STELLUNGNAHME

Berlin, 10. Oktober 2012

Deutscher Industrie- und Handelskammertag

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

15. Oktober 2012

Wir bedanken uns für die Möglichkeit, zu den Fragen der Fraktionen zum Thema „IT-Sicherheit in der Wirtschaft“ Stellung zu nehmen. Computeranlagen und Web-Seiten von Firmen werden zunehmend zum Angriffsziel national und international agierender Täter bzw. Tätergruppen. Internetpräsenzen, aber auch DV-Anlagen von Unternehmen können manipuliert und wichtige Kundendaten, Betriebsgeheimnisse, Inhalte der Finanzbuchhaltung oder Softwareprodukte verändert, gelöscht oder gestohlen werden. Die dadurch verursachten Schäden können sogar die Existenz der betroffenen Unternehmen bedrohen. Die Industrie- und Handelskammern (IHKs) haben zur angesprochenen Thematik Umfragen bei Unternehmen durchgeführt und auf Basis der Ergebnisse zahlreiche Aktivitäten entwickelt. Der Deutsche Industrie- und Handelskammertag (DIHK) und die IHKs engagieren sich in erster Linie für mehr Bewusstseinsbildung insbesondere bei kleinen und mittleren Unternehmen (KMU) und vermitteln praktikables Handwerkszeug zur Umsetzung von IT-Sicherheitsmaßnahmen in den Unternehmen.

Wir beantworten die Fragen auf Basis der Erfahrungen von Unternehmen aller Größenklassen, fokussieren uns mit unseren Antworten jedoch insbesondere KMU.

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? Welche Maßnahmen wurden bisher ergriffen bzw. sind in Planung, um einen

Informationsaustausch über Bedrohungslagen und mögliche Schwachstellen, Angriffe und Angreifer zu ermöglichen?

Eine Einteilung nach Branchen und/oder Unternehmensgröße erscheint uns wenig geeignet, um Aussagen zu Bedrohungspotenzialen zu treffen. Eher relevant erscheint uns in diesem Zusammenhang die Kategorie der genutzten Daten. Die Nutzung sicherheitsrelevanter Daten in Unternehmen kann beispielsweise in der Be- oder Verarbeitung personenbezogener Daten bestehen, bestimmte Leistungsmerkmale eines Unternehmens spielen eine Rolle (z. B. hoher Innovationsgrad, einzigartige Marktposition etc.) oder so genannte kritische Infrastrukturen. In den genannten und weiteren Bereichen gibt es einen gewissen Teil hochsicherheitsbedürftiger Daten, die per se durch ihre Existenz Ziel von Attacken sind. Ansonsten sehen kleinere Produktions- oder Dienstleistungsbetriebe die Datenlogistik als Spiegel bzw. Teil der Liefer- und Leistungskette an und behandeln diese – berechtigterweise – genauso wie die Besicherung des tangiblen Teils der Produktion: mit Sorgfalt, aber ohne Overhead.

Unserer Erfahrung nach mangelt es vor allem in KMU – und hier insbesondere bei denen, die weniger „IT-affin“ sind – an grundlegenden Sicherheitsmaßnahmen. Dabei liegt das größte Problem weniger in der technisch verfügbaren Infrastruktur, sondern vielmehr im fehlenden Bewusstsein – sowohl auf Managementebene als auch bei den Mitarbeitern. Dies hat zur Folge, dass in den Unternehmen häufig weder ein ausreichendes Budget noch Expertise vorhanden sind. Viele Unternehmen leisten sich keine Kompetenz für sicherheitsrelevante Themen. Auch ist häufig der organisatorische Umgang mit IT-Sicherheitsfragen nicht geregelt. Inhaltliche und organisatorische Fragen werden oftmals vom Inhaber/Geschäftsführer, bzw. einem Beauftragten, (nebenbei) mit erledigt, der jedoch in aller Regel kein ausgebildeter IT-Fachmann ist. Solange kein IT-Angriff erfolgt ist, bzw. bemerkt wurde, steht das Thema IT-Sicherheit weiter unten in der Prioritätenliste – das Tagesgeschäft geht vor.

