

Begrüßung

Rede

Sigmar Gabriel

Bundesminister für Wirtschaft und Energie

Anlass

IT-Sicherheitsforum

am 19.01.2016

Uhrzeit der Rede: 13:30 Uhr

in BMWi Berlin, Aula

Redezeit: 15 – 20 Minuten

Es gilt das gesprochene Wort!

Sperrfrist: Beginn der Rede!

Sehr geehrte Damen und Herren,

ich begrüße Sie ganz herzlich im Bundeswirtschaftsministerium zum heutigen IT-Sicherheitsforum.

IT-Sicherheit geht uns alle an:
Elf Virenangriffe per Email jeden Tag,
und mehr als vier Schadprogramme
pro Woche – das ist die Bilanz an IT-
Attacken auf dieses Haus, das
Bundeswirtschaftsministerium *[Zahlen für
2014].*

Und wenn Sie jetzt denken „Klingt doch gar nicht so viel“, dann machen Sie sich bitte klar:

Das BMWi ist Teil des Netzes der Bundesregierung [*Informationsverbund Bonn-Berlin IVBB*], das über das Bundesamt für Sicherheit in der IT (BSI) zentral geschützt wird. Deren Sicherheitsstrukturen filtern bereits über 99 % der als Schadcode erkannten Mails und Web-Seiten heraus.

Unsere eigene Sicherheitsarchitektur ist also mit dem einen Prozent der Angriffe konfrontiert, die den vorgelagerten Schutz überwinden.

Und ich versichere Ihnen, auch dieses eine Prozent hält die Kollegen in der IT-Abteilung auf Trab.

Sie sehen also, wir sprechen hier aus eigener Erfahrung: IT-Sicherheit geht uns alle an.

Digitalisierung und IT-Sicherheit

Die Sicherheitsproblematik bildet die Schattenseite der Digitalisierung. Dieser globale Trend, meine Damen und Herren, bringt für die deutsche Wirtschaft gewaltige Umbrüche mit sich.

Unsere Industrie erlebt wegen der Digitalisierung gerade die vierte industrielle Revolution – Industrie 4.0.

Mit modernster IT-Technologie entstehen Wertschöpfungsnetzwerke, die uns helfen, Prozesse effizienter zu gestalten, Umwelt und Ressourcen zu schonen, und auch noch Kosten zu sparen.

Große Unternehmen haben sich dem Trend längst angepasst, aber kleine und mittlere Unternehmen tun sich oft noch schwer, ihre etablierten Geschäftsmodelle zu hinterfragen und auf neue, digitale Grundlagen zu stellen.

Klar ist dabei, dass die IT-Sicherheit eine maßgebliche Voraussetzung dafür ist, dass und wie sich Digitalisierung durchsetzt.

Ohne vertrauenswürdige und sichere IT-Strukturen laufen wir Gefahr, unsere Wettbewerbsfähigkeit in Deutschland zu verlieren.

Wenn man sich anschaut, wie Unternehmen, gerade im Mittelstand, mit IT-Sicherheit umgehen, gibt es zwei Extreme.

Ein Teil der Mittelständler, vor allem Kleinbetriebe, scheut aus Sorge um die Sicherheit der eigenen Daten vor der stärkeren Vernetzung zurück. Da hört man oft: „Nie würden ich unsere Unternehmens-Daten in die Cloud geben. Mann kann ja nie wissen, wer die Firmeninterna dann mit liest.“

Risikobewusstsein ist gut, aber sich aus Sorge um die Datensicherheit der Digitalisierung insgesamt zu verweigern – das hieße, das Kind mit dem Bade auszuschütten.

Diesen Unternehmen müssen wir deutlich machen, dass es qualitativ hochwertige und vertrauenswürdige IT-Sicherheitslösungen gibt.

Das andere Extrem sind die Unternehmen, die sich für digitale und vernetzte Prozesse öffnen, aber dabei das Thema IT-Sicherheit unterschätzen und vernachlässigen.

Für diese Unternehmen sind Werkschutz und Fotografierverbot beim Betreten des Firmengeländes selbstverständlich. Aber wenn es um IT-Sicherheit geht, glauben sie, mit handgestrickten Lösungen aus Bordmitteln über die Runden zu kommen.

Aber IT-Sicherheit ist schon lange keine Sache für Amateure mehr. Die täglich stattfindenden erfolgreichen Hacker-Angriffe zeigen uns, wie verwundbar die von uns eingesetzte Informationstechnik ist und wie professionell die Angreifer vorgehen.

Der Schaden, den die Angreifer auslösen, ist immens. Nach aktuellen Schätzungen beläuft sich seine Höhe allein in Deutschland auf über 50 Mrd. Euro pro Jahr. [*Quelle: Bitkom*

Presseinformation „Digitale Angriffe auf jedes zweite Unternehmen“ vom 16.04.2015.]

