Bayerisches Staatsministerium
des Innern

Rede des Bayerischen Staatsministers des Innern,
Joachim Herrmann,

anlässlich der Eröffnung des Cyber-Allianz-Zentrums

am 1. Juli 2013 in München

Es gilt das gesprochene Wort!

Anrede!

Einleitende Worte

Der **Schutz** der **Wirtschaft** ist der **Staatsregierung** seit jeher ein großes **Anliegen**. Die **tragende Rolle** unseres innovativen **Mittelstands** und unserer **Industrie** für unser Wirtschaftsmodell und unseren Wohlstand kann **nicht oft genug betont** werden.

Im Rahmen des **Wirtschaftsschutzes** hat sich das Landesamt für Verfassungsschutz insbesondere im Bereich der **präventiven Spionage**- und **Sabotageabwehr** in vielen Jahren einen **hervorragenden Ruf** erarbeitet. Es genießt in der gesamten Bundesrepublik schon heute hohes Ansehen.

Das höre ich nicht nur aus der **Wirtschaft**, sondern auch aus **Bundeseinrichtungen**. Es freut mich sehr, dass heute auch Vertreter des **Bundesamts** für **Sicherheit** in der **Informationstechnik** (BSI) hierher

nach München gekommen sind. Ich begrüße Sie ganz herzlich und sehe Ihren Besuch als wichtiges Signal.

Die **anerkannte Arbeit** des **LfV** ist einer der Gründe, warum mein **Kollege Martin Zeil** und ich vor zwei Jahren hier im Amt das **Internetportal** „Wirtschaftsschutz Bayern“ der Öffentlichkeit **präsentieren** konnten.

Gefahren des Internet

Meine Damen und Herren, die **Sicherheit** im **Internet** ist ein **Kernthema** des **21. Jahrhunderts**. Mit der alle Lebensbereiche umfassenden Veränderung unserer Gesellschaft durch die Digitalisierung sind neue **Chancen**, aber auch neue **Gefahren** entstanden.

Dies gilt vor allem für die **Wirtschaft**, die infolge der Globalisierung mit den Märkten dieser Welt auch **virtuell** immer enger **vernetzt** ist.

Die **Möglichkeiten** der **Spionage** und **Sabotage** sind **anonymer** und für den Angreifer **risikoloser** geworden, weil z.B. der eigene Aufenthaltsort technisch verschleiert werden kann. **Deutschlands** und **Bayerns** Wohlstand gründet im Wesentlichen auf dem Rohstoff **Geist** und der **Innovationskraft** ihrer Wirtschaft. Sie sind besonders gefährdet. Insbesondere unseren Unternehmen droht, dass das **Werk** ihrer Mühen von **Datendieben gestohlen** oder von **Saboteuren geschädigt** wird. Damit steht unser gesamtes Gesellschaftssystem auf dem Spiel.

Anspruch auf Schutz durch den Staat

Meine Damen und Herren, das **Internet** ist **kein rechtsfreier Raum**. Wie in jedem anderen Lebensbereich haben Bürger, aber auch Unternehmen und Gewerbebetriebe, im Cyberraum einen **Schutzanspruch** gegenüber dem Staat. Genau dem entspricht das neue **Cyber**-**Allianz**–**Zentrums,** das mit Herrn **George** von einem im **Bereich**

Wirtschaftsschutz erfahrenen **Mitarbeiter geleitet wird**.

Für die Ausgestaltung des Cyber-Allianz-Zentrums waren letztlich **drei wesentliche Anliegen** der Wirtschaft maßgebend:

Bedarf der Wirtschaft

1. **Klare Organisation**
   Die Unternehmen wünschen sich **Transparenz**. Sie müssen wissen, wer ihr **Ansprechpartner** beim Staat ist. Mit dem Cyber-Allianz-Zentrum schaffen wir Klarheit. Es **ist** in **Bayern** der **zentrale Ansprechpartner** für alle Fragen bei Cyberangriffen auf Unternehmen in Bayern und koordiniert die weiteren Schritte.

