Strategische Studien und Analysen der Internationalen Politik und Globalisierung – zusammengefasst für Entscheidungsträger in Deutschland

November 2011

Schwerpunkt
Digitale Sicherheit

Liebe Leser,

seit geraumer Zeit steigt die Zahl der Angriffe im Cyberraum. Während die Attacken anfangs mehrheitlich klein und eher harmlos waren, verursachten sie zuletzt große wirtschaftliche Schäden. Mit dem Auftauchen von Stuxnet 2010 und dem auf gleichem Code basierenden Duqu 2011 erreichte der globale Einsatz von Schadsoftware seinen aktuellen Höhepunkt. Es ist vor allem Spionagesoftware, die Unternehmens- und Regierungsnetzwerke bedroht, da die entwendeten Daten oft aus sicherheitsrelevanten Bereichen stammen.

Die Angriffe unterscheiden sich in Art, Umfang, Ziel und Erfolg. Eines ist Ihnen jedoch gemeinsam: Sie haben hohes Schadenspotential und stellen besonders für kleine und mittlere Unternehmen eine große Bedrohung dar. Doch bisher müssen Bürger und Unternehmen sich selbst schützen. Sollte der Staat ihnen dabei regulierend helfen? Ist dies möglich, ohne die Freiheit im Internet zu beschneiden? Auch die deutsche Politik wird darauf Antworten finden müssen.

Welche Methoden gibt es, kriminelle Angriffe im Cyberspace zu unterbinden? Bisher setzt die Politik auf den Aufbau nationaler Abwehrzentren und die Entwicklung nationaler Cyberstrategien. Die USA gehen sogar so weit, digitale Angriffe mit physischen Angriffen gleichzustellen – und darauf mit physischen Vergeltungsmaßnahmen zu antworten. Das Internet ist eine globale Struktur; der einzige Lösungsansatz ist eine Kooperation aller Staaten, Unternehmen und Bürger. Eine gesamtgesellschaftliche Bewegung muss eine sicherere Nutzung des Cyberraums gewähren. Alternativen wie die Verringerung von Komplexität mögen zu mehr Sicherheit beitragen, weit genug gehen sie jedoch nicht. Eine Abtrennung vom Internet hingegen würde alle positiven Effekte der Nutzung von Informations- und Telekommunikationstechnologie aufheben.

Wirtschaft und Bürger müssen sich verstärkt einbringen, um ein Höchstmaß an digitaler Sicherheit zu gewährleisten. Hier setzte die fünfte transatlantische Konferenz zum Thema “Transatlantic Cooperation for Growth and Security – Protecting Critical Technology and Infrastructure“ an. Auf Einladung der Dräger-Stiftung, des DIN Deutsches Instituts für Normung e.V., dem German-American Business Council und der Sigram Schindler Stiftung diskutierten Persönlichkeiten aus Wissenschaft, Wirtschaft und Politik über Lösungsvorschläge für den Schutz von Unternehmen und Infrastruktur.

Viel Spaß beim Lesen wünschen Ihre

Dr. Johannes Bohnen & Jan-Friedrich Kallmorgen

Atlantische Initiative e. V.

Wilhelmstraße 67
10117 Berlin
Germany

Tel: +49.30.206 337 88
Fax: +49.30.246 303 633

www.atlantische-initiative.org
info@atlantische-initiative.org

Bankverbindung

Atlantische Initiative e. V.
Bankhaus Löbbecke AG
Bankleitzahl: 100 30 500
Kontonummer: 12 57 95 00

Registergericht

Amtsgericht Berlin Charlottenburg
Registernummer: VR 23583Nz

Steuernummer: 27/660/59701
USt-IdNr.: DE 252416799

Schwerpunkt: Digitale Sicherheit

Diese Ausgabe erscheint mit freundlicher Unterstützung der

Dräger-Stiftung

Die *Global Must Reads* werden von der Atlantischen Initiative e.V. herausgegeben.

ATLANTISCHE INITIATIVE

Vorstand: Dr. Johannes Bohnen und Jan-Friedrich Kallmorgen (V.i.S.d.P.)

Verantwortliche Redakteure: Falko Westenberger, Nina Keim

Tel: +49 - 30 - 206 337 88 – Fax: +49 - 30 - 246 303 633
Email: info@atlantische-initiative.org

Neuartige Bedrohungsszenarien durch Cyberspionage

Paneldiskussion: Transatlantic Cooperation for Growth and Security – Protecting Critical Technology and Infrastructure, 5th Transatlantic Market Conference, Oktober 2011

Die Probleme mangelnder Sicherheit von Informationstechnik in der Wirtschaft aufgrund von Cyberkriminalität sind extrem komplex. Es gibt noch viele unbekannte Bereiche und keine einfachen Lösungen. Daher ist es umso wichtiger, diese Fragen in einem transatlantischen Kontext zu diskutieren. Eine klare Trennung zwischen zufälligen Störungen und vorsätzlichen Cyberangriffen ist nötig.

