Unterausschuss Neue Medien

Öffentliches Gespräch mit Sachverständigen zum Thema "IT-Sicherheit in der Wirtschaft"

15. Oktober 2012, 13.00 Uhr, P-L-H E 800

Stellungnahme des BITKOM e.V. zu den Fragen der Koalitionsfraktionen CDU/CSU und FDP

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?

- Die Bandbreite an Bedrohungen ist äußerst vielfältig. Schäden können den Unternehmen durch Datendiebstahl und Wirtschaftsspionage, Cybervandalismus (z.B. Löschen oder Ändern von Daten), Erpressung (z.B. Angriff eines Online-Dienstes mit einer sogenannten Denial-of-Service-Attacke) oder Hacktivismus (z.B. die Veröffentlichung von einer großen Zahl von Kundenprofilen) entstehen. Eine Differenzierung nach Branche und Unternehmensgröße ist allerdings kaum darstellbar, weil die entsprechenden Risiken auf alle Unternehmen, aber auch Behörden und staatliche Stellen, zutreffen können. Tendenziell erleben größere Unternehmen - insbesondere aufgrund ihres Bekanntheitsgrades - mehr Angriffe.
- Der größte Nachholbedarf - insbesondere bei kleinen und mittleren Unternehmen - liegt häufig in einer fehlenden, individuellen Sicherheitsstrategie sowie der konsequenten Umsetzung von bereits heute bekannten Standardschutzmaßnahmen. Dazu gehört insbesondere auch die Sensibilisierung der Mitarbeiter hinsichtlich der weitgefächerten Bedrohungslage.
- Mit der zunehmenden Bedeutung von IT in Unternehmen muss eine grundsätzliche Befassung der Unternehmensleitung mit dem Thema sichergestellt sein. Insbesondere auf die folgenden Fragestellungen sollten Antworten gefunden und in einer Sicherheitsstrategie verarbeitet werden: Welche Geschäftsprozesse mit IT-Unterstützung sind für das Unternehmen besonders wichtig? Welche Daten sind besonders wertvoll und vertraulich? Welche IT-Systeme müssen vor unberechtigten Zugriff geschützt werden? Ist das Unternehmen tatsächlich im Fokus von Cyberkriminellen?
- Unternehmen müssen also insgesamt mehr Kompetenz auf verschiedenen Ebenen aufbauen. Weiterhin muss es gelingen, dass mehr Unternehmen bereit sind, Informationen und Erfahrungen zum Thema Cybersicherheit auszutauschen.

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

- In einzelnen Branchen finden bereits informelle, brancheninterne Abstimmungsrunden der Unternehmen statt. Das trifft u.a. auf die ITK-Netzbetreiber zu. Bekannt ist auch das Lage- und Krisenreaktionszentrum der Versicherungswirtschaft (LKRZV).
- Insbesondere Großunternehmen sind mit ihren Computer Emergency Response Teams (CERTs) im Deutschen CERT-Verbund organisiert. Hier findet ein regelmäßiger Austausch insbesondere zu technischen Fragestellungen statt.

