Stellungnahme des Chaos Computer Clubs e. V.

zum öffentlichen Gespräch mit Sachverständigen zum Thema

"IT-Sicherheit in der Wirtschaft"

Deutscher Bundestag, Unterausschuss Neue Medien

15. Oktober 2012, 13 Uhr, P-L-H E 800

1. Fragen der Koalitionsfraktionen CDU/CSU und FDP

1.1.1 Bedrohungspotentiale / Nachholbedarf
1.1.2 Ergriffene Maßnahmen

1.2. Maßnahmen im Branchenvergleich IKT / Sonstige, Optionen KMU

1.3.1 Häufigkeit gezielter "Cyberattacken"
1.3.2 Rückmeldungen betroffener Unternehmen
1.3.3 Häufigkeit strafrechtlicher Ermittlungen im Kontext von Angriffen
1.3.4 Kosten von Sicherheitsmaßnahmen

2. Fragen der Fraktionen der SPD, von Bündnis 90/Die Grünen und Die Linke

2.1.1 Resonanz der Kooperationsplattform zur Meldung von Angriffen
2.1.2 Zeitraum zur Evaluation einer Selbstverpflichtungsinitiative
2.1.3 Tragfähigkeit Selbstverpflichtung im Vergleich zur gesetzl. Meldepflicht

2.2. Realisierbarkeit eines allgemeinen Lagebildes

2.3.1 Beratungsfähigkeit des BSI für KMU im Kontext unterschiedlicher Interessen
2.3.2 Strukturelle Interessenskonflikte des BSI und Lösungsansätze

1. Fragen der Koalitionsfraktionen CDU/CSU und FDP

1.1.1 Worin sehen Sie derzeitig für deutsche Unternehmen (differenziert nach Branchen und Unternehmensgröße) die größten Bedrohungspotentiale, und wo sehen Sie den größten Nachholbedarf für Verbesserung der Sicherheitsstandards bei den Unternehmen?

Im Bezug auf das Vermögen, sich mit den prozessualen Anforderungen von IT-Sicherheit auseinanderzusetzen, ist Techniknähe und damit einhergehende Erfahrungen sowie die mit der Unternehmensgröße einhergehende Möglichkeit der Schaffung eigener Stellen für die Belange der IT-Sicherheit entscheidend.

Die IT-Abteilungen haben in der Regel nur die Aufgabe, den Betrieb aufrechtzuerhalten, IT-Sicherheit wird dieser Aufgabe – inkl. der budgettechnischen Implikationen – üblicherweise untergeordnet. Somit fehlen die Ressourcen, um sich umfassend mit Angriffstechniken und Risiken der eingesetzten Technik vertraut zu machen, oftmals gekoppelt mit einem naiven Vertrauen auf sogenannte "Sicherheitsprodukte".

Ausbaufähig ist in diesem Kontext auch die prozessuale Vorbereitung auf das Versagen sogenannter Sicherheitsprodukte durch Begrenzung des im jeweiligen Fall eintretbaren Schadens.

1.1.2 Welche Maßnahmen wurden bisher ergriffen bzw. sind in Planung, um einen Informationsaustausch über Bedrohungslagen und mögliche Schwachstellen, Angriffe und Angreifer zu ermöglichen?

Der Chaos Computer Club versucht seit vielen Jahren, vor allem die offene Kommunikation über Schwachstellen, Störfälle und Erfahrungen bei Sicherheitsschwankungen im IT-Kontext zu beleuchten. Dies scheint uns insofern ein kulturell wichtiger Aspekt, als daß die offene Kommunikation von Problemen existenziell für eine realistische Einschätzung der Sachlage ist, im Kontext von Unternehmen aber oftmals an Hierarchie- und Reputationsaspekten leidet.

Auch die Offenlegung technischer Details von Sicherheitsmaßnahmen ist für die Bewertung von Prozessen entscheidend, da in vielen Bereichen die Haftung der Betreiber unzureichend von Haftungsproblemen der Nutzer abgegrenzt ist. Die aktive Kommunikation der Strukturen, in denen die Daten von Benutzern verarbeitet werden (Datenbrief), ist noch nicht in dem Maße umgesetzt, um den Nutzern eine eigene Risikoeingrenzung zu ermöglichen.

