Bayerisches Staatsministerium
des Innern

Regierungserklärung des Bayerischen Staatsministers des Innern,
Joachim Herrmann,

am 11. April 2013 im Bayerischen Landtag

Thema „Bayern digital – Sicherheit im Internet“

Es gilt das gesprochene Wort!

Anrede!

Einleitende Worte

Der Freistaat **Bayern** ist das **sicherste** aller **deutschen** Länder. Hier leben die Menschen sicherer als anderswo. Das ist das Ergebnis einer konsequenten und **erfolgreichen Innen**- und **Rechtspolitik** der Bayerischen **Staatsregierung**. Es ist aber auch der Erfolg des großartigen Engagements unserer **Kolleginnen** und **Kollegen** in Polizei und Justiz. Ihnen sage ich für ihren steten Einsatz für unser aller Sicherheit herzlichen **Dank**.

Trotz dieser Erfolge müssen wir **neuen Gefahren** klar ins Auge sehen: Risiken von bisher unbekannter Dimension.

Südkorea bekommt momentan die Konfrontation mit dem kommunistischen Nordkorea auch durch massive Cyberangriffe zu spüren. Vor solchen Angriffen ist kein Land in der Welt sicher.

Der „Kalte Krieg“ ist vorbei – der **Krieg** in der **virtuellen Welt** des Internets aber wird von Jahr zu Jahr **heißer**. Dabei ist immer schwieriger zwischen inländischen und ausländischen Angriffen zu unterscheiden.

Alleine auf das **Bayerische Behördennetz** gibt es **täglich** über **36**.**000** Angriffsversuche aus dem Internet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Jahr 2011 pro Tag vier bis fünf gezielte und gravierende Trojaner-Angriffe auf das deutsche Regierungsnetz abwenden müssen.

Besonders gefährdet sind auch Einrichtungen der sogenannten **kritischen Infrastruktur.** Kraftwerke, Stromnetze, Telekommunikationsnetze oder auch Banken können mit Schadsoftware, Virenprogrammen und Trojanern gestört oder sogar lahmgelegt werden. Denken Sie an den bekannten Computer-Wurm **Stuxnet**.

Die Sicherheitsbranche hat im Jahr 2011 weltweit **5,5 Milliarden Cyberangriffe** auf **Wirtschaftsunternehmen** registriert – 81 % mehr als im Vorjahr. Deutschland ist dabei das häufigste Angriffsziel in Europa.

Meistens geht es um **Wirtschaftsspionage.** Deutsche und vor allem **bayerische mittelständische Unternehmen** gehören zu den **innovativsten weltweit**. Kleine und mittlere Unternehmen stehen im Fokus der Hacker: 2011 zielte die Hälfte der Angriffe in Deutschland auf Unternehmen mit weniger als 2.500 Beschäftigten. Nach der offiziellen Statistik des Bundeskriminalamts haben sich die **gemeldeten Schäden** durch Cyberkriminalität von 2009 bis 2011 auf 71,2 Millionen Euro **verdoppelt**. Dabei geht man aber davon aus, dass nur einer von 1.000 Cyberangriffen angezeigt wird. Manche Unternehmen haben zum Beispiel Angst vor einem Imageschaden.

Die **Vereinigung der Bayerischen Wirtschaft** schätzt den **Schaden** für die deut-

sche Wirtschaft auf bis zu **50 Milliarden Euro jährlich.**

Diese Angriffe haben oft auch den Zweck **Schaden anzurichten,** Systeme lahmzulegen und Unternehmen zu erpressen: Die Sabotage wird nur gegen Zahlung großer Summen beendet.

Extremisten und **Terroristen** nutzen die komplexen Strukturen des Netzes, um neue **Anhänger** zu rekrutieren, um sie zu **fanatisieren** und zu **radikalisieren**. Und sie stellen auch gleich die **Anleitung** zum **Bau** einer **Bombe** mit ins Netz.