Die IHKs bieten regelmäßig Veranstaltungen – vor allem für kleinere Unternehmen – an, beraten und betreiben Netzwerke, um zu sensibilisieren, Austausch zu ermöglichen und Informationen zu vermitteln. Dafür sind die Informationen des BSI z. B. im Grundschutzhandbuch oder in Technischen Richtlinien eine gute und umfassende Grundlage. Für deren Studium und für die Umsetzung der Maßnahmen werden jedoch spezielle Kenntnisse benötigt, die in vielen kleineren

Unternehmen nicht vorhanden sind. In diesen scheint "IT-Sicherheit mit Augenmaß", also eine Risikoreduzierung mit überschaubaren Maßnahmen, eher ein nutzbringender Ansatz zu sein. Dazu zählen z. B. organisatorische Maßnahmen wie eine Benutzerordnung für die betriebsinterne IT oder Informationen darüber, was von einem guten IT-Dienstleister technisch erwartet werden kann.

Eine Vernetzung von IT-Sicherheitsexperten, die in größeren Unternehmen für die Erkennung und Abwehr von Cyber-Bedrohungen und Angriffen zuständig sind (i. d. R. Cyber Emergency Response Teams - CERTs), findet auf nationaler Ebene beispielsweise über den CERT-Verbund und auf internationaler Ebene über die FIRST – Forum of Incident Response Teams statt. Mittels dieser langjährig etablierten Informationsplattformen haben Unternehmen branchenübergreifend die Möglichkeit, sich pro-aktiv über Bedrohungen und Sicherheitsmaßnahmen zu informieren und sich bei Sicherheitsvorfällen gegenseitig zu unterstützen.

Die Bedrohungslage wird sich weiter verschärfen – gerade vor dem Hintergrund der vermehrten Nutzung mobiler Endgeräte und einer stärkeren Verknüpfung sämtlicher Arbeitsprozesse mit IKT auch in KMU. Unternehmen müssen auch auf den Trend „Bring Your Own Device“ mit veränderten Sicherheitsmaßnahmen reagieren. Auch hier liegt der Schwerpunkt im Umgang mit vertraulicher Information durch den jeweiligen Benutzer. Eine zunehmend wichtige Rolle spielt zudem das Angebot von Cloud-Diensten und die Auslagerung von IT-Prozessen. Mitarbeiter können damit immer einfacher die gesuchten Funktionalitäten realisieren. Dadurch nimmt die Gefahr zu, dass (Cloud-)Applikationen innerhalb der Unternehmen ohne vorherige Risikoanalyse eingerichtet 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 müssen sich naturgemäß schon seit vielen Jahren mit möglichen Formen von Angriffen auf deren Systeme und Infrastrukturen auseinandersetzen. Die Entscheider befassen sich im Tagesgeschäft stärker mit den Themen IT-Sicherheit und Datenschutz, weil deren Nichtbeachtung schnell zu einem existenzbedrohenden Risiko werden kann. Allerdings haben die bisherigen Aktivitäten der Branche selbst (Vielzahl an Papieren, Veranstaltungen etc.) kaum eine bessere Sensibilisierung von KMU vermocht.

Im Zuge der zunehmenden „Digitalisierung" ganzer Wertschöpfungsprozesse anderer Wirtschaftsbereiche gewinnen die Fragen der IT-Sicherheit auch für diese an Bedeutung. Ein wesentlich grundsätzlicher und direkterer Ansatz, Sicherheit auf andere Branchen zu übertragen, wäre, die Infrastrukturen und Dienste insgesamt sicherer zu machen. Denn IT-Sicherheit fängt nicht beim Endanwender an, sondern bereits bei der Produktion von Hard- und Software. Hier steht der jeweilige Hersteller, die IT-Industrie, in der Pflicht, Schwachstellen-Meldungen in IT-Systemen und entsprechende Sicherheitsmaßnahmen (z. B. der Bereitstellung von Sicherheits-Software-Updates) zeitnah über einen dezidierten Informationsdienst zu liefern. Zudem kommt es vor, dass IT-Systeme unzureichend im Hinblick auf Sicherheitsanforderungen getestet wurden und nach Auslieferung Schwachstellen aufweisen, die nur durch einen Austausch der Systeme durch den Hersteller behoben werden können. In beiden Fällen müssen Unternehmen heute über Einzelverträge mit Herstellern sicherstellen, dass diese die genannten Pflichten erfüllen. Der Aufwand für Unternehmen, entsprechende Vertragsabkommen aufzusetzen, kann – je nach Umfang und Vielfältigkeit der eingesetzten IT-Landschaft – erheblich variieren.