- Das BSI steuert im Auftrag des BMI den Umsetzungsplan Kritische IT-Infrastrukturen (UP KRITIS), in dem Unternehmen der KRITIS-Branchen (Banken, Versicherungen, Energie, Telekommunikation, Verkehr ...) sich regelmäßig zu Cybersicherheitsthemen austauschen.
- Das BSI hat im vergangenen Jahr einen Bedrohungskatalog in Abstimmung mit der Wirtschaft, insbesondere auch dem BITKOM, entwickelt und auf der BSI-Webseite veröffentlicht.
- Im Rahmen der Allianz für Cybersicherheit sollen insbesondere Branchen- und regional verankerte Verbände als Multiplikatoren für Inhalte einer zentralen Cybersicherheitsbibliothek der Allianz dienen und mit eigenen Veranstaltungen einen Informations- und Erfahrungsaustausch im eigenen Mitgliederkreis organisieren. Hierzu wird die Allianz auch eng mit der Taskforce „IT-Sicherheit in der Wirtschaft“ des BMWi kooperieren, die verschiedene Multiplikatorenprojekte insbesondere zu kleinen und mittleren Unternehmen unterstützt.
- Voraussichtlich im November wird Nordrhein-Westfalen in seiner „Sicherheitspartnerschaft NRW“ das Thema Cybersicherheit übernehmen und mit entsprechenden Veranstaltungen in IHKs starten. Zur „Sicherheitspartnerschaft NRW“ gehören das Innen- und Wirtschaftsministerium NRW, das LKA, das LfV, die Vereinigung für Sicherheit in der Wirtschaft NW e.V. und die Industrie- und Handelskammern NRW.
- Staat und Wirtschaft engagieren sich seit 2006 auch im Rahmen des Vereins „Deutschland sicher im Netz e.V.“ – auch hier ist die Zielgruppe kleine und mittlere Unternehmen.
- Im Rahmen der allgemeinen Verbandstätigkeit führt der BITKOM regelmäßig Veranstaltungen zum Thema Cybersicherheit im Dialog mit den Anwenderbranchen durch. Diese Aktivitäten sollen bezogen auf die Inhalte der Allianz für Cybersicherheit zukünftig noch intensiviert werden.

2. Unternehmen aus der IKT-Branche haben signifikant höhere Sicherheitsvorkehrungen getroffen als Unternehmen anderer Branchen[1]. 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 der ITK-Branche sind im Hinblick auf die Herausforderungen im Bereich der Cybersicherheit sensibilisierter als viele andere Branchen. Produkte und Dienstleistungen sind insbesondere unter dem Gesichtspunkt Sicherheit unter permanenter Beobachtung der Öffentlichkeit. Für die allgemeine Geschäftstätigkeit und das Vertrauen der Kunden der ITK-Branche hat die Vertraulichkeit, Verfügbarkeit und Integrität von Daten und Systemen eine entscheidende Bedeutung.
- Die wesentlichen Mechanismen zum Schutz vor Cyberbedrohungen sind im Prinzip bekannt. Das gilt auch für die Tatsache, dass mit der konsequenten Umsetzung von Standard-Schutzmaßnahmen rund 80 Prozent der bekannten Risiken mit überschaubarem Aufwand vermieden werden können.
- Die ITK-Branche wird auch weiterhin gerne ihre Erfahrungen im Bereich der Cybersicherheit mit anderen Sektoren teilen. Hierzu werden regelmäßig Leitfäden beim BITKOM veröffentlich und entsprechende Aktivitäten, zum Beispiel über Deutschland sicher im Netz e.V., initiiert. Dies sind auch elementarere Bausteine der Allianz für Cybersicherheit. Ein wesentliches Erfolgskriterium für eine nachhaltige Steigerung des Sicherheitsniveaus in anderen Branchen ist allerdings deren Bereitschaft, die vorhandenen Empfehlungen mit vergleichbarer Konsequenz umzusetzen.

[1] Bitkom (2012): Vertrauen und Sicherheit im Netz

3. Wie häufig sind nach Ihrer Kenntnis deutsche Unternehmen (differenziert nach Branchen) gezielten Cyberattacken ausgesetzt gewesen? Wie sind die bisherigen Rückmeldungen von Unternehmen, die Opfer von Angriffen auf ihre elektronische Infrastruktur geworden sind?

- Auf Basis einer BITKOM-Umfrage unter rund 800 Unternehmen sind bereits 40 Prozent der Unternehmen Opfer von Cyberattacken geworden. (Marktforschungsinstitut ARIS, Umfrage unter 810 Unternehmen per Telefoninterview) Viele davon mehr als einmal. Eine genauere Zahl läßt sich hier aktuell nicht ermitteln, da insbesondere die große Zahl der mittelständischen Unternehmen nach unserer Einschätzung Attacken aber insbesondere auch gelungene Angriffe häufig nicht feststellen können. Hintergrund ist hierfür sowohl fehlende Expertise der Mitarbeiter aber auch der fehlende Einsatz einschlägiger Sicherheits- und Kontrollsysteme.