Die **Anonymität** des Internets wird aber auch zu **Verbrechen an** den **Schutzbedürftigsten** unserer Gesellschaft genutzt: unseren **Kindern**. Im Jahr 2012 haben wir alleine in Bayern 493 Fälle aufgedeckt, in denen Kinderpornografie über das Netz „verbreitet“ worden ist. Hinter jedem dieser Fälle steht ein konkreter Missbrauch eines Kindes.

Meine Damen und Herren, gleich ob Cyberangriffe fremder Staaten oder brutaler sexueller Missbrauch kleiner Kinder: Wir müssen diese **Bedrohungen** noch entschlossener **bekämpfen**.

Die zunehmende **Digitalisierung** bietet **für den Wirtschaftsstandort Bayern zweifellos große Chancen**: Die „Bayern digital“-Strategie der Staatsregierung setzt deshalb bewusst darauf, dass wir auch hier an der Spitze des Fortschritts marschieren.

Gerade deswegen müssen wir aber auch **Gefahren ernst nehmen**, Risiken reduzieren und Missbrauch eindämmen, Und dabei die Aufgabe des Staates klar definieren.

Egal ob es um Mord oder Totschlag, um Einbruchsdiebstahl oder Erpressung geht – es ist in der realen Welt **Kernaufgabe** des demokratischen **Rechtsstaats**, Kriminalität zu bekämpfen und Verbrecher zu bestrafen. Kurz gesagt: Unsere Bürger

bestmöglich zu schützen und für gleiches Recht für alle zu sorgen. Darüber gibt es einen breiten Konsens.

Doch wie sieht das in der virtuellen Welt aus? Im Internet? Im Cyberspace?

Manch einer propagierte in den letzten Jahren das **staatsfreie Internet**, das Netz des **rechtsfreien Raumes**. Den Schutz geistigen Eigentums gibt es für die Piraten im Netz nicht mehr!

Gerade angesichts der fast unser gesamtes Leben dominierenden Bedeutung des Internets würde ein solches **rechts**- und **staatsfreies Netz** zu **Chaos** und **Anarchie** führen.

Das **Internet** kann **kein rechtsfreier Raum** sein. Daten und Datennetze bedeuten Geld und Macht. Und Geld und Macht sind die zentralen Treiber für organisiertes Verbrechen und Terrorismus.

Deshalb gilt für mich ohne Zweifel: Auch im Cyberspace hat der **Staat** eine **Schutzpflicht** für unsere Bürgerinnen und Bürger.

Strategie für Cyber-sicherheit

Unser Ziel ist es, ein **hohes Sicherheits-niveau** für Bayerns Bürger und Unterneh-men zu **schaffen,** die **kritischen Infra-strukturen** und die **Handlungsfähigkeit** des **Staates** zu **schützen.**

Dazu benenne ich heute fünf Kernpunkte unserer Cyber-Sicherheits-Strategie:

Schutz Bürgerinnen und Bürger

1. Schutz der Bürgerinnen und Bürger

Wie auf den Straßen so ist auch auf der Datenautobahn die **Sicherheit** des Einzel-nen nur zu gewährleisten, wenn jeder seiner **Verantwortung** selbst gerecht wird.

Alle IT-Nutzer müssen sich bewusst sein, dass sie mit ihren **eigenen Systemen** viel zur **Sicherheit** unserer Datennetze **bei-tragen** können. Wer ohne aktuellen Viren-schutz oder Firewall unterwegs ist, gefähr-det nicht nur sich, sondern auch Andere.

Ungeschützte Rechner geraten leicht in die **Macht von Cyberkriminellen** und werden zu „Virenschleudern“ umfunktioniert oder

fügen als Teil von sogenannten Botnetzwerken anderen Rechnern Schaden zu.

Die Nutzer müssen sich auch Gedanken darüber machen, welche Massen an sensiblen **Daten** sie generieren und unbedarft über das Netz **weitergeben**, sei es in sozialen Netzwerken, über Smartphone-Apps oder Suchmaschinen.

Wir müssen die **Nutzer** – das ist inzwischen die große Mehrheit aller Bürgerinnen und Bürger - für diese Probleme **sensibilisieren** und aufklären.