Unternehmen können ihr Sicherheitsniveau auch durch die Anwendungen von Cloud-Applikationen erhöhen. Dies klingt in erster Linie vielleicht paradox, denn wer an „Cloud" denkt, denkt gleichzeitig auch an ein höheres Risikopotenzial. Dies muss für kleinere oder mittelgroße Firmen nicht

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

unbedingt gelten, da Cloud-Anbieter in der Regel technische Sicherheitsmaßnahmen realisiert haben, die bei KMU oft nicht zu finden sind (z. B. 24x7 Security Operations Center).

Sinnvoll sind auch Aktivitäten im Bereich „Unternehmer lernen von Unternehmen". Hier gibt es zahlreiche Initiativen von Kammern und Verbänden sowie Erfahrungen aus dem BMWi/NEG-Begleitprojekt „Sichere eGeschäftsprozesse in KMU und Handwerk".

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

Es gibt unseres Wissens zur Zeit keine deutschlandweit eindeutigen Zahlen zur Häufigkeit von gezielten Cyber-Attacken und den damit verbundenen Kosten für Unternehmen. Umfragen dazu gestalten sich schwierig, zumal gerade KMU häufig nicht einmal wissen, ob sie überhaupt angegriffen wurden. Und selbst wenn Angriffe als solche erkannt wurden, können sie häufig nicht sinnvoll kategorisiert werden. Wissenschaftliche, durch die Bundesregierung oder die EU geförderte Forschung könnte hier eventuell zur Aufklärung beitragen.

Aktuelle Umfragen, z. B. unter Hamburger Unternehmern, haben ergeben, dass im vergangenen Jahr jedes dritte Unternehmen Angriffe auf seine IT-Infrastruktur oder aus dem Internet verzeichnet hat. Die Bedrohung für IT-Sicherheit und Datenschutz wird von den Unternehmen demzufolge auch

als mit Abstand größte Gefahr für den Unternehmenserfolg eingeschätzt: 75 Prozent der Unternehmen sehen hier die größten Risiken, fast ebenso viele Betriebe rechnen jedoch auch mit einer steigenden Bedrohung durch die allgemeine Wirtschaftskriminalität.

Angriffe auf die IT-Infrastrukur werden von den Unternehmen jedoch nur selten zur Anzeige gebracht. So haben Umfragen gezeigt, dass fast alle Einbruchdiebstähle angezeigt werden – aber weniger als 10 Prozent der Fälle im Bereich der IT- und Internetkriminalität. Von einer Anzeige wird nach Unternehmensangaben häufig auch deshalb abgesehen, weil (angeblich) kein Schaden entstanden ist. Bei den sonstigen Gründen, warum es zu keiner Anzeige kam, zeigte sich, dass bislang überwiegend von der Erfolglosigkeit einer polizeilichen Verfolgung ausgegangen wird. Unternehmen müssten gezielter über die Fachkompetenz der Polizei informiert werden.

Verständlicherweise sind Unternehmen sehr zurückhaltend mit der Veröffentlichung von gezielten und erfolgreichen Angriffen. Durch die systematische Aufbereitung erfolgreicher Angriffe befürchten Unternehmen Reputationsverlust und Imageschäden sowie neue Risiken durch etwaige Streuung der "Anleitung für einen erfolgreichen Angriff". Offensichtlich besteht hier eine Vertrauenslücke zwischen Wirtschaft und staatlichen Ermittlungsbehörden. Statt einer gesetzlichen Verpflichtung, Attacken zu melden, besteht ein erster richtiger Schritt darin, eine Vertrauensbasis herzustellen, die Grundlage für eine Diskussion und Zusammenarbeit privater Unternehmen und öffentlicher Stellen ist. Eine Meldepflicht von Cyber-Attacken ist auch aufgrund der hohen Angriffszahlen und der unterschiedlichen Qualitäten nicht sinnvoll. Schon heute bestehen auf Grundlage unterschiedlicher Gesetze Melde- und Transparenz-Pflichten – insbesondere für die IKT-Branche. Alle weiteren Aktivitäten auf diesem Feld würden einen erheblichen bürokratischen Aufwand bei den Unternehmen generieren, dessen Mehrwert in Frage steht. Zudem wäre eine Kontrolle der gesetzlichen Vorgabe in der Praxis kaum möglich. Hilfreich wären sicher zielgerichtete, verständlich aufbereitete und aktuelle Informationen von BSI, BMI und dem Cyber-Abwehrzentrum.