Die Gefahr durch digitale Angriffe hat sich in den vergangenen Jahren drastisch erhöht. Digitale Industriespionage verursacht große Schäden. Angriffe auf Industrienetzwerke sind einfach durchzuführen und werden bereits getätigt, wie die Angriffe durch Stuxnet 2010 und Duqu 2011 zeigten. Die Auswirkung auf kritische Infrastruktur – vitale Systeme wie Energie, Wasser, Kommunikation und Verkehr – können verheerend sein.

Es besteht die Gefahr, dass organisierte Gruppen und staatliche Industriespionage zunehmend zur Bedrohung von Unternehmen werden. Dies kann zu einem kalten Wirtschaftskrieg führen. Dadurch ist die Sicherheit im Cyberraum etwas komplett Neues und nicht mit alten Sicherheitsdilemmata zu vergleichen. Dies liegt auch daran, dass die Angreifer den Abwehrmaßnahmen stets einen Schritt voraus sind. Auch fehlt es an Evaluationstools, um Angriffe und ihre finanziellen Auswirkungen erfassen zu können. Eine realistische Schätzung der wirtschaftlichen Schäden in Deutschland durch das Bundeskriminalamt kommt auf 61,5 Milliarden Euro. Weltweit sind es laut Europol bis zu 750 Milliarden Euro.

Der einfache Zugang zu Schadsoftware, die geringe Entdeckungsgefahr und die enormen Gewinne machen Cyberkriminalität zu einer boomenden Industrie. Heute ist jede Art von Schadsoftware über digitale Schwarzmärkte zu beziehen. Und selbst in staatlicher Software sind Fehler enthalten, welche die Nutzung der Software durch Dritte ermöglichen. Dies zeigt die aktuelle Debatte über den Bundestrojaner.

Eine absolute Sicherheit lässt die Struktur von digitalen Netzwerken nicht zu, die Angreifer sind stets einen Schritt voraus. Die Offenheit der Netze verhindert Kontrolle und Rückverfolgung sowohl der Nutzer als auch des Datenflusses: Während die Angreifer nur eine einzelne Zugangsmöglichkeit benötigen, müssen die Verteidiger unzählige Zugänge sichern. Um Fehler in Software und Hardware zu minimieren, muss daher auf Komplexität verzichtet werden.

Fraglich ist folglich, ob zukünftige Technologien zum Schutz vor Cyberangriffen beitragen können. Technische Innovationen sind in der Lage, den Zugang Fremder zu den eigenen Systemen zu erschweren. Daher besteht ein Ausweg darin, Softwareunternehmen durch Normen zu zwingen, sichere und fehlerfreie Software zu entwickeln.

Des Weiteren ist es von großer Bedeutung, dass die Unternehmensführung eng mit den technischen Mitarbeitern zusammenarbeitet, um Zugriff auf unternehmensrelevante Daten zu verhindern und unbefugte Aktivitäten zu entdecken. Bisher wird der Cybersicherheit gerade in der Unternehmensspitze zu wenig Bedeutung beigemessen – die Schulung des Managements kann hier Abhilfe schaffen.

Weiterer Schutz lässt sich durch bessere Leistung und Nutzbarkeit von Software, Investitionen in IT-Sicherheit, Homogenisierung oder Abtrennung von Netzen sowie einem besseren Risikomanagement erreichen. Da diese Maßnahmen jedoch hohe Kosten produzieren, muss die Versicherungsindustrie für innovative Lösungen einbezogen werden.

Im Zeitalter der Informationsfreiheit muss die Gesellschaft in der Lage sein, ihre Bürgerrechte zu schützen. Die Bundestrojaner zeigen, dass diese Rechte schon jetzt in Gefahr sind.

Gruppenimmunität gegen Cyberbedrohungen

Jeffrey Moss, Konferenzbeitrag: From the Hacker's Insider Knowledge: How to Secure Networks from Cyber Attacks?, 5th Transtlantic Market Conference, Oktober 2011

Die Menschheit im Informationszeitalter kämpft mit dem Überfluss an Informationen. Die zunehmende Komplexität der Systeme bildet hierbei eine

zentrale Herausforderung, die durch fortschreitende Spezialisierung überwunden werden kann. Höhere Spezialisierung bedeutet mehr Gewinn, aber auch höheres Risiko. Durch Diversität hingegen herrscht weniger Risiko, es ist jedoch auch nur geringerer Gewinn möglich.

