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

Antworten des Bundesamtes für die Sicherheit der Informationstechnik, BSI, auf die 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?**

Bedrohungspotenziale für die deutschen Unternehmen ergeben sich aus vielfältigen Cyber-Bedrohungen und sind nicht zwangsweise an Branchenzugehörigkeiten und Unternehmensgrößen gekoppelt.

So können prinzipiell alle Unternehmen von Cyberspionage betroffen sein, neben Großunternehmen betrifft dies insbesondere auch die vielen mittelständischen Unternehmen (insbesondere die sog. „hidden champions"), deren geistiges Eigentum ein attraktives Ziel für Spionage darstellt. Auch die Erpressung mit DDoS-Angriffen oder der Diebstahl und Rückkauf von Kundendaten kann prinzipiell jedes Unternehmen treffen.

Im Bereich der Kritischen Infrastrukturen ergeben sich vor allem Bedrohungen durch Cybersabotage, z.B. durch die Manipulation von Steuerungssystemen, die zu schwerwiegenden Beeinträchtigungen für die Versorgung und Sicherheit der Bevölkerung führen könnten. Auch hier ist eine Unterscheidung anhand der Größe der potenziell betroffenen KRITIS-Unternehmen bzgl. des Bedrohungspotenzials nicht immer zielführend, da hiervon eher die darauffolgende Auswirkung eines Ausfalls abhängig sein wird.

Eine Verbesserung des allgemeinen Sicherheitsniveaus in der Wirtschaft wird grundsätzlich von einer möglichst flächendeckenden Umsetzung grundlegender Sicherheitsmaßnahmen – vor allem im Bereich der KMU - abhängen. Kann hier entsprechend des Pareto-Prinzips (80% der maximal möglichen Wirkung kann bereits unter Aufbringung von nur 20% des maximal möglichen Aufwands erzielt werden) ein ausreichender Basisschutz etabliert werden, so werden die Folgen von Ausfällen spürbar gemildert und die Betätigungsmöglichkeiten für Angreifer bereits stark eingeschränkt.

Während einige - vor allem stark von IT-durchsetzte – Branchen dieses Kriterium bereits häufig erfüllen, so ergibt sich hier für andere Branchen durchaus noch großer Handlungsbedarf. Dies trifft insbesondere auf solche Branchen zu, deren Geschäftsprozesse traditionell nicht stark von IT abhängig waren, aber heute zunehmend abhängiger werden. Auch hier ergeben sich in der Regel Unterschiede in der Umsetzung zwischen großen, mittleren und kleinen Unternehmen hinsichtlich der vorhandenen Möglichkeiten zur Implementierung solcher Maßnahmen.

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

Deutschland hat mit dem „Deutschen CERT-Verbund“ eine national gut vernetzte CERT-Community. Auch international in Europa mit RegierungsCERTs und global ist das BSI gut vernetzt, sodass der Informationsaustausch hierzu funktioniert. Zurzeit wird mit den Bundesländern auf Initiative des IT-Planungsrats ein Verbund der LänderCERTs mit dem Bund, der sog. VerwaltungsCERT-Verbund aufgebaut. Damit können die Länder ihre landesinterne Rolle zum Austausch wahrnehmen und sind darüber hinaus untereinander und mit den Bundesteams (CERT-Bund, Bundeswehr, Bundespolizei) vernetzt.

Darüber hinaus steht das BSI mit den großen Software-Herstellern und Antivirensoftwareherstellern im intensiven Dialog. Informationen zu Schwachstellen und Angriffen, die das BSI auf diesen und anderen Wegen erreichen, werden über die Initiativen des UP KRITIS, der Allianz für Cyber-Sicherheit und des Bürger-CERT den in den jeweiligen Initiativen organisierten Unternehmen oder auch der Öffentlichkeit in Form von Warnmeldungen zur Verfügung gestellt. Ziel ist ein gegenseitiger Informationsaustausch, um die Informationsbasis auf beiden Seiten zu verbessern. Über die Allianz für Cyber-Sicherheit steht der Zugang zu Warnmeldungen des BSI grundsätzlich allen deutschen Unternehmen offen. Unternehmen, die den Kritischen Infrastrukturen angehören oder die als Institutionen im besonderen staatlichen Interesse anzusehen sind, erhalten über den UP KRITIS bzw. die Allianz für Cyber-Sicherheit ein passendes Informationsangebot.

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?

Es trifft nicht pauschal zu, dass Unternehmen aus der IKT-Branche (z.B. Internet-Provider, Telekommunikationsdienstanbieter) über bessere Vorkehrungen zur Absicherung von Systemen und Daten verfügen als Unternehmen anderer Branchen. So werden z.B. im Bereich der Banken, nicht zuletzt durch umfassende regulatorische Vorgaben, branchenweit sehr hohe Standards zur Absicherung umgesetzt. Vielmehr handelt es sich hier um einen – ebenfalls nicht generell auf alle Unternehmen anwendbaren – Effekt, der durch mehrere Faktoren zustande kommt. Einerseits steigt mit dem generellen Grad der IT-Abhängigkeit der Geschäftsprozesse in der jeweiligen Branche das unternehmenseigene Know-how bzgl. des IT-Einsatzes und entsprechender Sicherheitsmaßnahmen. Andererseits ist bei abnehmender Unternehmensgröße auch oft eine Einschränkung der Möglichkeiten zur personellen wie auch zur finanziellen Umsetzung solcher Maßnahmen verbunden.