Da in der öffentlichen Berichterstattung noch keine einheitliche Klassifizierung und Abgrenzung von Störfällen, IT-Angriffen, Datenlecks und Innentäter-Delikten eingeführt ist, wäre eine Klassifizierung auch für die öffentliche Diskussion hilfreich. Hierzu wäre es außerdem hilfreich, sich an den wissenschaftlichen Begriffen (Verfügbarkeit, Authentizität, Integrität etc.) zu orientieren und sowohl Konsequenzen als auch Betroffene/ Verantwortliche klarer zu benennen.

Aspekte der IT-Sicherheit spielen zwar bei der Gestaltung von IT-Infrastrukturen heute schon eine Rolle, die Offenlegung eigener Unzulänglichkeiten hingegen hat in der marketingorientierten Kommunikation von Unternehmen keinen Stellenwert.

Zur realistischen Bewertung von Marketingaussagen sind die Aussagen des japanischen AKW-Betreibers Tepco im Kontext des Fukushima-Reaktors ein interessantes Lehrbeispiel im Bezug auf die Kluft von Darstellungen und Realitäten, die sich auch auf IT-Sicherheit übertragen lassen, wenn auch mit weniger drastischen Konsequenzen.

IT-Sicherheit muss als fortlaufender Prozess mit stetigem Kommunikationsbedarf verstanden werden, Momentaufnahmen vermitteln u. U. kein realistisches Bild von Risiko- und Schadenshöhen-Faktoren.

In wenigen Branchen (etwa bei den Nachrichtendiensten und beim Militär) ist es möglich, IT-Kommunikationsstrukturen aufgrund entstehender Sicherheitsrisiken noch im erheblichem Umfang zu reduzieren. Die in diesem Kontext genutzten regulatorischen Mittel sind jedoch in der freien Wirtschaft nicht realistisch anzuwenden. Die erhebliche Entwicklungsdynamik steht der Theorie zertifizierter Software dabei ebenso entgegen wie die notwendige Interoperabilität von vernetzten Systemen.

1.2 Unternehmen aus der IKT-Branche haben signifikant höhere Sicherheitsvorkehrungen getroffen als Unternehmen anderer Branchen. Worin sehen Sie die Ursachen hierfür und wie können insbesondere kleine und mittlere Unternehmen (KMU) anderer Branchen stärker von den Erfahrungen und Wissen aus der IKT-Branche profitieren?

Unternehmen mit branchenbedingter Nähe zur ITK-Technik profitieren in Ihrem Einschätzungsvermögen von den eigenen Erfahrungen, auch im Bezug auf sogenannte "Sicherheitstechnik" und ihren oft unerfüllten Versprechungen.

Die allgemein zunehmende Abhängigkeit von ITK-Technik darf aber in allen Branchen als normal gelten, daher ist der Aufbau eigenen Personalstamms für die Beherrschung von IT-Technologie und -Risiken grundsätzlich empfehlenswert.

Hierbei ist für die Unternehmen entscheidend, sich eigenes Know-How für die Einschätzung der IT-Risiken aufzubauen, um auch die prozessualen Implikationen für Ihre Geschäftsprozesse bei Gestaltung derselben zu berücksichtigen.

Auch wenn externe Dienstleister in speziellen Bereichen unumgänglich sind, ist generell die Abhängigkeit von externen Dienstleistern beim Betrieb der eigenen IT-Strukturen grundsätzlich zu vermeiden, da es sich zunehmend um vitale Lebensadern der Unternehmen handeln. Investitionen in eigenes Personal und Know-How sind daher Investitionen in externe Dienstleister grundsätzlich vorzuziehen.

1.3.1 Wie häufig sind nach Ihrer Kenntnis deutsche Unternehmen (differenziert nach Branchen) gezielten Cyberattacken ausgesetzt gewesen?

Der Begriff "Cyberattacke" ist nicht geeignet, in diesem Kontext die notwendige Differenzierung von Angriffsformen einzuleiten. Zu unterscheiden sind u. a. Abtastungen von Infrastrukturen, Erprobung von Angriffstechniken (etwa im Kontext von Überprüfungen), Injizierung von Angriffswerkzeugen, Ausspähen von Verbindungen, Angriffe auf die Verfügbarkeit und viele weitere Formen.

Verläßliche Zahlen sind in diesem Kontext von keinem Akteur zu erwarten, oftmals handelt es sich bei übersichtshaften Darstellungen von IT-Angriffen mit Zahlen nur um Marketingmaßnahmen zur Bewerbung sogenannter (aber kaum zielführender) "Sicherheitsprodukte" oder um Regierungsstellen mit Kompetenzausweitungsbedarf.