Die ursprünglich zu kontaminierenden Krankheiten aufgestellte Gruppenimmunitäts-Theorie besagt, dass eine immune Mehrheit die anfällige Minderheit schützen kann. Angewandt im Kontext der Cybersicherheit, bildet diese Theorie einen Lösungsansatz, um Cyberbedrohungen zu entgegnen und die Immunität externer Subjekte – welche nicht Teil der geschützten Gruppe sind – zu erklären. Hierfür lässt sich das Internet in die drei Gruppen Wirtschaft, Staat und Zivilgesellschaft kategorisieren.

Die Wirtschaft geht einen eigenen Weg zum Schutz ihrer IT: Die Entwicklung sicherer und besserer Produkte zwingt konkurrierende Unternehmen dazu, noch bessere Produkte zu entwickeln. Eine Möglichkeit hierzu sind die Bug-Kopfgeld-Programme. Unternehmen bieten Externen Prämien an, wenn diese Bugs in ihrer Software finden. Dies ist wesentlich billiger als einen Angestellten für die gleiche Arbeit zu bezahlen. Microsoft hingegen kauft Verteidigungstechnologien auf, um diese Funktionen in ihre Software zu implementieren und geht juristisch gegen Botnetze vor. Facebook verklagt regelmäßig Netzwerke, die Spam versenden. Dieses Verhalten zwingt die Legislative dazu, sich anzupassen und neue Tools zu entwickeln.

Staaten sollten sich die USA als Vorbild nehmen. Im Rahmen einer breit gefächerten Cyber Security Strategie versuchen die USA, den Gefahren im Cyberspace durch nationale Verfahren entschlossen zu entgegnen. Russland und China legten den Vereinten Nationen den Entwurf eines Internationalen Code of Conducts für Informationssicherheit vor. China geht sogar noch einen Schritt weiter und plant die Kontrolle aller Inhalte des Internets. Indien, Brasilien und Südafrika fordern hingegen die Einrichtung einer internationalen Körperschaft, welche das Internet regulieren soll. Ohne koordiniertes, spezifisches Vorgehen werden die kooperationsfördernden Maßnahmen das Auftreten von Spam, Botnetzen und Pornografie jedoch nicht maßgeblich verringern können.

Die Zivilgesellschaft ist höchst abhängig von den von Staat und Wirtschaft etablierten Rahmenbedingungen. Sie sollte aber mehr Eigeninitiative zeigen. Einen Ansatz bildet die Gründung einer Non-Profit-Organisation durch Rechtsanwälte und Experten im Bereich der Cyberkriminalität. Diese Organisation könnte durch private Spenden, Sponsoring von Wirtschaftsunternehmen und staatliche Zuschüsse finanziert werden. Ihre Aufgabe wären rechtliche Schritte gegen alle Arten von Cyberkriminalität. Die Bürger können zudem über ihre Kaufkraft Einfluss auf Unternehmen ausüben, Gruppen bilden, Ressourcen wie Rechenleistung spenden oder Projekte vorantreiben.

Cybersicherheit durch Deglobalisierung der Technik

Les Bloom, John E. Savage: On Cyber Peace, *Atlantic Council Issue Brief*, August 2011

Der Cyberraum hat eine besondere Stellung im Wettbewerb der Staaten, zu dessen Erklärung das Heranziehen früherer sicherheitspolitischer Erfahrungen nicht ausreicht. Ein grundlegendes Problem ist die Unmöglichkeit absoluter Sicherheit, da die Netzwerke auf Funktionalität und nicht auf Sicherheit ausgelegt sind. Des Weiteren sind Netzwerke anfällig für die kleinsten Änderungen. Durch die globale Vernetzung sind Attacken jederzeit anonym ausführbar. Folglich hat sich in den letzten Jahren die Cyberkriminalität stark verbreitet. Mit geringem Können und einfacher Technik kann hoher Schaden verursacht werden.

Gegenmaßnahmen wie die Überprüfung auf schadhafte Soft- und Hardware sind zeitaufwändig und kostenintensiv; auch die Bekämpfung von Botnets ist extrem aufwendig. Doch Staaten müssen aktiv werden, um Schutz, Monitoring und normatives Verhalten durch Forschung und Entwicklung voranzutreiben.

Besonders der Schutz kritischer Infrastruktur stellt eine Herausforderung dar. Hier muss die Kooperation zwischen Regierung und privatem Sektor in großem Umfang ausgebaut werden. Weiterhin muss die Generierung von Cyber Incident Response Teams (CIRTs) folgen, welche durch Monitoring der Angriffe das Risikomanagement unterstützen. Doch bisher fehlt es an Methodik und umfassenden Standards zur Datenerfassung, um ein Frühwarnsystem zu

entwickeln, das die Reaktionszeiten der Abwehrmaßnahmen verkürzt. Gelingt dies, können CIRTs Best Practice-Vorgaben erstellen. Zudem müssen nationale Polizeieinheiten müssen ausgebildet werden und transnational kooperieren, wie dies die Konvention zu Cyberkriminalität des Europarates fordert.