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

- Hierzu gibt leider es keine umfassende Datenbasis. Das Bundeskriminalamt geht insbesondere im Hinblick auf geschädigte Unternehmen von einem hohen Dunkelfeld aus. Insofern hat das BKA in der gemeinsam mit dem BITKOM durchgeführten Pressekonferenz Angang September 2012 eingeräumt, dass die Zahlen der polizeilichen Kriminalstatistik in dieser Hinsicht nur eine eingeschränkte Aussagekraft besitzen können.

  Das BKA listet in seiner Broschüre „Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime“ (2012)[2] wesentliche Beweggründe auf (siehe Seite Seite 5):

  - Es handelt sich oftmals um Innentäter, so dass eine firmeninterne Regulierung bevorzugt wird.
  - Die Angriffe werden abgewehrt bzw. bleiben erfolglos.
  - Häufig sind zunächst keine Schäden erkenn oder messbar.
  - Fehlende Sensibilisierung/Awareness bei den Verantwortlichen auf Leitungsebene
  - Keine Anzeigen aus Sorge vor Imageschäden durch befürchtete Presseveröffentlichungen.
  - Befürchtete negative Auswirkungen unter Konkurrenz-/Wettbewerbsaspekten.
  - Die Strafverfolgung dauert aus Sicht der Unternehmen zu lange bzw. es wird die Erfolglosigkeit der polizeilichen Ermittlungen angenommen.
  - Insbesondere kleinere Firmen befürchten, dass die Polizei Firmenrechner sicherstellt und diese erst nach einem längeren Zeitraum wieder aushändigt.
  - Teilweise verfügen Unternehmen nicht über lizenzierte Software, so dass die Angst vor einem Strafverfahren gegen die Firma überwiegt. Gleiches gilt bei einem bekannten oder angenommenen Vorhandensein illegaler Dateien auf den Computern oder Profilen einzelner Beschäftigter der Firma.

2 http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/HandlungsempfehlungenWirtschaft/handlungsempfehlungen__node.html?__nnn=true

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?

- Meldungen sind grundsätzlich wichtig, um valide Daten über die tatsächliche Bedrohung zu erhalten. Die Zielsetzung ist ein umfassendes und aktuelles Lagebild und die Möglichkeit zur frühen Warnung vor Bedrohungen, z.B. im Rahmen der Allianz für Cybersicherheit. Ein regelmäßiger Überblick über die aktuelle Lage kann auf der einen Seite ein wesentliches Instrument sein, um die knappen finanziellen und personellen Ressourcen von Staat und Wirtschaft richtig zu allokieren. Gleichzeitig kann eine, auf einer breiten Datenbasis aufbauende Statistik zur Sensibilisierung von Unternehmen dienen, die bislang noch zu wenig für ihre IT-Sicherheit tun.
- Der gesetzliche Zwang zur Meldung unterstützt aber nicht zwangsläufig die Zielsetzung einer Änderung der Sicherheitskultur und damit Übernahme von Eigenverantwortung in den Unternehmen. Vielmehr könnte die Erwartungshaltung der Unternehmen gestärkt werden, dass die IT-Sicherheit primär durch den Staat gewährleistet wird.
- Damit eine Vielzahl entsprechender Meldungen überhaupt erzeugt werden können, muss in vielen Unternehmen zunächst eine entsprechende Kompetenz aufgebaut werden und auch organisatorische Maßnahmen erfolgen. In vielen – gerade mittelständischen - Unternehmen ist die Rolle eines IT-Sicherheitsbeauftragten (analog zum Datenschutzbeauftragten) in der Organisation nicht beschrieben oder nicht besetzt. Das Know-how einen Sicherheitsvorfall in den eigenen Systemen zu bemerken und danach unter Sicherung der notwendigen Beweise ordentlich zu dokumentieren ist vielfach noch nicht vorhanden.
- Positive Aspekte einer gesetzlichen Meldepflicht sind die zu erwartende quantitative Zunahme an Meldungen und die Tatsache, dass sich Unternehmen grundsätzlich mit dem Thema Cybersicherheit beschäftigen und Mitarbeiter mit dem Thema/mit der Aufgabe betrauen
- Durch eine gesetzliche Meldepflicht entstehen aber voraussichtlich auch erhebliche Bürokratiekosten, da Unternehmen zunächst umfassend informiert, aber im Sinne der Durchsetzung auch kontrolliert werden müssten.
- Unternehmen melden das, was dem Gesetz nach gemeldet werden muss. Dabei werden wichtige Zusatzinformationen möglicherweise nicht berücksichtigt. Somit besteht die Gefahr, dass die inhaltliche Qualität der Meldung stark eingeschränkt ist.
- Meldungen der Unternehmen dürfen nicht bei den Sicherheitsbehörden versickern, sondern müssen als analysierte und bewertete Informationen - zum Beispiel in Form des Lagebildes oder einzelner Warnmeldungen - wieder an die Wirtschaft zurückgegeben werden. Der Mehrwert der Informationsweitergabe eines Vorfalls (Meldung) muss für die Unternehmen sichtbar werden.

