Bayerisches Staatsministerium
des Innern

Rede des Bayerischen Staatsministers des Innern,
Joachim Herrmann,

anlässlich der Konferenz der vbw zur Cybersicherheit
am 25. Juni 2013 in der Münchner Residenz

Thema „Bayerns Strategie für Cybersicherheit“

Es gilt das gesprochene Wort!

25.06.2013 AS

Anrede!

Einleitende Worte

Am **11. April** habe ich eine **Regierungserklärung** im Bayerischen Landtag abgegeben zu unserer neuen **Strategie** für **Cybersicherheit**. **Kerngedanke** ist eine Vernetzung unserer **Verwaltung** mit **Wirtschaft** und **Wissenschaft**, um gegen die Gefahren aus dem Netz besser gewappnet zu sein.

Ich **danke** der **vbw**, und insbesondere Ihnen, lieber Herr **Brossardt**, nachdrücklich, dass Sie dies aufgegriffen haben. Was das **Networking** anbelangt, ist die **vbw** ja ein **hervorragender Partner**.

Ausgangslage

Meine Damen und Herren, der Freistaat **Bayern** ist zwar das **sicherste** aller **deutschen** Länder. Gleichwohl müssen wir **neuen Gefahren** klar ins Auge sehen.

Strategie für Cybersicherheit

Mit unserer Strategie für Cybersicherheit wollen wir ein **hohes Sicherheitsniveau** für Bayerns Bürger und Unternehmen

schaffen und die **kritischen Infrastrukturen** sowie die **Handlungsfähigkeit** des **Staates schützen.** Es geht uns konkret um folgende Punkte:

Schutz der Wirtschaft

1. Ganz zentral ist für uns der **Schutz** der **Wirtschaft**. Das **Bayerische Landesamt für Verfassungsschutz** hat eine hohe Kompetenz im Bereich der Abwehr von **Wirtschaftsspionage** entwickelt. Ein Beispiel ist das **Wirtschaftsschutzportal**, das in **Zusammenarbeit** mit dem **Wirtschaftsministerium** aufgebaut wurde. Das Landesamt verfügt bereits heute über **gute** und **vertrauensvolle Verbindungen** zu zahlreichen Unternehmen.

Cyber-Allianz-Zentrum im LfV

Daran anschließend schaffen wir nun beim Bayerischen Landesamt für Verfassungsschutz das „**Cyber-Allianz-Zentrum Bayern“.** Es soll als **zentraler Ansprechpartner** und **Kompetenzzentrum** für **Unternehmen** sowie **Betreiber kritischer Infrastrukturen** so-

wohl hinsichtlich der **Prävention** als auch der **Abwehr konkreter Gefahren** dienen. Damit schaffen wir für die Wirtschaft ein konkretes Angebot, das ihrem besonderen **Bedürfnis nach Vertraulichkeit** gerecht wird.

Das **Cyber-Allianz-Zentrum** wird am **1. Juli** seinen Betrieb aufnehmen. Es freut mich sehr, dass die **ersten Reaktionen** auf die **Ansiedelung beim Verfassungsschutz** sowohl aus der **Wirtschaft** wie auch vom **Bundesamt** für **Sicherheit** in der **Informationstechnik ausnahmslos positiv** sind!

Vernetzung der wichtigsten Akteure

2. Wir wollen jedoch nicht nur die **Zusammenarbeit** mit der Wirtschaft auf eine neue Grundlage stellen, sondern mit **allen** für die Cybersicherheit wichtigen **Akteuren**. Unsere heutige **Konferenz** bildet hierzu einen wichtigen **Baustein**. Wir **intensivieren** und **institutionalisieren** hierzu einen **dauerhaften Dialog** im Bereich Cybercrime, Cybersicherheit

sowie Datenschutz zwischen unseren **Sicherheitsbehörden**, dem **IT-Beauftragten** der Staatsregierung, den anderen Ressorts, der Wissenschaft, und insbesondere den **Verbänden** und **Unternehmen**. Wir tun dies in **enger Kooperation** mit dem **Wirtschaftsministerium**. StM Martin Zeil wird Ihnen gleich im Anschluss das **Förderprogramm Digital Bavaria** vorstellen.

Koordination im StMI

3. Aus genau diesem Grund haben wir zur Koordination der strategischen Belange im **Innenministerium** das **Sachgebiet „Cybersicherheit“** geschaffen. Besonders wichtig ist mir dabei die **enge Kooperation** mit **Bund** und **Ländern**, wie der **EU**. Begrüßen will ich an dieser Stelle den neuen Referatsleiter, Herrn **Dr. Bär**. Damit kann die **Vernetzung** heute gleich weiter **ausgebaut** werden.

Schutz Bürgerinnen und Bürger

4. Ziel unserer Strategie ist auch, die **Cybersicherheit** der **Bürgerinnen** und **Bürger** zu **verbessern**. Die **Sicherheit**

des Einzelnen ist jedoch nur zu gewährleisten, wenn jeder seiner **Verantwortung** gerecht wird. Denn **ungeschützte Rechner** können zu „**Virenschleudern**“ umfunktioniert oder als Teil von sogenannten Botnetzwerken anderen Rechnern Schaden zufügen. Dabei hilft oft schon ein **aktueller Virenschutz** oder eine **Firewall**.