Um die Zahl befallener Computer zu minimieren, müssen die Internetprovider (ISP) stärker eingebunden werden. Sie könnten etwa kompromittierte Computer oder Netzwerke sperren. Zusätzlich ist die Durchsetzung eines Prüfsiegels für internetfähige Computer denkbar. Hierfür müssen jedoch sowohl User als auch ISPs zur Rechenschaft gezogen werden, wenn sie die Bedingungen nicht einhalten. Auch die Hersteller von Soft- und Hardware müssen diesen Rechtsnormen unterworfen werden, Bugs in Software zu verhindern und eine zeitnahe Reparatur von Soft- oder Hardwarefehlern durch die Hersteller durchführen zu lassen. Dies gilt insbesondere für die Besitzer kritischer Infrastruktur.

Durch regelmäßige Neuaufsetzung des Systems könnten die Zeiträume potentieller Infektionen von Computern verkürzt werden. Auch die Arbeit in infizierten Systemen ist technisch machbar. Schwieriger ist die Sicherung des Border Gateway Protocols, welches den globalen Datenfluss zwischen den ISPs reguliert. Transnationale Kooperationen auf technischer und psychologischer Ebene bilden einen Lösungsansatz. Zudem muss die Einbindung anderer Akteure in Betracht gezogen werden. Versicherungsunternehmen können durch die Zertifizierung sicherer Systeme monetäre Anreize schaffen.

Ein bisher wenig beachteter Ansatz ist die Notwendigkeit der digitalen Entwicklungszusammenarbeit. Während Wissen und Technik in den Industrienationen verfügbar ist, stellt das Fehlen derselben in Entwicklungsländern ein Risiko für die globale Sicherheit im Cyberraum dar. Hier muss durch Wissenstransfer technischer Grundlagen sowie Hilfe beim Implementieren aktueller Software die Durchsetzung von Sicherheitsstandards unterstützt werden. Mehr…

Erhöhte Sicherheit durch Monitoring von Attacken

Shari Lawrence Pfleeger, Rachel Rue: Cybersecurity Economic Issues, *RAND Research Brief*, 2011

Es besteht ein massiver Bedarf an umfangreicheren Daten, einem breiteren Verständnis sowie einer genauen Methodik, um Cybersicherheit zu untersuchen. Hierbei muss der Fokus vor allem auf dem Schutz kritischer Infrastruktur sowie garantiert sicherer Software liegen. Für die Wirtschaft ergeben sich somit unterschiedliche Situationen, da einige Unternehmen stärker von Cyberunsicherheit betroffen sind als andere und die Bedeutung von Cybersicherheit folglich auch unterschiedlich bewertet wird.

So strebt ein betrieblich exzellentes Unternehmen primär nach hochwertigem Kundenservice. Da Effizienz und Engagement wichtig sind, wird auf eine gute Lieferkette geachtet. Digitale Sicherheit ist somit ein Aspekt von Qualität. Produktführer hingegen richten ihr Unternehmen nach Features und Funktionalität des Produktes aus. Innovation und Experimentierfreudigkeit gewinnen daher an Bedeutung. Dies erhöht das Risiko potentieller Bedrohungen, da Innovation und nicht der Prozess die Umsetzung der Sicherheit definiert. Somit muss sich Sicherheit der Leistung unterordnen. Bei dem dritten Wirtschaftszweig, der den Fokus auf Kundenvertrauen legt, ist Sicherheit durch die zentralisierten und auf den Kunden ausgerichteten Prozesse nur wichtig, sofern dies vom Kunden gewünscht wird.

Ein großes Problem für die digitale Sicherheit ist die bisher fehlende Standardisierung von Definition, Verfolgung und Meldung von Vorfällen. Die weit differierenden Bezeichnungen zur Art der Attacken sowie der Probenauswahl erschweren es Softwaremanagern, Datenauswahl und Komparativstudien korrekt auszuwerten. Die Mehrheit der Angriffsquellen ist unbekannt, ebenso gibt es große Unterschiede bei den Angriffstypen. Es werden jedoch Informationen zum Verhältnis von Grund und Effekt von Angriffen benötigt, um die Defensiventwicklungen voranzutreiben. Ein wesentlich schwerwiegenderes Problem ist das Unvermögen, die direkten und indirekten Kosten eines Sicherheitsbruches zu erfassen. Es kann davon ausgegangen werden, dass die Kosten meist um das 7- bis 10-fache unterschätzt werden.