Ein Ende dieser Entwicklung ist nicht abzusehen. Im Gegenteil: 58 Prozent der Unternehmen und Behörden waren in den vergangenen zwei Jahren Ziel von Cyber-Angriffen. Im Vergleich zum Vorjahr ist die Rate der festgestellten erfolgreichen Angriffe um 8 Prozentpunkte gestiegen.

[*Quelle: Bundesamt für Sicherheit in der Informationstechnik „Cyber-Sicherheits-Umfrage 2015“ vom 06.10.2015.]*

Halten wir deshalb fest: IT-Sicherheit ist für beide Gruppen, wie ich sie hier – nur unwesentlich überzeichnet – vorgestellt habe, ein wichtiges, ja notwendiges Konzept.

Zum Glück haben auch viele Mittelständler die Bedeutung des Themas erkannt. Das Wachstum des IT-Sicherheitsmarktes spiegelt diese Entwicklung wieder.

Seit dem Jahr 2009 ist die Bedeutung der IT-Sicherheitswirtschaft stetig gewachsen.

Bereits vor 3 Jahren hat das Volumen des Markts für IT-Sicherheitsgüter den Wert von 10 Mrd. Euro überschritten.

[Quelle: BMWi, „Der IT-Sicherheitsmarkt in Deutschland“, November 2014]

Die technischen Neuerungen der letzten Jahre werden diesen Trend zusätzlich verstärken: beispielsweise in den Bereichen *Internet der Dinge*, *Mobile* und *Cloud Computing*.

Diese Entwicklung verdeutlicht, zu welchem wichtigem Grundpfeiler die Sicherheit der Informationstechnik mittlerweile geworden ist. Wir befinden uns in einem Wettlauf gegen die immer raffinierter vorgehenden Angreifer.

Diesen Wettlauf dürfen wir auf keinen Fall verlieren. Von den Chancen der Digitalen Gesellschaft können wir nur dann langfristig profitieren, wenn das Vertrauen in die IT-Sicherheit bestehen bleibt.

Denn auch zukünftige Anwendungen wie das intelligente Heim oder das autonome Auto sind auf sichere digitale Technologien angewiesen.

[Ein Beispiel: Im Sommer 2015 gelang es US-Computerexperten über das Internet, in das Infotainmentsystem eines Geländewagens einzudringen und die Kontrolle über die elektronische Steuerung bis hin zur Gas- und Bremsregulierung zu übernehmen.]

Sie können sich vorstellen, welche verheerenden Konsequenzen für die weitere Entwicklung des autonomen Fahrens es hätte, wenn es Automobilherstellern nicht gelingt, die Fahrzeug-IT sicher zu gestalten.]

Vor uns liegen also große Aufgaben!

Meine sehr geehrten Damen und Herren,
die Politik ist sich der Größe und Dringlichkeit dieser Aufgabe sehr bewusst. Es zählt zu den wichtigsten Zielen der Bundesregierung, die IT-Sicherheit nachhaltig und effektiv zu stärken.

Mit dem IT-Sicherheitsgesetz, das im Sommer 2015 in Kraft getreten ist, hat die Bundesregierung in einem ersten, wichtigen Schritt dafür gesorgt, dass kritische Infrastrukturen, also für unsere Wirtschaft besonders sensible Bereiche *[Energie, IKT, Logistik, Gesundheit, Wasser, Ernährung, Finanzen]*, besser geschützt werden.

Mit der Initiative „IT-Sicherheit in der Wirtschaft“ fördern wir seit 2011 das Bewusstsein für IT-Sicherheit – speziell in kleinen und mittleren

Unternehmen. *[Mit kostenlosen*

Unterstützungsmaßnahmen wie dem

IT-Sicherheitsnavigator bündeln wir Informationen und Angebote wie Broschüren, Schnelltests und regionale Beratungsstellen.]

Zum Beispiel geben wir
Mittelständlern Hilfestellung dabei,
ihren IT-Sicherheitsbedarf qualitativ
und quantitativ abzuschätzen.

Mit dem von uns geförderten Projekt
des *eco-Verbands der
Internetwirtschaft* können
Unternehmen ihre Web-Seiten auf
den Befall mit Schadcode überprüfen
und bereinigen lassen.

Ein deutschlandweites Netzwerk von
IT-Sicherheitsbotschaftern im
Handwerk kann vor Ort bei der
Umsetzung von
Sicherheitsmaßnahmen helfen.

[Zusätzlich fördern wir Projekte wie „KMU Aware“, bei dem über eine Online-Plattform branchenspezifisch neue Bewusstseins- und Ausbildungsmaßnahmen angeboten werden.]