2. **Vertraulichkeit**
   Die Wirtschaft hat – vollkommen **zu Recht** – absolute **Vertraulichkeit** bei **Meldungen** über mögliche Angriffe gefordert. Vertraulichkeit war aus Angst vor Reputationsverlust und damit wirtschaf-

tlichen Folgen ein zentrales Anliegen der befragten Unternehmen. Wir betreten hier Neuland, indem wir den **Verfassungsschutz** mit dieser Aufgabe betrauen. Hier können wir die **Vertraulichkeit** am besten **garantieren**.

Und die **Zahlen** *zeigen*, dass wir auf dem **richtigen Weg** sind: Während oft geklagt wird, dass die Unternehmen von sich aus Angriffe nicht melden würden, sind im BayLfV schon vor Gründung des Cyber-Allianz-Zentrums **binnen** eines **Jahres** ca. **150 vertrauliche Meldungen** zu möglichen Angriffen eingegangen und abgearbeitet worden.

3. **Schnelle Rückmeldung**
   Die Wirtschaft muss aus dem Kontakt zum Staat schließlich auch einen **Mehrwert** haben. Er besteht nach eigenem Bekunden in einer möglichst **schnellen Rückmeldung**. Damit ermöglichen wir den Unternehmen, die Gefahren einzu-

schätzen. Durch die Voranalyse von Angriffen im LfV und die **enge Zusammenarbeit** mit dem **BfV** und dem **BSI** können wir diesem Wunsch der Unternehmen nachkommen.

Bund als Dienstleister

Hierbei sind wir auch auf ein **starkes** und **schnelles Kompetenzzentrum** auf Bundesebene angewiesen. Deshalb setze ich mich ausdrücklich für eine **gute fachliche Ausstattung des BSI** und des **BfV** ein. Sie müssen sich zum **Dienstleister auch für die Länder** entwickeln.

Nur durch die enge Zusammenarbeit zwischen **Bund**, **Ländern** und **unseren internationalen Partnern** können wir ein starkes Netzwerk gegen Cybergefahren errichten.

Kritische Infrastrukturen

Besonderen Gefahren ist unserer Gesellschaft bei **Beeinträchtigung** von **kritischen Infrastrukturen** ausgesetzt.

Auch für sie ist nun mit dem Cyber-Allianz-Zentrum ein kompetenter, staatlicher **Ansprechpartner** vorhanden. Alle **Betreiber kritischer Infrastrukturen** – auch die öffentlich-rechtlich organisierten – sind heute unternehmerisch am Markt tätig. Sie **haben Konkurrenz**. Hier besteht daher ebenfalls die Forderung nach vertraulicher Abarbeitung ihrer Meldung.

Drei Säulen der Bearbeitung

Meine Damen und Herren, innerhalb des Cyber Allianz Zentrums wird es mit

- der **forensisch-technischen Analyse**,
- der **nachrichtendienstlichen Bewertung** und
- der **Kommunikation und Netzwerkbildung**

drei Kernbereiche geben**,** die in der täglichen Arbeit wie Zahnräder ineinander greifen werden.

Beispiel

Nehmen wir an, ein Unternehmen ist möglicherweise von einem gezielten Angriff betroffen. Der **Sicherheitsbeauftragte** wen-

det sich vertrauensvoll und vertraulich an das **Cyber-Allianz-Zentrum**.

Säule 1: Technisch-forensische Analyse

Zunächst wird dieser Vorfall aus technischer Sicht **forensisch analysiert**. Es findet dabei auch ein **anonymer Abgleich** beim **Bundesamt** für Verfassungsschutz statt. Um stets auf dem aktuellen Stand zu bleiben, wird es auch einen **Austausch** mit **externen Know-how-Trägern** aus der Wirtschaft – etwa Herstellern von **Antivirensoftware** – geben.

Säule 2: Nachrichtendienstliche Bewertung

Die **Ergebnisse** der technischen Analysen **fließen** weiter in die **zweite Säule** des Cyber Allianz Zentrums, in der die **nachrichtendienstliche Bewertung** stattfindet. Gerade bei dieser Art der Analyse konnten wir immer wieder **weitere Opfer ausmachen**.

Das **Besondere** ist jetzt: Die Ergebnisse werden nicht nur gesammelt und intern weiterverarbeitet; wir **informieren** neben dem betroffenen Unternehmen **auch ande-**

re möglicherweise von einem Angriff **betroffene Unternehmen** aus der **gleichen Branche** – sie erhalten die technischen Informationen zum Angriff, um selbst agieren zu können – **selbstverständlich** in **anonymisierter Form**. Damit erzielen wir einen echten **Mehrwert** für eine **Vielzahl von Unternehmen**. Wir schaffen dadurch gleichzeitig einen Anreiz, solche Vorfälle zu melden.