Dafür verfügen wir bereits jetzt über gute Beratungsangebote - von der Vermittlung von Medienkompetenz mit dem **Medienführerschein Bayern** bis zu Präventionsangeboten des Bayerischen Landeskriminalamts.

Herausheben möchte ich unser **Bayerisches Landesamt für Datenschutzaufsicht**. Es hat sich zu einem deutschlandweit anerkannten **Kompetenzzentrum** für Datenschutzfragen im Umgang mit

Unternehmen oder Sozialen Netzwerken entwickelt. Es ist beispielsweise Partner der Initiative „**Datenschutz geht zur Schule**“. Ich bin überhaupt der Meinung, dass die Schulen unsere Jugendlichen noch umfassender für die Chancen, aber auch die Risiken im Netz sensibilisieren müssen.

Schutz staatlicher Handlungs-fähigkeit

2. Schutz der staatlichen Handlungs-fähigkeit, Stärkung der Sicherheits-behörden

Die **Handlungsfähigkeit** unseres **Staates** hängt immer mehr von **verlässlichen IT-Netzen** ab – das gilt für Polizeieinsatz-zentralen ebenso wie für kommunale Verkehrssteuerung oder die gesamte Steuerverwaltung. Die **ressortübergreifende Verantwortung** für die Funktionsfähigkeit der staatlichen IT-Nutzung obliegt in Bayern dem **IT-Beauftragten** der Bayerischen Staatsregierung. Das **Bayern-CERT** schützt zum Beispiel die Internetangebote der Behörden erfolgreich vor Hackeran-

griffen. Aber auch der **Landesbeauftragte** für den **Datenschutz** trägt dazu bei, dass sensible Daten nicht in falsche Hände geraten können.

Maßnahmen der Sicherheits-behörden

Unsere **Sicherheitsbehörden haben sich** im Laufe der letzten Jahre kontinuierlich auf die neuen Herausforderungen der digitalen Welt **eingestellt**.

Als erstes Land haben wir bereits 1995 im **Bayerischen Landeskriminalamt** die anlassunabhängige Netzwerkfahndung eingeführt. Beim LKA wurden außerdem eine Task-Force-Cybercrime eingerichtet und komplexe Cybercrimeverfahren konzentriert.

In den Ballungsräumen gibt es zudem **Schwerpunktkommissariate** zur Bekämpfung der Computer- und Internetkriminalität. Als erstes Bundesland haben wir die **Sonderlaufbahn** der **IuK-Kriminalisten** geschaffen. 25 gelernte Informatiker haben wir bisher zu „echten“ Polizisten ausgebildet. Aufgrund der guten Erfahrun-

gen mit diesem Modell 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. **IT-Täter** sind **keine Kleinkriminellen**. Sie sind meist Teil von Banden und organisierter Kriminalität.

Am digitalen Tatort hilft kein Fingerabdruckpulver. Wir brauchen **Möglichkeiten der Sicherung digitaler Spuren.** Nur so können wir den Opfern effektiv zu ihrem Recht verhelfen.

Bei unserer Forderung nach der Speicherung von **Verbindungsdaten** wie IP-Adressen geht es um notwendige Werkzeuge im Kampf gegen Bedrohungen aus dem Cyberbereich – nach den Regeln des Rechtsstaats und dem Grundsatz der Verhältnismäßigkeit.

Schutz der Wirtschaft

3. Schutz der Wirtschaft

Das **Bayerische Landesamt für Verfassungsschutz** hat eine hohe Kompetenz im

Bereich des Schutzes von Wirtschaftsunternehmen gegen Spionage entwickelt. Ein Beispiel ist das **Wirtschaftsschutzportal**, das in Zusammenarbeit mit dem Wirtschaftsministerium aufgebaut wurde. Es gibt **gute** und vertrauensvolle **Verbindungen** zwischen dem Landesamt und zahlreichen Unternehmen.