Gespannt darf man auf die „Internet Security Strategy“ sein, die die EU-Kommission zurzeit ausarbeitet. Darin sollen der Aufbau eines europäischen Frühwarnsystems, der Umgang mit Sicherheitsvorfällen sowie entsprechende Förderschwerpunkte im kommenden Forschungsrahmenprogramm konkretisiert werden.

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? Wie viel Zeit sollte einer solchen Selbstverpflichtungsinitiative eingeräumt werden? 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?**

Der Weg der Selbstregulierung sollte auch weiterhin genutzt werden. Die „Allianz für Cyber Sicherheit“ ist ein richtiger Ansatz. Wir erwarten, dass dies ein guter Rahmen für eine Zusammenarbeit und einen Austausch unterhalb einer gesetzlichen Meldepflicht oder normierter Informationsstrukturen darstellt.

Nach Auskunft von KMU wäre es für diese sehr interessant, von den Erfahrungen großer Unternehmen mit Sicherheitsattacken zu profitieren. Informationen über mögliche Gegenmaßnahmen könnten bei der schnellen Schließung von festgestellten Sicherheitslücken in KMU helfen. Allerdings ist unserer Kenntnis nach die Kooperations-Plattform bei KMU noch viel zu wenig bekannt.

Im Übrigen siehe unsere Antwort zu Frage 3.

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?

Auf welcher Informationsgrundlage das Cyberabwehrzentrum arbeitet, können wir nicht beantworten.

Die Qualität der Cyber-Angriffe, mit denen Unternehmen und Behörden konfrontiert werden, steigt stetig. Diese Angriffe kennen keine Landesgrenzen, so wie das Internet auch keine Grenzen kennt. Unternehmen können sich in Zukunft nicht mehr vollständig alleine vor diesen Angriffen schützen und es bedarf einer starken Zusammenarbeit zwischen Staat und Wirtschaft. Gerade bei der gemeinsamen Erlangung eines komplexen Lagebildes und der Ableitung möglicher Maßnahmen kann die enge Zusammenarbeit einen wichtigen Beitrag leisten.

Ein allgemeines Lagebild über IT-Angriffe auf bundesdeutsche IT-Strukturen kann nur in internationaler Zusammenarbeit mit anderen Regierungen, Telekommunikationsanbietern und der Wirtschaft erarbeitet werden. Die EU bietet hierfür Strukturen mit Anbindung für jedes Mitgliedsland. Darüber hinaus ist eine weitere Zusammenarbeit mit Staaten wie z. B. USA, Russland, China, Indien nötig.

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?

Die öffentliche Hand hat eine wichtige Vorbildfunktion für Unternehmen und Verbraucher. Gleichwohl muss sich auch bei der öffentlichen Hand die Sensibilität für Sicherheitsfragen noch weiter entwickeln. Das BSI gibt mit seiner Arbeit hier Orientierung. Aus diesem Grund ist die Arbeit des BSI insgesamt als sehr positiv zu bewerten.

Die heutige Struktur des BSI scheint uns allerdings bezüglich Schnelligkeit und Flexibilität wenig geeignet, auch KMU unbürokratisch als Dienstleister zu unterstützen. Neutrale und gesicherte Informationen zu IT-Sicherheitsbelangen sind sinnvoll und notwendig. Eine eigene unabhängige Instanz könnte eventuelle Interessenskonflikte vermeiden helfen. Primäre Zielsetzung sollte eine enge Zusammenarbeit zwischen Wirtschaft und Staat in der Bekämpfung von Cyberkriminalität und -terrorismus sein, wobei auch die Zusammenarbeit mit Instanzen außerhalb Deutschlands gesucht werden muss. Das BSI wäre hierbei einer der staatlichen Partner, der in enger Vernetzung mit anderen Kompetenzträgern und einem breiten Spektrum von Transferpartnern agiert.

Ansprechpartner im DIHK:
Dr. Katrin Sobania, Tel. 030/20308-2109, sobania.katrin@dihk.de