Im Umkehrschluß gibt es auch Angriffe erheblicher Relevanz und Brisanz, die zwar von den beteiligten technisch bewanderten Akteuren erfaßt werden, aber aufgrund ihrer Komplexität und des auf der Entscheiderebene mangelnden Sachverstands dort nicht diskutiert werden können.

1.3.2 Wie sind die bisherigen Rückmeldungen von Unternehmen, die Opfer von Angriffen auf ihre elektronische Infrastruktur geworden sind?

Zu Unterscheiden sind hier zunächst

a) Unternehmen, die Opfer von Angriffen auf ihre elektronische Infrastruktur geworden sind und diese Angriffe bemerkt haben

b) Unternehmen, die Opfer von Angriffen auf ihre elektronische Infrastruktur geworden sind und diese Angriffe (noch) nicht bemerkt haben

zudem kommt die sehr unterschiedliche ausgeprägte Bereitschaft von Unternehmen, über Probleme zu sprechen, unabhängig davon, ob man dort schon bemerkt hat, daß man angegriffen wurde.

Die in 1.3.1 bereits angesprochenen Klassifizierungen und Definitionen unterschiedlicher Angriffsform muß zunächst durchgeführt werden. Hier ist auch zu berücksichtigen, ob personenbezogene Daten und Systeme Dritter durch Angriffe in Mitleidenschaft gezogen wurden.

Weder eine Meldepflicht noch anonymisierte Befragungen werden hier die Hemmschwelle von Unternehmen abbauen, die eigenen Probleme in ihrer Infrastruktur Dritten gegenüber zu beleuchten. Aus unserer Sicht kann nur eine offene Kommunikationskultur langfristig die so entstehenden Dunkelziffern beseitigen.

Die öffentliche Diskussion über Angriffe auf die IT-Infrastruktur von Unternehmen leidet unter dem Wunsch der Unternehmen, die Sicherheit ihrer Infrastruktur gegenüber Dritten aus Reputationsgründen als sicher darzustellen. Angriffe werden in der Regel auch innerhalb von Unternehmen nur im Kreis der unmittelbar Betroffenen diskutiert, auch die Unternehmensleitung wird in der Regel nur involviert, wenn die Ereignisse erhebliche Auswirkungen auf die Geschäftsprozesse oder das Ansehen des Unternehmens haben, da die Beteiligten auch ungern gegenüber Vorgesetzten Probleme bei der Beherrschung der Ihnen anvertrauten Infrastruktur eingestehen.

1.3.3 Haben Sie Kenntnis darüber, wie häufig sich an Übergriffe strafrechtliche Ermittlungen anschließen und warum von Unternehmen von diesen unter Umständen abgesehen wird?

Mögliche Gründe, warum Unternehmen von strafrechtlichen Ermittlungen absehen:

- Der Angriff soll intern wie extern vertuscht werden.
- Der Angriff soll nicht Dritten gegenüber offengelegt werden.
- Strafanzeigen sind grundsätzlich öffentliche Akte oder können zu solchen werden, was es zu vermeiden gilt.
- Reputationsschäden wirken sich u. U. sehr direkt auf den Unternehmenswert oder Aktienkurs aus.
- Das Vertrauen auf Erfolg bei den Ermittlungen anhand der vorliegenden Spuren ist zu gering.
- Der Angriff wurde erst durch die Verletzung einer Schutzpflicht möglich.
- Wenn personenbezogene Daten betroffen sind, besteht Angst vor weiteren Rechtsfolgen.
- Haftung bei Verlust von Geschäftsdaten anderer Unternehmen (z. B. CAD-Dateien) droht.
- Der Angriff wird gar nicht erst erkannt.

Diese Liste erhebt keinen Anspruch auf Vollständigkeit.

1.3.4 Besteht aus Ihrer Sicht die Notwendigkeit zu einer gesetzlich verpflichtenden zentralen Registrierung der Attacken und möglicher Folgen, um daraus eventuelle Schlüsse auf geeignete Abwehrmaßnahmen ziehen zu können?

Eine gesetzlich verpflichtende Registrierung von Angriffen auf IT-Systeme kann nur dort eingefordert werden, wo die Interessen Dritten unmittelbar betroffen sind, etwa:

- wenn personenbezogene Daten betroffen sind (Identitätsdiebstahl, Ausspähen von Kreditkarten-, Konten-, Meldedaten etc.)

- wenn Dritte durch Angriffe von der eigenen Infrastruktur ausgehend betroffen sind (zum Beispiel Entdeckung von Botnetz-Komponenten in der eigenen Infrastruktur, die dem legendierten Angriff auf Dritte dienen und/oder womöglich gedient haben).