Cyber-Allianz-Zentrum im LfV

Daran anschließend schaffen wir nun beim Bayerischen Landesamt für Verfassungsschutz das „**Cyber-Allianz-Zentrum Bayern“.**

Das Cyber-Allianz-Zentrum Bayern wird als zentraler Ansprechpartner und **Kompetenzzentrum** Unternehmen sowie Betreiber kritischer Infrastrukturen bei der Prävention und Abwehr von Bedrohungen aus dem Netz unterstützen. Damit schaffen wir ein konkretes Angebot für die **Wirtschaft**, das dem **Bedürfnis nach Vertraulichkeit** in der Bearbeitung von Cybervorfällen gerecht wird.

Das Cyber-Allianz-Zentrum wird eng mit Einrichtungen von Bund und Ländern zusammenarbeiten und als **Frühwarnsystem** fungieren.

Das Cyber-Allianz-Zentrum Bayern wird am **1. Juli** seinen Betrieb aufnehmen.

Vernetzung der wichtigsten Akteure

4. Vernetzung der Akteure

Wir wollen die Zusammenarbeit jedoch nicht nur mit der Wirtschaft auf eine neue Grundlage stellen, sondern mit **allen** für die Cybersicherheit wichtigen **Akteuren**.

Wir intensivieren und institutionalisieren einen **dauerhaften Dialog** im Bereich Cybercrime, Cybersicherheit sowie Datenschutz zwischen unseren Sicherheitsbehörden, dem IT-Beauftragten der Staatsregierung, den anderen Ressorts, der Wissenschaft, den Verbänden und den Unternehmen. Wir werden dies in enger Kooperation mit dem Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie tun.

Ich begrüße es sehr, dass unser Wirtschaftsministerium unter anderem die **Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit (AISEC)** fördert. Diese Einrichtung beschäftigt sich mit Forschungsthemen wie Softwaresicherheit und Zuverlässigkeit von IT-Systemen.

So können wir frühzeitig **Bedrohungen erkennen**, sie **gemeinsam bewältigen** sowie Präventionsstrategien ausbauen und weiterentwickeln.

Mein Ziel ist eine enge und **vertrauensvolle Zusammenarbeit** aller Beteiligten im Bereich der Cybersicherheit. Nur so werden wir es schaffen, auf den Daten-Autobahnen für mehr Sicherheit zu sorgen.

Koordination im StMI

5. Koordination im Innenministerium

Um alle Akteure auf die Bewältigung dieser Herausforderungen auszurichten, schaffen wir im Bayerischen Staatsministerium des Innern ein neues **Sachgebiet „Cybersicherheit“.** Dieses wird alle strategischen Belange der „Cybersicherheit“ im Ministeri-

um, mit den Ressorts der Staatsregierung sowie mit unseren Partnern in Verwaltung, Wirtschaft, Wissenschaft und Verbänden koordinieren.

Ich lege hier auch großen Wert auf eine **enge Zusammenarbeit** mit dem Bund und den anderen Ländern, dem Bundesamt für Sicherheit in der Informationstechnik und der Europäischen Union.

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 z.B. 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 z.B. die Steuerung eines **Kernkraftwerks** attackiert wird oder wenn wegen eines Cyberangriffs ein

großflächiger Stromausfall droht. Das muss der Staat wissen.

Wir stehen vor einer **Herausforderung** für **Staat** und **Gesellschaft**, wie sie in jeder Generation nur einmal vorkommt. Die Digitalisierung ist der große Megatrend unserer Zeit. Sie durchdringt alle Lebensbereiche.

Mein **Ziel** ist es ein **starkes Netzwerk**, eine **Allianz** für **Cybersicherheit** zu schaffen – zum **Schutz** der **Bürgerinnen** und **Bürger**, unseres **Staates** und der **Wirtschaft**.

Ob Kinderschänder oder Betrüger, ob Wirtschaftsspione oder Terroristen: Wir sagen allen **Cyberkriminellen** den **Kampf** an.

Auch das global vernetzte digitale **Bayern** muss und wird **sichere Heimat** bleiben.

Dazu bitte ich Sie alle um Ihre **Mitarbeit** und um Ihre **Unterstützung**!