Immer noch ist unbekannt, welche Entscheidungsprozesse zu welchen Investitionen in Sicherheitsarchitektur führen und wie effektiv diese Investitionen letztlich sind. Diesbezüglich ergab eine RAND Studie unter 36.000 US-amerikanischen Unternehmen, dass Projektmanager mehr Daten brauchen, um Entscheidungen zur Verteilung knapper Ressourcen im Bereich der digitalen Sicherheit zu treffen. Regierungen müssen nationale Standards und Richtlinien erarbeiten, welche die Erfassung von Vorfällen erleichtern und somit die Entwicklung von Best Practices und kosteneffektiven Technologien ermöglichen. Zusätzlich können Versicherungen auf Basis erhobene Daten spezifische Angebote für Policen gegen Cyberangriffe entwickeln. Benchmarks von Schutzmaßnahmen der kritischen Infrastruktur können zudem helfen, Art und Effektivität von Schutzmaßnahmen zu untersuchen und eine Trendanalyse durchzuführen.

Unternehmen leisten somit einen Beitrag, um die Cybersicherheit zu erhöhen. Durch standardisierte Datenerhebungen von Vorfällen, Sicherheitsmaßnahmen und Entscheidungsprozessen können Unternehmen Daten sammeln, welche koordinierte Initiativen zur Verhinderung von Attacken ermöglichen. Hier kann zusätzlich der Staat eingreifen und über normative und monetäre Anreize zur Harmonisierung der Sicherungsmaßnahmen beitragen. Mehr…

Cybersicherheit als Pflicht des Staates

Birgit Brünger et al: Digitale/Un-Sicherheit: Empfehlungen für mehr Sicherheit im Cyberraum, *stiftung neue verantwortung Policy Brief*, März 2011

Cybersicherheit wird aktuell als Zustand verstanden. Dies ist jedoch ein Trugschluss, denn Sicherheit als absoluter Zustand lässt sich im Cyberraum nicht erreichen. Cybersicherheit muss als Prozess verstanden werden, welcher unter Einbeziehung technischer, organisatorischer, rechtlicher und politischer Aspekte die Risiken auf ein gesellschaftlich akzeptiertes Maß reduziert. Da Staat und Wirtschaft teilweise unterschiedliche Interessen verfolgen, ergeben sich zwei Spannungsfelder: Im Spannungsfeld zwischen Staat und Gesellschaft versucht die Politik, negative Konsequenzen der Liberalisierung von in privater Hand befindlicher kritischer Infrastruktur aufzufangen, ohne zusätzlich regulieren zu müssen. Im Spannungsfeld zwischen Staat und Bürgern steht die Balance zwischen Sicherheit und Freiheit im digitalen Raum im Vordergrund.

Die Hauptaufgabe des Staates ist der Schutz kritischer Infrastruktur. In sensiblen Bereichen kann dies über eine Entnetzung – die Abtrennung des Netzwerks vom Internet – erreicht werden, in anderen Bereichen darf die Vernetzung als Teil des Fortschrittes nicht eingeschränkt werden. Der Schutz von Infrastruktur generell obliegt der Wirtschaft, zum Beispiel durch die Einführung selbstregulatorischer Maßnahmen. Besonders bei öffentlich-privaten Partnerschaften kann allerdings nicht auf die freiwillige Kooperation der Wirtschaft mit dem Staat gehofft werden. Hier muss der Staat Maßnahmen entwickeln, die auf Betreiber kritischer Infrastruktur zielen. Dies kann über ein verbindliches Zertifikat erreicht werden. Da unzureichend gepatchte Systeme den Hauptangriffsweg für einfach Cyberangriffe darstellen, muss grob fahrlässiges Sicherheitsverhalten rechtliche Konsequenzen haben.

Oft sind auf Druck von Regierungen Hintertüren für Spionagezwecke in Software eingebaut. Aufgrund des globalen Marktes kann hier eine nationale Gesetzgebung nichts ausrichten. Im militärischen Bereich hingegen wird Open-Source-Software genutzt, da diese auf erprobten und sichtbaren Sicherheitsstandards beruht. Open-Source-Software muss aber konkurrenzfähig zu anderen Geschäftsmodellen operieren können. Dazu muss die Patentierung von Software durch klare rechtliche Vorgaben unterbunden werden, da dies für kleine und mittelständische Unternehmen ohne eigene Rechtsabteilung ein Existenzrisiko darstellt.

Auch die Gesetzgebung muss praxisnah weiterentwickelt werden. Denn bisher werden vom Gesetz nur Tools erfasst, die ausschließlich für die Durchführung einer Straftat nutzbar sind. Doch alle dual-use Tools, die mehrere Verwendungszwecke haben können, werden hiervon nicht erfasst. Zusätzlich greift die Gesetzgebung mit reiner Abschreckung der Angreifer zu kurz – auch grob fahrlässig handelnde Betreiber von IT-Systemen müssen belangt werden.

Zuletzt bedarf es eines globalen Cyberfriedens. Das Mistrauen der Staaten gegenüber operativen Kapazitäten und Intentionen anderer Staaten kann leicht

zu einem neuen Sicherheitsdilemma führen. Es bedarf internationaler Normen mit deeskalierendem Charakter. Zusätzlich sollten Vertrauensnormen und vertrauensfördernde Maßnahmen erarbeitet und die rhetorische Aufrüstung des Cyberraums zum virtuellen Schlachtfeld unterbunden werden.