Vertrauen und **Vertraulichkeit** spielen bei der Kooperation von Staat und Wirtschaft eine **zentrale Rolle**. Ohne dieses Band werden Unternehmen nicht bereit sein, **interne** und **höchst sensible Informationen** mit Behörden zu teilen. Umgekehrt wird auch der **Staat nicht bereit** sein, **Informationen** aus der **Spionageabwehr** an die **Wirtschaft** zu geben.

Die Erfahrungen beim Wirtschaftsschutz zeigen, dass **Vertrauen** nur dann **entsteht**, wenn man **vor Ort** ein **persönli-**

ches Vertrauensverhältnis pflegt. Die Menschen müssen sich kennen – von **Angesicht zu Angesicht**. Genau darum glaube ich auch, dass die Zentralisierung einer solchen **Schnittstelle** von **Staat** und **Wirtschaft** beim **Bund nicht ausreichend** wäre.

Deshalb schaffen wir im Cyber-Allianz-Zentrum Bayern auch eine **eigene Säule „Kommunikation und Netzwerkarbeit“**. Sie garantiert einen dauerhaften **persönlichen Austausch**. Darauf lege ich allergrößten Wert.

Eigenverantwortung

Meine Damen und Herren, natürlich bleiben die Unternehmen für ihre IT-Sicherheit weiterhin **selbst verantwortlich**. Mit der Einrichtung des Cyber-Allianz-Zentrum schaffen wir aber ein konkretes **staatliches Angebot** zum vertraulichen **Austausch** sensibelster **IT-Sicherheitsinformationen**. **Staat** und **Wirtschaft entwickeln** sich in meiner Wunschvorstellung

hier **gemeinsam** zu einer **lernenden Organisation**.

Verhältnis zur Polizei, Beispielsfall

Das Landesamt für Verfassungsschutz übernimmt auch die sehr wichtige Rolle des **Vermittlers zu Ermittlungsbehörden** von Justiz und Polizei, wenn dies erforderlich wird:

Vor ca. einem Jahr stellte beispielsweise ein **Unternehmen** einen **Informationsabfluss** fest. Ein **USB-Stick** der Firma wurde auf der **Straße gefunden**. Der Finder leitete ihn dem Unternehmen zu. Als die IT-Abteilung seinen **Inhalt** überprüfte, war man verwundert. Auf ihm waren **höchst brisante Informationen** abgelegt. Sie hätten **niemals extern gespeichert** werden dürfen. Der ermittelte Eigentümer des USB-Sticks war ein Mitarbeiter, der in der Entwicklungsabteilung eingesetzt war.

Da nicht ausgeschlossen werden konnte, dass es sich um einen **gezielten Ausspä-**

hungsversuch des Unternehmens handelte, wurde zunächst ein Beamter des Verfassungsschutzes beigezogen und der Sachverhalt **vertraulich** erörtert.

Er riet dem Konzern, sich mit dem Vorfall an die **Polizei** zu **wenden**. Nach einigem Zögern stimmte das Unternehmen zu. Bereits **30 Minuten später** war das bayerische Landeskriminalamt vor Ort, um eine **offizielle Anzeige des Unternehmens** entgegen zu nehmen.

Aber nicht nur den Ermittlungsbehörden, sondern auch der Bundesebene dient das **LfV** als **Kooperationspartner**: Es ist integraler Bestandteil **der IT-Sicherheitsstrategie der Bundesregierung** und wird sich hier aktiv einbringen.

Wünsche, Schlussworte

Meine Damen und Herren, ich freue mich, dass das **Cyber-Allianz-Zentrum Bayern** unserer **Wirtschaft** und unseren **Behörden** mit dem heutigen Tag hilfreich zur

Seite steht. Ich kann nur an die **Wirtschaft appellieren**, von diesem **Angebot** rege **Gebrauch** zu **machen**!

Von Herzen **wünsche** ich dem **Cyber-Allianz-Zentrum** für seine verantwortungsvolle Tätigkeit **viel Glück** und **Erfolg**.