IT-Sicherheit ist keine Angelegenheit nur für wenige Experten, denn sie geht jeden im Betrieb an. Mit dem Programm „IT-Sicherheit für Berufsschüler“ *[von: Deutschland sicher im Netz e.V., gefördert durch das BMWi]* wird frühzeitig praxisnahes IT-Sicherheitswissen vermittelt.

Ein tolles Instrument, die Digitalkompetenz und Kreativität von jungen Leuten in die richtigen Bahnen zu lenken, ist der „Cyber Security Challenge Germany“.

Dieser Wettbewerb, bei dem sich junge Hacker messen, hilft uns, frühzeitig neue IT-Talente zu entdecken und sie auf die richtige Seite zu bringen. Die erste Challenge fand 2015 hier im Haus statt. *[eröffnet durch PSt Zypries]*

Ich denke, das kann sich schon mal sehen lassen, aber wir können – und müssen - noch mehr tun – jedoch nicht alleine.

Nur wenn der Staat, Unternehmen, Verbände, Wissenschaft und Anwender diese Aufgabe gemeinsam angehen, werden wir erfolgreich sein.

IT-Sicherheitsforum

Aus diesem Grund richten wir heute im Bundeswirtschaftsministerium dieses „IT-Sicherheitsforum“ aus.

Wir wollen noch konkreter wissen, wo genau – und bei welchen Branchen speziell – die Schwierigkeiten oder Hemmnisse im sicheren Umgang mit IT liegen. So erfahren wir, wo wir die Unternehmen am besten unterstützen können.

[Dazu lässt BMWi auch grundlegende Studien zum Thema erstellen und die Wirtschaft, speziell KMU, repräsentativ befragen. Geplant sind auch Workshops, in denen wir die heute gefundenen Schwerpunktthemen vertiefen. St Machnig hat seine Beteiligung hierzu in Aussicht gestellt.]

Und lassen Sie mich bereits an dieser Stelle betonen: Nach der heutigen Veranstaltung ist nicht Schluss mit dem Dialog. Die Diskussionen und die wirkliche Arbeit gehen danach erst los.

Heute möchten wir den Dialog mit Ihnen zu drei Themenfeldern eröffnen.

1. Durch eine Verbesserung des Ordnungs- und Rechtsrahmens sollen Unternehmen und Anwender entlastet werden.

Genannt werden hier etwa

- eine Produkthaftung für IT-Sicherheitsmängel,
- eine Pflicht zur Verschlüsselung von sensiblen Daten,

- sowie sichere Identitäten im Internet der Dinge.

Auch eine Stärkung der Prüf- und Durchsetzungsbefugnisse des BSI bis hin zur Unabhängigkeit der Behörde werden diskutiert [*Zuständigkeit BMI !*]

2. Das zweite Themenfeld ist die Verbesserung der IT-Sicherheit in der Wirtschaft.

Dazu gehören etwa:

- verbesserte Informationsangebote über Software-Schwachstellen,
- neue, einfach handhabbare Werkzeuge für die Anwender,
- Gütesiegel und Zertifikate
- oder unabhängige Prüfungen der Sicherheit von Hard- und Software.

3. Das dritte Themenfeld betrifft die Stärkung der nationalen und europäischen IT-Sicherheitswirtschaft.

Stichpunkte sind hier:

- Identifikation von Kernkompetenzen unserer IT-Sicherheitswirtschaft,
- Förderung der Information und Vernetzung der Branche,
- Sicherung des Fachkräftebedarfs
- sowie Maßnahmen der Wirtschaftsförderung, wie etwa Stärkung der Marke „IT-Sicherheit in Germany“.

Schluss

Meine Damen und Herren,
wir haben uns auf dem heutigen
Forum viel vorgenommen:

Wir wollen mit Ihnen konkrete Ansätze
entwickeln und Ideen aufnehmen.
Und wir wollen gemeinsam eine
Priorisierung vornehmen. Denn wir
wissen, wir können nicht alles
gleichzeitig und mit gleicher Intensität
angehen.

Ich will an dieser Stelle betonen: IT-
Sicherheit berührt mehrere Ressorts
und daher werden wir uns
selbstverständlich mit den Kollegen,
insbesondere aus dem BMI und dem
BMBF abstimmen.

Vertreter dieser Häuser sind heute auch anwesend.

Ich freue mich auch, dass wir für das heutige Forum so viele kompetente Sprecher und Experten gewinnen konnten. Bereits im Vorfeld der heutigen Veranstaltung haben wir einige Anregungen erhalten. Auch dafür danke ich Ihnen! *[Im November 2015*

fand auf Arbeitsebene ein erstes Treffen mit Vertretern aus der Wirtschaft, Wissenschaft und Gesellschaft statt.

Ich möchte Sie ermutigen, den weiteren Prozess aktiv mitzugestalten! Die heutige Veranstaltung bietet dafür alle Möglichkeiten!

Vielen Dank!