Eine gesetzlich zwingende Registrierung kann auch im Kontext von Schadensregulierung (Klärung von Haftungsfragen) eine Komponente sind, so daß die Meldung von Angriffen incentiviert werden kann.

Zur Sicherstellung, daß die den Angriffen zugrundeliegenden technischen Details allen Betroffenen zur Verfügung stellen, wären CERT-Strukturen geeignet.

1.3.5 Können Sie beziffern, in welcher Höhe deutschen Unternehmen derzeitig Kosten für die eigene Sicherheit im Cyberraum entstehen und welche Veränderungen erwarten Sie hier in Zukunft?

Wie schon bei Frage 1.3.1 entstammen die in diesem Kontext vagabundierenden Zahlen aus Marketingmaßnahmen oder der Budgetallozierung staatlicher Stellen.

Klar ist: Die im Kontext der Vernachlässigung und Fehleinschätzung von IT-Sicherheit eintretenden Probleme sind *teuer*, mit zunehmenden Einsatz von IT-Systemen in allen Bereich und Branchen wird es in Zukunft richtig *teuer*.

Sehr teuer sind in diesem Kontext allerdings auch oft sogenannte "Sicherheitsprodukte", die keine prozessualen Verbesserungen bewirken, sowie "Compliance-Lösung", die der Anpassung an Regelwerke dienen, die wiederum oft unabhängig von den betrieblichen Erordernissen eine rein fiktive Sicherheitsrealität erzeugen sollen.

Das bei den Behörden wie dem BSI vorhandene Fachwissen sollte nicht nur dazu genutzt werden, sogenannte "Sicherheitsprodukte" durch Zertifizierungen aufzuwerten, sondern auch dazu, Produkte und Maßnahmen, die keinen zielführenden Charakter für die Erhöhung des Sicherheitsniveaus haben, als solche zu benennen.

2. Fragen der Fraktionen der SPD, von Bündnis 90/Die Grünen und Die Linke.

2.1.1 Welche Resonanz hat die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) angestoßene freiwillige Kooperationsplattform für die Meldung von IT-Angriffen bislang erfahren?

Eine Resonanz konnten wir bei unserer Erforschung des Sachverhaltes nicht feststellen, wenn man von einer herausgegebenen Pressemitteilung absieht.

2.1.2 Wie viel Zeit sollte einer solchen Selbstverpflichtungsinitiative eingeräumt werden?

Mangels ausführlicher Beleuchtung des Vorhabens kann diese Maßnahme zum jetzigen Zeitpunkt (noch) nicht seriös bewertet werden. Eine der aus unserer Sicht unbeantworteten Kernfragen lautet, welchen Anreiz betroffene Unternehmen haben sollten, sich bei Vorfällen an das BSI oder ähnliche Stellen zu wenden.

2.1.3 Stellt sie eine tragfähige Alternative zu einer allgemeinen Meldepflicht dar und wenn nein, wie ist die Einführung einer allgemeinen Meldepflicht auch und gerade vor dem Hintergrund der bereits bestehenden Meldepflicht bei Datenpannen im Bundesdatenschutzgesetz zu bewerten?

Grundsätzlich sie hier auf die bei der Antwort zu Frage 1.3.4 skizzierten Parameter verwiesen.

Eine allgemeine Meldepflicht kann hier realistischerweise nur im Kontext von betroffenen Dritten und gravierendem öffentlichen Interesse eingeführt werden, allerdings wird die Aussagebereitschaft von Unternehmen zu Störfällen in direktem Zusammenhang damit stehen, welche positiven Effekte für die Unternehmen daraus entstehen können.

2.2. Wie illusionär ist die Vorstellung der Erlangung eines allgemeinen Lagebildes über IT-Angriffe auf bundesdeutsche IT-Strukturen angesichts der Vielschichtigkeit der Angriffsmöglichkeiten und der unterschiedlichen Bewertungen von möglichen Sicherheitsstandards?

Ein solches Lagebild würde voraussetzen, daß es wirklich so etwas wie eine bundesdeutsche IT-Struktur gibt. Die Vorstellung mag vor fünf oder zehn Jahren noch teilweise korrekt gewesen sein. Da jetzt aber immer mehr Firmen externe Dienstleistungen sowie Dienste im Ausland einkaufen und einsetzen, kann ein Angriff beispielsweise auf einen US-amerikanischen Cloud-Provider oder eine koreanische Softwarefirma schwere und direkte Auswirkungen auf die IT-Infrastruktur deutscher Firmen haben.