Eine umfassende Gewährleistung von Sicherheit ist nicht mehr möglich. Cyberkriminalität und -spionage wird ein Problem bleiben. Die Gesellschaft muss lernen, mit der Unsicherheit zu leben, Szenarien für Ausfälle zu erlernen und eine latente Toleranz gegenüber solchen Ereignissen entwickeln. Mehr…

Fehlende interne Kommunikation gefährdet digitale Sicherheit

Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen: Grad der Sensibilisierung des Mittelstandes in Deutschland, *Bundesamt für Sicherheit in der Informationstechnik*, Oktober 2011

99% aller deutschen Unternehmen werden den kleinen und mittleren Unternehmen (KMU) zugeordnet, ihre Bedeutung für die Wirtschaft ist hoch. Eine funktionierende IT-Infrastruktur im Zuge elektronischer Geschäftsprozesse ist unabdingbar. Vertraulichkeit, Verfügbarkeit und Integrität der KMU müssen durch Cybersicherheit gewährleistet werden.

Durch getrennte Befragung von Geschäftsführung und IT-Bereich konnte eine grundsätzlich geeignete Aufstellung der KMU bezüglich der IT-Sicherheitsmaßnahmen nachgewiesen werden. Die KMU setzen rund zwei Drittel der von Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Maßnahmen um. Dennoch besteht massiver Nachbesserungsbedarf, besonders im Bereich der geschäftskritischen IT-Sicherheitsprozesse. Der Umgang mit Sicherheitsvorfällen und dem Notfallmanagement sowie die Bewertung der Gefahrenbereiche weisen gravierende Schwächen auf. Hierfür ist der weit verbreitete ‚Funktionale Optimismus' verantwortlich. So ist es wenig verwunderlich, dass die Reaktion auf Vorfälle eine Folge nicht aufeinander abgestimmter Einzelaktionen ist und nicht – wie erforderlich – einem Prozess als Arbeitsgrundlage entspricht. Oftmals sind diese Handlungsfolgen das Ergebnis von Versuch und Irrtum, anstatt einem vorher festgelegten Konzept zu folgen. Dies ist umso erstaunlicher, da Cybersicherheit sowohl von Seiten der Geschäftsführung als auch von Seiten der IT-Techniker hohe Bedeutung beigemessen wird. Das Bewusstsein für das Thema ist nachweisbar hoch, jedoch lässt die Etablierung eines IT-Sicherheitsmanagements stark zu wünschen übrig. Besonders langjährige IT-Techniker werden als Garant für Sicherheit gesehen, jedoch wird durch finanziellen und zeitlichen Druck eine Auseinandersetzung mit Cybersecurity oftmals verhindert. Dabei ist speziell geschultes und ausgebildetes IT-Personal in der Lage, Angriffe zu erkennen und frühzeitig abzuwehren.

Die Unternehmensführung sieht die IT als Kostenfaktor an. Investitionen erfolgen nur bei akuten Bedrohungen und nur in unbedingt erforderlichem Kostenrahmen. Hier können regionale Aktionsbündnisse stärkerer Wirtschaftsunternehmen mit Projekten zur Selbsthilfe die Initiative übernehmen. Ergänzend sollten die Zusammenarbeit mit Verbänden und Kammern vor Ort gestärkt und Kompetenzzentren gegründet werden. Bisher sind die verfügbaren Angebote regional unterschiedlich stark ausgeprägt. Ein von Unternehmen selbst organisierter partnerschaftlicher Wissensaustausch mit gegenseitiger Beratung zu Cybersicherheit durch IT-Mitarbeiter kann als Multiplikationsereignis durch die Verbände und Kammern gefördert werden.

Die teilweise Auslagerung der IT-Sicherheit mit Komplettlösungen von IT-Sicherheitsdienstleistern ist ein weiterer Weg, der rapide zunehmenden Bedrohung entgegenzutreten. Da dies jedoch Unternehmensinterna offen legt, muss großer Wert auf die Auswahl eines zuverlässigen und vertrauenswürdigen Partners gelegt werden. Obwohl es viele Angebote zu Hilfestellungen und Informationen gibt, sind diese den Unternehmen kaum bekannt. Die Landesämter für Verfassungsschutz beraten zu Wirtschaftsspionage, das BSI bietet Sicherheitsprodukte und Bildungsangebote an. Die kostenfreien und seriösen Angebote sind allerdings aufgrund der Reizüberflutung im Segment des Cyberschutzes sehr schwer wahrzunehmen. Mehr…

Fehlender Schutz bedroht britische Cybersicherheit

Paul Cornish et al: Cyber Security and the UK's Critical National Infrastructure, *Chatham House Report*, September 2011

Die Integration von Informations- und Kommunikationstechnik ist ein bestimmender Faktor unseres modernen Lebens und hat Auswirkungen für Staat, Wirtschaft und Gesellschaft. Durch diese Abhängigkeit entsteht jedoch auch ein Schadenspotential. Dies gilt besonders im Bereich vitaler Strukturen – der kritischen Infrastruktur (KI). Großbritannien entwickelte hierzu die National Security Strategy (NSS) und Strategic Defence and Security Review (SDSR).