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?

- Der Markt für IT-Sicherheitsprodukte (Hard- und Software) sowie IT-Sicherheitsdienstleistungen lag 2010 in Deutschland bei rund 2,5 – 3 Mrd. € (Quelle: Studie „IT-Sicherheitsmarkt in Deutschland“ von Booz und Co. im Auftrag des BMWi). Der größte Teil hiervon wird durch Unternehmen getragen. Marktforscher gehen von Wachstumsraten p.a. > 10 Prozent aus.
- Nicht eingerechnet sind die Aufwände für Sicherheitsorganisationen und Personalkosten in Unternehmen Tendenziell wird der Bedarf an IT-Sicherheitsexperten und werden die Ausgaben der Unternehmen für Produkte, Dienstleistungen und Personalaufwände überdurchschnittlich steigen.

Stellungnahme des BITKOM e.V. zu den Fragen der Fraktionen der SPD, von Bündnis 90/Die Grünen und Die Linke.

4. 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?

- Das Interesse sich an einer zentralen und übergreifenden Initiative zur Verbesserung der Cybersicherheit in Deutschland zu beteiligen ist von allen potenziellen Akteuren (Anwenderbranchen, ITK-Branche, staatlichen Stellen, Wissenschaft) gleichermaßen hoch.
- Die Allianz hat neben der neben der Meldung von Vorfällen und die Verarbeitung in ein Lagebild auch zum Ziel einen kontinuierlichen Informations- und Erfahrungsaustausch zu initiieren und die Kompetenz in Unternehmen, staatlichen Stellen und sonstigen Organisationen zu stärken.
- Bislang wurde die Allianz noch nicht offiziell über die zur Verfügung stehenden Kanäle beworben, sondern ist bislang eher in Fachkreisen bekannt. Insbesondere aus dem Kreis der ITK-Branche haben sich bereits viele Unternehmen (>20) mit Vorschlägen zu aktiven Beiträgen als Partner der Allianz beworben. Diese Partnerbeiträge werden dazu dienen, die Cybersicherheit in Deutschland in verschiedenen Themenfeldern mitzugestalten. Mit dem offiziellen Start soll intensiv mit der Bewerbung über Multiplikatoren (z.B. Branchenverbände, regionale Sicherheitsverbände, etc.) begonnen werden.

Wie viel Zeit sollte einer solchen Selbstverpflichtungsinitiative eingeräumt werden?