Die Nutzer machen sich oft auch zu wenige Gedanken darüber, welche Massen an **sensiblen Daten** sie generieren und unbedarft über das Netz **weitergeben**. Um sie zu sensibilisieren, setzen wir auf **Beratungsangebote** - von der Vermittlung von Medienkompetenz mit dem **Medienführerschein Bayern** bis zu Präventionsangeboten des Landeskriminalamtes. Besonders hinweisen möchte ich Sie auf das **Landesamt für Datenschutzaufsicht**. Es hat sich zu einem deutschlandweit anerkannten **Kompetenzzentrum** für Datenschutzfragen im

Umgang mit Unternehmen oder Sozialen Netzwerken entwickelt.

Schutz staatlicher Handlungsfähigkeit

5. Meine Damen und Herren, es geht uns bei unserer Strategie für Cybersicherheit auch darum, unsere **Sicherheitsbehörden** zu **stärken** und die **Handlungsfähigkeit** des **Staates sicherzustellen**. Sie hängt immer mehr von **verlässlichen IT-Netzen** ab. Das gilt für Polizeieinsatzzentralen ebenso wie für die gesamte Steuerverwaltung. Die **ressortübergreifende Verantwortung** für die Funktionsfähigkeit der staatlichen IT-Nutzung trägt der **IT-Beauftragte** der Bayerischen Staatsregierung, Herr **Staatssekretär Pschierer**. Er wird in Kürze das Wort an Sie richten.

Maßnahmen der Sicherheitsbehörden

Unsere **Sicherheitsbehörden haben sich** in den letzten Jahren kontinuierlich auf die neuen Herausforderungen **eingestellt**. So haben wir als erstes Land 1995 im **LKA** die anlassunabhängige Netzwerkfahndung

eingeführt und für komplexe Cybercrime-verfahren eine Task-Force eingerichtet.

In den Ballungsräumen gibt es **Schwerpunktkommissariate** zur Bekämpfung der Computer- und Internetkriminalität. Als erstes Land haben wir auch die **Sonderlaufbahn** der **IuK-Kriminalisten** geschaffen. 25 Informatiker haben wir zu „echten“ Polizisten ausgebildet. Aufgrund der guten Erfahrungen führen wir die Initiative dieses Jahr in der **gleichen Größenordnung** fort.

Ermöglichung effektiver Strafverfolgung

Diesen Kolleginnen und Kollegen müssen wir aber auch die richtigen Instrumente an die Hand geben. Wir brauchen deshalb **Möglichkeiten** zur **Sicherung digitaler Spuren,** wie eine **verfassungskonforme** Speicherung von **Verbindungsdaten** wie **IP-Adressen**.

Wie die aktuelle Debatte zum Überwachungsprogramm **PRISM** der **USA** zeigt, gilt es dabei stets, die berechtigten **Sicherheitsinteressen** des Staates in **Einklang**

mit dem **Datenschutz** der Nutzer zu bringen. Dass die **datenschutzrechtlichen Standards** in den **USA** und Europa nicht vergleichbar sind, haben schon die Debatten um **SWIFT** oder die Übermittlung von **Flugverkehrsdaten** gezeigt. Hier gilt es, mit der **notwendigen Transparenz** auf eine verlässliche **Kooperation** nach **rechtsstaatlichen Standards** zu setzen.

Schlussworte

Meine Damen und Herren, große Aufgaben stehen vor uns: Im Bund und auf EU-Ebene wird beispielsweise über **neue rechtliche Regelungen** diskutiert, mit denen Energieversorger oder andere **Betreiber kritischer Infrastrukturen verpflichtet** werden sollen, ihre **Netze besser zu schützen** und einschlägige Vorfälle zu melden. Ich bin davon überzeugt, dass es **nicht** unter das **Betriebsgeheimnis** eines Energieversorgers fällt, wenn die Steuerung eines **Kernkraftwerks** attackiert wird oder wegen eines Cyberangriffs ein großflächiger Stromausfall droht.

Zentrale Frage wird dabei sicher sein, an welche Stellen diese Meldungen sinnvollerweise **als erstes** erfolgen sollen. Meldewege an den Gefahrenabwehr- und Katastrophenschutzbehörden **der Länder vorbei** kann es aus meiner Sicht nicht geben.

Schutzpflicht des Staates umfasst Cyberspace

Meine Damen und Herren, es gibt einen breiten Konsens darüber, dass es **Kernaufgabe** des Staates ist, **Kriminalität zu bekämpfen** und Verbrecher zu bestrafen. Gerade angesichts seiner dominierenden Bedeutung für alle Lebensbereiche kann es für das **Internet keine Ausnahme** geben: Es darf **kein rechtsfreier Raum** sein. Die **Schutzpflicht** des Staates besteht auch im Cyberspace!

Mein **Ziel** ist deshalb, ein **starkes Netzwerk**, eine **Allianz** für **Cybersicherheit** zu schaffen – zum **Schutz** der **Bürgerinnen** und **Bürger**, unseres **Staates** und der **Wirtschaft**. Dazu bitte ich Sie alle um Ihre **Unterstützung**!