Im Zuge von Erhebungen wurde deutlich, welch differierenden Kenntnisse, Kapazitäten und Prozesse die Verbindung von IT und KI bedingen. Wenn das Sinnbild von Sicherheit eine Mauer wäre, müsste diese in erster Instanz nicht hoch sein, sondern fortlaufend und unversehrt. Die Realität ist jedoch wesentlich zersplitterter, dies zeigt sich unter anderem an der Fülle verschiedener Best-Practice-Ansätze. Einige Unternehmen haben Sicherheitsprotokolle eingerichtet, welche jedoch von unverantwortlichen, schädigenden Maßnahmen begleitet werden und den Sicherheitsgewinn negieren. Da sich besonders viele kritische Infrastrukturen in der Hand öffentlich-privater Partnerschaften befinden, lässt sich mit einer zentralisierten Struktur sehr wenig nachhaltig beeinflussen. Daher liegt eine deutliche Verantwortung in den Händen derer, die von der Bedrohungslage am stärksten betroffen sind: den Unternehmen des privaten Sektors.

Auch bei britischen Unternehmensführungen herrscht großes Unwissen über das Schadenpotential von Cyberbedrohungen. Ebenso ist den Geschäftsführungen nicht klar, wohin sie sich für Hilfe wenden sollen. Firmen ohne Cybersicherheit laufen Gefahr, großen Schaden zu nehmen. Regierungsämter arbeiten wesentlich schneller und engagierter als Wirtschaftsunternehmen an der Verbesserung ihrer Schutzmechanismen. Trotz konstanter Zunahme der Bedeutung von Cybersicherheit nimmt der Wille für zusätzliche Ressourcen im Bereich Cybersicherheit konstant ab.

Die größte Verwundbarkeit im Cyberraum ist nicht die mögliche Ausnutzung von Lücken. Es sind die fehlende Wahrnehmung und Mission, die Abwesenheit uniformer Strategien und die Unfähigkeit effektiver Kommunikation. Fundamentale Prozesse, die zum Bild einer sich ins Negative verändernden Gesellschaft beitragen. Es ist dringend nötig, eine Sicherheitskultur innerhalb kritischer Infrastrukturzweige aufzubauen. Hierzu bedarf es konstanten Managements durch informierte und proaktive Führungspersonen in Wirtschaft und Staat. Mehr…

Kürzung der EU-Verteidigungshaushalte schränkt Sicherheit ein

Fabio Liberti: Defence spending in Europe: Can we do better without spending more, *Notre Europe Policy Paper 46*, Juni 2011

Seit Ende des Kalten Krieges sind im Zuge des plötzlichen Ausblicks auf eine friedliche Ära in Europa die Verteidigungshaushalte radikal gekürzt worden. Viele Ressourcen wurden in andere Bereiche umverteilt – Bereiche, die erfolgversprechender für eine Wiederwahl schienen. Während in der zweiten Hälfte der 1980er Jahre die Verteidigungsausgaben europäischer Staaten bei 3,1% des BIP lagen, verringerten sie sich bis 2008 auf 1,7%. Im gleichen Zeitraum sank der Anteil der Verteidigungsausgaben der USA von 6% auf 4%.

Das Ende des Kalten Krieges bot den USA die Möglichkeit, ihre Verteidigungsindustrie und -technik neu zu organisieren. Der folgende Umbau erzeugte über massive industrielle Zentralisierung die fünf großen Rüstungskonzerne, welche komplexe Aufgaben übernehmen und durch den großen internen US-Markt sowie von der Regierung unterstützte Exporte profitieren konnten. In Europa hingegen wurde diese Restrukturierung nur teilweise durchgeführt. Die Ausrichtung auf schwere Verteidigungssysteme in Erwartung einer sowjetischen Panzerinvasion musste umgestellt werden. Doch schnell wurde das Fehlen wichtiger Kapazitäten deutlich. Strategische Transportkapazitäten, Kommunikation, Aufklärung, Logistik und Satellitenunterstützung waren rar und kostenintensive Ressourcen für deren Entwicklung und Einführung wurden benötigt. Doch nur 20% der Verteidigungshaushalte kamen für Forschung und Entwicklung zum Einsatz. Die USA hatten hier den Vorteil, mit einer zentralisierten Struktur zu arbeiten,

während die Entscheidungen innerhalb der EU von 27 souveränen Staaten dezentralisiert getroffen werden mussten.