Insbesondere kleineren und mittleren Unternehmen (KMU), die nicht aus der IKT-Branche stammen, sondern höchstens IKT-Technik als Anwender einsetzen, fehlt häufig das Verständnis für die zugrunde liegende komplexe Technik. Ein solches Verständnis ist jedoch Voraussetzung, um die mit dieser Technik einhergehenden Gefährdungen überhaupt einschätzen zu können. Nur wer sich eingehend mit der IKT-Technik beschäftigt, lernt Gefährdungen und Gegenmaßnahmen zu begreifen. Unternehmen, die selbst in der IKT-Branche tätig sind, bringen entsprechendes Know-how bereits mit und haben somit eine bessere Voraussetzung, das Potential von Cyber-Angriffen zu erkennen und erforderliche Gegenmaßnahmen zu ergreifen.

Viele Privatanwender sind aus entsprechenden Gründen ebenfalls überfordert, Gefährdungen zu erkennen und Gegenmaßnahmen richtig umzusetzen. Aus diesem Grunde hat das BSI den eco-Verband bei der Gründung des die Antibotnetz-Beratungszentrum unterstützt. Hierbei informieren Internet Service Provider ihre Kunden über infizierte Rechner. Des Weiteren gibt es mit botfrei.de eine Webplattform, die Betroffenen umfangreiche Hilfestellung zur Verfügung stellt. Auch KMU können von demselben Angebot profitieren. Insgesamt müssen die Bürger besser über die Gefährdungen und Gegenmaßnahmen aufgeklärt werden. Bereits an den Schulen sollten die Themen Sicherheit und Datenschutz fest im Lehrplan verankert werden. Des Weiteren sollten Hilfsangebote wie botfrei.de ausgeweitet werden. Auch die

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

Verbände, die Industrie und Handelskammern, etc. sollten unterstützen, ihre Mitglieder bzgl. Sicherheit zu sensibilisieren, und Aufklärungsangebote bereitstellen. Das Problem der Cyber-Angriffe kann nur gelöst werden, wenn sich alle Institutionen der Gesellschaft einbringen und jeder tut, was er tun kann.

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?**

Repräsentative Zahlen zu gezielten Cyber-Angriffen auf deutsche Unternehmen liegen dem BSI nicht vor. Es ist davon auszugehen, dass sich international agierende Unternehmen regelmäßigen Angriffen ausgesetzt sehen. Dies wird durch verschiedene Studien bestätigt (z.B. Symantec Intelligence Report, Juni 2012).

Unternehmen äußern sich sehr selten Dritten gegenüber, dass sie Opfer von Angriffen geworden sind. Sie fürchten um ihre Reputation und damit drohende finanzielle Verluste. Informationen zu erfolgreichen Angriffen erhält das BSI bislang nur durch längere Vertrauensbeziehungen oder verbunden mit der Bitte um Hilfe oder Unterstützung.

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

Die Unternehmen entscheiden selbst, ob sie Anzeige erstatten. (Dies muss bei der lokalen Polizeidienststelle erfolgen, da das BKA nur in Ausnahmefällen zuständig ist. Die Erfolgsaussichten der Strafverfolgung sind i.d.R. gering.) Nach unserer Erfahrung verzichten die meisten Unternehmen auf eine Anzeige, da mit den folgenden Ermittlungen bzw. Strafverfahren der Angriff öffentlich würde und damit die Reputation geschädigt werden könnte und finanzielle Verluste nicht ausgeschlossen wären.

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 zentrale Registrierung sowie der schnelle Informationsaustausch von schwerwiegenden IT-Attacken auf wichtige Infrastrukturen (z. B. die von Betreibern Kritischer Infrastrukturen) ist unerlässlich, um ein belastbares Lagebild der Cyber-Sicherheit für Deutschland erstellen zu können. Nur anhand eines vollständigen und aktuellen Lagebildes ist es möglich,

vorhandene Zusammenhänge zwischen IT-Attacken auf verschiedene Infrastrukturen aufzudecken und die richtigen Bewertungen, Handlungsoptionen und ggf. Abwehrmaßnahmen abzuleiten. Auch können nur dann die staatlichen Sicherheitsbehörden ihrem gesetzlichen Auftrag hinsichtlich der Sicherstellung der öffentlichen und staatlichen Sicherheit vollumfänglich nachkommen, wenn Informationen über schadensauslösende oder gefährdende IT-Angriffe vorliegen. Im Zusammenhang mit einer zentralen Registrierung sind allerdings zahlreiche Fragen und Rahmenbedingungen in einem komplexen Umfeld zu klären (u.a. Art und Umfang der Registrierung, Schwellwerte, Bearbeitungsprozesse, etc.). Erfahrungen mit zentraler Registrierung können im Rahmen der Allianz für Cyber-Sicherheit gesammelt werden, bei der auf Freiwilligkeit beruhende direkte und indirekte Registrierungsverfahren zwischen dem BSI und teilnehmenden Unternehmen erprobt 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?