- Die Allianz für Cybersicherheit ist keine Selbstverpflichtungsinitiative. Es gibt also keinen festen Katalog an Anforderungen, zu denen sich Unternehmen und Behörden verpflichten sollen.
- Die Allianz für Cybersicherheit sollte prinzipiell auf unbestimmte Zeit angelegt sein - eine Evaluierungsphase ist allerdings nach einem Zeitraum von ein bis zwei Jahren sinnvoll. Das BSI, die Wirtschaft, Behörden und sonstige Organisationen werden sich ohnehin dauerhaft mit dem Thema Cybersicherheit beschäftigen müssen. Die Allianz hat die Zielsetzung, die dringend notwendige Zusammenarbeit und den Informations- und Erfahrungsaustausch in bereits heute bekannten Themengebieten zu intensivieren und von Anfang an einen sinnvollen Rahmen zu geben. BSI und der BITKOM sind derzeit die prädestinierten Organisationen eine Kooperation von Staat und Wirtschaft im Thema Cybersicherheit in Deutschland aufzubauen. Wie auch bei anderen Initiativen im Sicherheitsumfeld ist die Entwicklung von Vertrauen für den Erfolg essentiell. Vertrauen kann sich allerdings nicht sofort einstellen, sondern muss sich über die Zusammenarbeit der jeweiligen Partner entwickeln.

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?

- Vergleiche die Antwort zur Frage 3 der Koalition
- Die Verpflichtungen zur Meldung von Vorkommnissen hinsichtlich BDSG beruhen auf einem sehr klar eingegrenzten Bereich (es gibt betroffene Dritte bzw. drohende Beeinträchtigungen von Dritten, es geht um personenbezogene Daten). Bei Cybersicherheitsvorfällen kann die Vorfallslage wesentlich vielschichtiger sein. Nicht jeder Vorfall hat einen Geschädigten oder wesentliche Auswirkungen auf das Unternehmen. Die betroffenen Daten können auch vergleichsweise wenig brisant sein. Insofern sollte es einen Ermessensspielraum für das betroffene Unternehmen geben, den Vorfall zu melden oder nicht. Die Vorgaben des BDSG sind selbstverständlich nachwievor zu berücksichtigen.

5. Auf welcher konkreten Informationsgrundlage arbeitet das Cyberabwehrzentrum derzeit im Hinblick auf IT-Angriffe und wie ist diese vor dem Hintergrund der Forderungen nach einer allgemeinen Meldepflicht für die Privatwirtschaft zu bewerten? 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?

- Das Cyberabwehrzentrum ist aktuell als Informationsdrehscheibe von staatlichen Stellen (wie dem BSI, BKA, BfV, BBK, der Bundeswehr) ausgelegt. Der BITKOM und der BDI haben bereits bei Veröffentlichung der Cybersicherheitsstrategie im Februar 2011 darauf gedrungen, eine Andockstelle für die Wirtschaft zu schaffen. Dies ist bislang noch nicht erfolgt. Insofern ist nicht bekannt, welche Erkenntnisse über IT-Sicherheitsvorfälle in der Wirtschaft im Cyberabwehrzentrum vorliegen (über diejenigen hinaus, die ohnehin in den Medien bekanntgewordenen sind).
- Wesentliche Voraussetzung für ein qualifiziertes Lagebild ist eine vereinheitlichte Meldesystematik (z.B. zu welchen Bedrohungstypen und ab welchem Schweregrad soll eine Meldung vorgenommen werden) und ausreichende personelle und technische Ressourcen für die Analyse und Aufbereitung der Lageinformationen. Diese beiden Voraussetzungen lassen sich nach unserer Auffassung realisieren.

6. 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?

   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?

- Im Rahmen der Allianz für Cybersicherheit ist die beratende Rolle des BSI insbesondere für präventive Maßnahmen zu betonen. Mögliche Interessenkonflikte lassen sich hier nicht erkennen.

- Das BSI ist seit Jahren ein wichtiger und geschätzter Partner sowohl der Behörden als auch der Unternehmen. Die Relevanz der Inhalte von Sicherheitsempfehlungen hängen ohne nicht davon ab, ob eine Organisation zum privaten oder staatlichen Sektor gehört, sondern welchen Schutzbedarf die jeweiligen Prozesse und Daten haben. Viele Konzepte und Inhalte, die vom BSI für die öffentliche Verwaltung erstellt wurden, lassen sich mit geringen Anpassungen auch im privatwirtschaftlichen Kontext verwenden.