Die Wirtschaftskrise führt dazu, dass Personal eingespart und die Ausmusterung von Material vorangetrieben wird. Inzwischen sind nur 5% bis 6% der 1,8 Mio. europäischen Soldaten ausreichend trainiert und ausgerüstet. Die europäischen Staaten haben von den 2008 für Verteidigung ausgegebenen 200 Milliarden Euro nur 40 Milliarden für Forschung ausgegeben. Zukünftig ist eine weitere Reduzierung der Verteidigungsbudgets sehr wahrscheinlich. Diese Sparmaßnahmen werden nicht kohärent mit den europäischen Partnern durchgeführt werden. Sie werden die Modernisierung der Streitkräfte merklich verzögern und die Unterschiede zwischen den europäischen Streitkräften erhöhen. Die Folge wird ein Souveränitätsverlust der Europäer bei Sicherheits- und Verteidigungstechnologien sein. Mehr…

USA besorgt über Sicherheit pakistanischer Nuklearwaffen

Jeffrey Goldberg, Marc Ambinder: The Ally From Hell, *The Atlantic*, Dezember 2011

Die unilaterale Aktion der USA zur Gefangennahme von Bin-Laden belastet die US-pakistanischen Beziehungen sehr. Doch nicht erst seit den teilweise geheimen Drohneneinsätzen im pakistanischem Luftraum ist das US-amerikanische Verhalten Pakistans und speziell dem militärischer Geheimdienst Pakistans (ISI) gegenüber belastet.

Eine der Hauptsorgen der USA sind die Sicherheitsrisiken pakistanischer Nuklearwaffen. Sowohl die genaue Anzahl der nuklearen Sprengköpfe – man rechnet mit 100 – als auch ihre Lage sind unklar. Pakistan verlegt zur Verhinderung von Angriffen sein Nuklearpotential regelmäßig. Islamabad will so den Zugriff terroristischer Gruppen und indische Angriffe auf ihr Nuklearmaterial sowie US-amerikanische Aktionen verhindern. Die USA befürchten jedoch, dass nukleare Offensivkapazitäten in die Hände terroristischer Gruppen gelangen könnten. Einerseits gilt das pakistanische Militär, allen voran die Marine, als mit Terrorgruppen sympathisierend. Dies wurde durch Insider-Hilfe bei Angriffen auf Stützpunkte, an denen mutmaßlich Nuklearwaffen lagerten, deutlich. Andererseits verlagert Pakistan seine Nuklearwaffen nicht mithilfe massiv gesicherter Konvois, sondern mit gering geschützten zivilen Fahrzeugen. Dies soll die Auffälligkeit verringern und damit mögliche Angriffe verhindern. Zusätzlich werden aus Sicherheitsgründen Nuklearsprengköpfe und Zünder getrennt gelagert, beim Transport werden sie jedoch mitunter gemeinsam transportiert. Eine so erbeutete Nuklearwaffe kann sofort gezündet werden.

Militär und Geheimdienst Pakistans – von Terrorgruppen unterwandert – wie auch die permanente unsichere Verlagerung der Nuklearkapazitäten stellen ein hohes Risiko für die Region dar. Zudem ist das Verhältnis zwischen Pakistan und den USA geprägt von Lügen. Pakistan lügt ob der Verbindungen des ISI zu Terrorgruppen, die USA täuschen sich selbst, indem sie die Lügen als solche akzeptieren. Jedoch gibt es seit geraumer Zeit Pläne, was bei der Entwendung einer kleinen Anzahl von taktischen Nuklearwaffen durch US-Spezialkräfte zu tun wäre. Auch Einsatzpläne für den Verlust großer Mengen pakistanischer Nuklearwaffen existieren. Diese sehen vor, große Streitkräftetruppen für die Dauer der Sicherstellung und Entschärfung des Nuklearpotentials einzusetzen. Pakistan wiederum würde eine Invasion von US-Truppen nicht hinnehmen und seinerseits offensiv gegen die US-Kräfte vorgehen.

Die Sicherung pakistanischer Nuklearsenale wird durch tiefgehendes Misstrauen erschwert. Anzahl, Ort und tatsächliche Gefährdungslage der pakistanischen Nuklearwaffen sind unbekannt. Der neue Direktor der CIA, General Petraeus, kann hier über seine guten persönlichen Beziehungen in das Land die Beziehungen zwischen den USA und Pakistan stabilisieren. Zusätzlich darf der Stabilisierungsansatz der USA in der Region nicht unilateral erfolgen. Ihm muss ein breites Verständnis der pakistanischen Gesellschaft zugrunde liegen. Nur so kann eine Sicherung pakistanischer Nuklearwaffen erreicht und zur Stabilisierung der ganzen Region beigetragen werden. Mehr…