Repräsentative Zahlen zu den Aufwendungen deutscher Unternehmen für Maßnahmen zur Absicherung liegen dem BSI nicht vor. Für die Zukunft ist prinzipiell durch ein zunehmendes Problembewusstsein und einer damit verbundenen großflächigeren Umsetzung derartiger Maßnahmen mit insgesamt steigenden Aufwendungen zu rechnen. Für die einzelnen Unternehmen wird der Aufwand aber auch von den bisher bereits umgesetzten Maßnahmen abhängen.

Antworten des Bundesamtes für die Sicherheit der Informationstechnik, BSI, auf die 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?

Die Kooperationsplattform befindet sich derzeit im Pilotbetrieb und ist daher – bis auf weiteres - nur für registrierte Teilnehmer der Allianz für Cyber-Sicherheit erreichbar. Aufgrund des während der Pilotphase geringen Mitteleinsatzes zur öffentlichkeitswirksamen Werbung für die in die Plattform integrierte Meldestelle hat diese bislang nur sehr geringe Resonanz erfahren.

Parallel gibt es Ansätze, durch die Einbeziehung der Wirtschaft im Rahmen des Programms für Partner der Allianz für Cyber-Sicherheit eine nicht durch das BSI betriebene Meldeplattform anzubieten, die den Kontakt zum BSI nur optional herstellt. Durch eine zweite Möglichkeit zur Meldung von Sicherheitsvorfällen ohne direkte staatliche Beteiligung sollen somit eventuell vorhandene Hemmschwellen abgebaut werden.

Wie viel Zeit sollte einer solchen Selbstverpflichtungsinitiative eingeräumt werden?

Derartige Kooperationsformen basieren auf Vertrauen und Erfahrung. Dies bedarf Zeit, um zu wachsen. Daher sollte mindestens ein Jahr nach dem offiziellen Start, sprich nach Ende der Pilotphase, abgewartet werden, um Vertrauen aufzubauen und Erfahrung zu sammeln. Hinzu kommt, dass die Zielgruppe entsprechend wachsen muss.

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?

Die Allianz ist ein Baustein, um die nationale IT-Lagebewertung im BSI zu verbessern. Gemeinsam mit anderen, bestehenden Mechanismen wie den Meldewegen aus dem Umsetzungsplan KRITIS muss das BSI in die Lage versetzt werden, das nationale IT-Lagebild kontinuierlich fortzuschreiben und Handlungsempfehlungen abzuleiten. Aktuell reichen die

Informationen – insbesondere aus der Wirtschaft – dafür noch nicht aus. Es bleibt jetzt zu evaluieren, inwiefern die Aktivitäten zur Optimierung, zum Beispiel im Rahmen der Spitzengespräche von Herr Minister Dr. Friedrich mit Vertretern der Deutschen KRITIS-Wirtschaft oder auch die Cyber-Allianz, die Industriepartner ausreichend motivieren, einen engen Austausch mit dem BSI zu pflegen. Des Weiteren gibt es bislang keine dezentrale/zentrale Struktur wie die des Datenschutzbeauftragten im IT-Umfeld mit den entsprechenden Rechten.

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?

Angriffsmechanismen orientieren sich nicht an der Aufgabenteilung bzw. an den Zuständigkeiten von Behörden. Daher ist der Informationsaustausch im Rahmen des Cyber-Abwehrzentrums Grundlage für eine fundierte Lageeinschätzung. Neben der eigenen Analyse öffentlicher Quellen bezieht das Cyber-Abwehrzentrum seine Informationen aus dem täglichen Lagebericht des BSI-Lagezentrums/CERT-Bund sowie aus Zulieferungen der übrigen angeschlossenen Behörden. IT-Vorfälle werden – entsprechend einer Vorfilterfunktion – zunächst in dem BSI-Lagezentrum/CERT-Bund auf technischer Ebene bearbeitet und zur strategischen Beurteilung an das Cyber-Abwehrzentrum übermittelt. Generell gilt, dass die Kenntnisse über Angriffe, Akteure und deren Motive umso umfassender sind, desto vollständiger das Lagebild ist.

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 BSI fügt in seinen Analysen das nationale Lagebild aus einem Mosaik von Lagebeiträgen zu einem Gesamtbild zusammen. Je mehr Beiträge und „Steinchen“ von den unterschiedlichen Quellen geliefert werden, um so klarer wird das Bild und es hat weniger „weiße Flecken“. Das BSI greift dabei auf seine Fachkompetenz und Erfahrung zurück.

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?

Das BSI wirkt gemäß seines gesetzlichen Auftrages als zivile und präventive Sicherheitsbehörde. Ein Konflikt ist aus Sicht des BSI nicht erkennbar. Im Gegenteil profitieren beide Seiten voneinander, da die Gefährdungen ähnlich und damit die Maßnahmen vergleichbar sind. Zudem kann das BSI aus den Informationen über IT-Vorfälle präventive Maßnahmen ableiten.