Daher empfehlen wir, ein solches Lagebild nach Möglichkeit international auszurichten.

Dabei wäre ein Lagebild auch jetzt schon eine sinnvolle Aufgabe für die beteiligten Stellen wie das BSI, da hier auch mit dem jetzt bereits vorhandenem Wissen ein Anreiz für Unternehmen geschaffen werden kann, die öffentliche Darstellung und Wahrnehmung der Probleme zu ergänzen, um zu realistischen Einschätzungen und Maßnahmen zu kommen.

2.3.1 Inwieweit kann das BSI in seiner jetzigen Ausrichtung und Organisationsstruktur in seiner Doppelfunktion als Beratungszentrum für staatliche Einrichtungen und Sicherheitsbehörden auch die Wirtschaftsunternehmen – und zwar von den KMU bis hin zu den weltweit operierenden Unternehmen – unabhängig beraten, oder entstehen hier Interessenskonflikte?

Die im Rahmen der behördlichen Dienstleistungsfunktion an das BSI herangetragenen Aufgaben (z. B. von Ermittlungsbehörden) sind u. U. nicht komplikationsfrei mit dem Ziel zu verbinden, ein möglichst hohes technisches Sicherheitsniveau zu erwirken. Eine der technischen Sicherheit verpflichtete Stelle wäre daher grundsätzlich eher im Aufgabengebiet des Forschungs- oder Bundeswirtschaftsministeriums als beim Innenministerium anzusiedeln, um die Entscheidungsträger nicht unnötig diesen Zielkonflikten auszusetzen.

In der Vergangenheit gab es bereits mehrfach entsprechende Konflikte, ohne daß die entsprechenden Konsequenzen einer Entflechtung gezogen wurden.

2.3.2 Bestehen unterschiedliche Interessenlagen zwischen den Sicherheitsinteressen der Behörden einerseits und anderseits für die Sicherheitsinteressen von Unternehmen sowie aus der Beschaffung für die öffentliche Hand? Wenn Sie der Auffassung sind, dass es hier – um die Unternehmen auch von staatlicher Seite in ihren Sicherheitsvorkehrungen zu unterstützen – Änderungen bedarf, wo sehen Sie die Notwendigkeit und wie sollte die Ausgestaltung des BSI aussehen?

Ermittlungsbehörden und Nachrichtendienste sind bis zu einem gewissen Grad an IT-Unsicherheit interessiert, um z. B. staatliche Überwachung oder (Industrie-)Spionage durchführen zu können.

Firmen, die auf einem Markt aktiv sind, in dem IT-Sicherheit reguliert wird und in dem Zertifizierungen verlangt werden, haben ein großes Interesse daran, diese Zertifizierung zu bekommen. Fehlen zum Einsatz von neuen Techniken in der IT-Sicherheit notwendige Zertifizierungen oder sind diese nur mit großem finanziellen Aufwand zu erlangen, werden diese vermutlich nicht eingesetzt werden. Besteht durch eine Zertifizierung noch zusätzlich ein Haftungsausschluß, dann hat die betroffene Firma nur noch sehr geringes Interesse daran, noch weiter in IT-Sicherheit zu investieren.

Firmen, die sich auf einem Markt bewegen, in dem IT-Sicherheit nicht reguliert ist, werden versuchen, durch geeignete Maßnamen ihren Profit zu erhöhen. Das bedeutet im allgemeinen nicht, daß die IT-Infrastruktur bestmöglich geschützt ist, sondern nur, daß die Gesamtsumme aus Schaden und IT-Sicherheitsmaßnamen minimiert wird.

Behörden und andere staatliche Stellen haben ähnliche Interessen wie die Industrie, allerdings wird hier kein Gewinn im traditionellen Sinne erwirtschaftet. Das macht die Abwägungen in Investitionen in die IT-Sicherheit schwieriger. Bei Behörden ist das Handeln möglicherweise noch von politischem Interesse geprägt.

Die Verquickung von Gremien, die für "technische Sicherheit" zuständig sind, erzeugt Beißhemmungen zwischen den Beteiligten, die sowohl der transparenten Darstellung der Probleme als auch Ihrer Lösung abträglich sind. Eine Förderung von unabhängigen Forschungseinreichungen außerhalb der Zuständigkeitsbereich des Bundesinnenministeriums wäre daher hilfreich.