen benötigt, um aktuellen Gefahrenlagen besser begegnen zu können.

Zunächst einmal sind dafür die allgemein bekannten Sicherheitsmaßnahmen wie Schutz gegen Computerviren, Firewall Systeme aber auch regelmäßige Softwareupdates und Sicherheitstests einzusetzen. Um laufende Angriffe unterbinden zu können, ist aber mehr

erforderlich. Hier bedarf es insbesondere analytischer Fähigkeiten, um die Ursache und Wirkung eines individuellen Angriffs zu erkennen, um dann maßgeschneiderte Gegenmaßnahmen einleiten zu können. Da kaum ein Cyberangriff dem Anderen gleicht, ist in diesem Feld neben der Technologie der menschliche Faktor entscheidend. Für die erfolgreiche Abwehr von Cyberangriffen sind vertiefte Detailkenntnisse von Angriffstechniken und Werkzeugen zwingend erforderlich. Ob diese Fähigkeiten dann ausschließlich für die Abwehr oder auch für aktive Angriffe genutzt werden, ist keine technische Frage und keine Frage der Ausbildung. Unabhängig von diesen Kompetenzen sind außerdem sichere IT-Komponenten erforderlich, deren Hersteller fast ausschließlich nur noch im außereuropäischen Ausland zu finden sind. Deshalb ist es so wichtig, dass beim Thema Cybersicherheit die gesamte Wertschöpfungskette betrachtet wird: Von den Herstellern der Hard- und Software über die Betreiber der Infrastruktur bis zu den Diensteanbietern. Für alle müssen hohe Standards bei IT-Sicherheit und Datenschutz gelten – und das international.

Zur konkreten Beurteilung des Sicherheitsniveaus einer Komponente bedarf es ebenfalls tiefer Detailkenntnisse über Angriffstechniken und Werkzeuge. Sogenannte Penetrations- oder Sicherheitstests sind letztendlich nichts anderes als im Labor simulierte Cyberangriffe.

IT-Experten ausbilden

Für mehr IT-Sicherheit braucht es allerdings Fachkräfte, die heute am Markt kaum verfügbar sind. Die Rekrutierung von Experten aus anderen Ländern ist vielfach mit Risiken verbunden. In vielen Fällen haben sie in ihrem Herkunftsland für staatliche Institutionen oder Behörden gearbeitet. Der Fachkräftemangel an Cybersecurity-Experten wird für Unternehmen zunehmend zum Problem. Allein die Deutsche Telekom sucht bis 2018 über 300 qualifizierte Experten für unsere Business Unit Telekom Security. Um den eigenen Bedarf auch in Zukunft decken zu können, wurde begonnen, Cybersecurity-Spezialisten im Rahmen einer Kooperation mit der Industrie- und Handelskammer Köln selbst auszubilden. An der unternehmenseigenen Hochschule für Telekommunikation in Leipzig (HfTL) wurde darüber hinaus ein Lehrstuhl für Datensicherheit eingerichtet und besetzt. Auch die Bundeswehr könnte ihre renommierten Hochschulen, z.B. mit der Schaffung eines Cybersecurity Clusters, dafür einsetzen – vielleicht auch in Kooperation mit Unternehmen.. Insgesamt kann über die kommenden Jahre von einem vier- bis fünfstelligen Zusatzbedarf an derartigen Fachkräften ausgegangen werden. Parallel dazu sollte die

Forschungsförderung im Bereich der Cybersicherheit intensiviert und entsprechende Budgets bereitgestellt werden. Dabei ist es wichtig, mehr auf anwendungsorientierte Forschung zu setzen, deren Ergebnisse unmittelbar in den Schutz der kritischen Infrastrukturen einfließen können.

Digitale Verantwortung wahrnehmen

Es gibt keine Sicherheit, wenn wir die zunehmenden virtuellen Bedrohungen ignorieren. Dazu gehört, dass Sicherheit immer auch digital gedacht werden muss. Wir müssen uns alle der digitalen Verantwortung stellen. Dafür benötigen wir:

- Erstens: EU-weite und nationale Regeln, die für einen hohen Standard bei Datenschutz- und IT-Sicherheit sorgen. Hier hat die Bundesregierung mit dem IT-Sicherheitsgesetz einen Schritt in die richtige Richtung getan. Aber: Es muss die gesamte digitale Wertschöpfungskette berücksichtigt werden; nicht nur Netzbetreiber, sondern auch die Hersteller von Hard- und Software sowie sogenannte Over-the-top-Player müssen hier einbezogen werden. Es ist nicht konsequent, dass die beiden Letzteren bisher nicht verpflichtet sind, mehr Verantwortung für IT-Sicherheit in Europa zu übernehmen. Und das zeigt auch, dass wir global betrachtet leider immer noch weit davon entfernt sind, dass Sicherheit ein selbstverständliches Designkriterium für Telekommunikations- und IT- Produkte ist.
- Zweitens: Hohe Sicherheit der IT-Systeme von Staat und Wirtschaft. Keine Abhängigkeit von einzelnen Zulieferern und unabhängige Testcenter für Komponenten, die in kritischen Infrastrukturen eingesetzt werden.
- Drittens: Gut vernetzte schnelle Eingreiftruppen in Unternehmen und bei staatlichen Institutionen, die sich als Partner gegenseitig über neue Gefahren informieren. Wir brauchen mehr Transparenz über Cyberangriffe. Eine enge Zusammenarbeit von Unternehmen und Behörden untereinander und übergreifend, wie sie zum Beispiel zwischen dem Bundesamt für Sicherheit in der Informationstechnik und der Deutsche Telekom AG praktiziert wird, ist erforderlich. Durch einen intensiven Austausch kann sichergestellt werden, dass Sicherheitsvorkehrungen schneller getroffen werden – und so wird etwa verhindert, dass ein bestimmtes Angriffsmuster mehrfach erfolgreich ist. In diesem Zusammenhang sind auch klare Zuständigkeiten auf staatlicher Seite erforderlich, denn Cyber-Angriffe lassen sich nicht nach bestimmten Kriterien (kriminell/kriegerisch, Staat/Wirtschaft) trennen.

- Viertens: Einfache Lösungen für einen wirksamen Schutz von Informationen. Dazu gehören insbesondere die wirksame Ende-zu-Ende-Verschlüsselung sowie datenschutzfreundliche und sichere Lösungen für neue digitale Geschäftsmodelle.

Sicher ist: Cybersicherheit gibt es nicht zum Nulltarif. Verbraucher, Unternehmen und Staaten werden sich darauf einstellen müssen, für die virtuelle Sicherheit in Zukunft deutlich mehr Geld ausgeben zu müssen. Auch das bedeutet digitale Verantwortung.