Der Bayerische Staatsminister der
Justiz
Prof. Dr. Winfried Bausback

Rede beim

Münchner Cyber Dialog 2017

zum Thema

*„Cyber-Security in Bayern:
Keine Chance für Viren, Würmer, Trolle“*

am 29. Juni 2017

Telefon: 089/5597-3111
Telefax: 089/5597-2332
e-mail: presse@stmj.bayern.de
Internet: www.justiz.bayern.de
Prielmayerstraße 7
80335 München

Es gilt das gesprochene Wort

Anrede!

Als mich letzte Woche mein Kabinettskollege Dr. Huber, der heute zu seinem großen Bedauern verhindert ist, gefragt hat, ob ich heute für ihn **"einspringen" könnte**, hätte das **nicht besser passen können.**

Denn vor etwas über einer Stunde bin ich von einer **Dienstreise aus den USA zurückgekommen,** bei der ich mich **intensiv mit dem Thema "Cybercrime" beschäftigt habe!**

Telefon: 089/5597-3111
Telefax: 089/5597-2332
e-mail: presse@stmj.bayern.de
Internet: www.justiz.bayern.de
Prielmayerstraße 7
80335 München

Sie erlauben mir daher ein paar Worte zu **diesem Thema**, auch wenn der Schwerpunkt Ihrer Tagung auf der Bedeutung der **IT-Infrastruktur insbesondere für die industrielle Produktion liegt.** Aber ich denke, das brandaktuelle Thema "Cybercrime-Bekämpfung" ist in diesem Rahmen sicherlich auch von Interesse.

Anrede!

"Cyber-Security in Bayern: Keine Chancen für Viren, Würmer, Trolle" - so lautet das Thema meiner Rede.

Das Wort **„Troll“** stand in der nordischen Mythologie ja ursprünglich als Oberbegriff für **plumpe, unheimliche, übernatürliche Wesen**. Aber seit nette Trollfiguren mit bunten Haaren in viele **Kinderzimmer** Einzug gehalten haben, ist der Begriff eher niedlich besetzt. Auch das Wort „**Würmer**“ klingt eigentlich recht **harmlos**.

Dieser Eindruck ändert sich sehr schnell, wenn ich stattdessen von **Kinderpornographie, Waffenhandel im Internet und Hackerangriffen** spreche. Dies sind alles hochaktuelle Phänomene, die die bayerischen Ermittlungsbehörden tagtäglich vor **neue Herausforderungen** stellen.

Erst am vergangenen Freitag [1] warnte das **Bundesamt für Sicherheit in der Informationstechnik** vor einer Angriffskampagne, die zielgerichtet auf **E-Mail-Konten** des **Spitzenpersonals aus Wirtschaft und Politik** gerichtet war.

Und wir alle erinnern uns an verschiedene Meldungen zu **Cyberattacken** aus den **vergangenen Monaten**.

Ich denke dabei an die Zerschlagung eines **internationalen Botnetzes** bestehend aus 11.000 Computern in über 90 Staaten durch das BKA.

[1] dpa-Meldung vom 23. Juni 2017

Oder den großen Cyberangriff mit der Schadsoftware „**WannaCry**“ auf über 230.000 Computer in 150 Ländern, der unter anderem auch die Deutsche Bahn betraf. Allein die **IT-Infrastruktur bayerischer Behörden** ist täglich **bis zu 40.000 Angriffsversuchen** ausgesetzt.

Um diesen Herausforderungen in Bayern wirksam begegnen zu können, wurden bei **Polizei, Verfassungsschutz und Justiz spezialisierte Einheiten gegründet,** welche Know-How bündeln und als zentrale Ansprechpartner zur Verfügung stehen.

So wurde beispielsweise beim Bayerischen LKA ein **Cybercrime-Kompetenzzentrum** eingerichtet. Beim Landesamt für Verfassungsschutz besteht das **Cyber-Allianz-Zentrum Bayern**, das insbesondere als **vertraulicher Ansprechpartner** unter anderem für Unternehmen und Forschungseinrichtungen fungiert.

Und auch die **bayerische Justiz ist gut gerüstet**: Neben weiteren Maßnahmen haben wir bei der Generalstaatsanwaltschaft Bamberg die **Zentralstelle Cybercrime Bayern**, kurz ZCB genannt, eingerichtet.

Bei der Errichtung der ZCB haben wir uns von folgendem Grundgedanken leiten lassen: **Vernetzten Straftätern im Cyberspace** kann man nur durch **ebenso gut vernetzte und hoch spezialisierte Arbeit der Strafverfolgungsbehörden** begegnen.

Die ZCB ist daher einerseits **bayernweit zuständig für die Bearbeitung besonders herausgehobener Ermittlungsverfahren im Bereich der Cyberkriminalität**.

Dabei kann es zum Beispiel um **illegale Geschäfte im Darknet** gehen, um das **Ausspähen von Daten** oder **Computersabotage**, um **Hackerangriffe auf prominente Personen** oder auch um sog. **Fakeshops**, durch die eine Vielzahl von Personen geschädigt werden. Dazu gehören aber auch **Angriffe auf kritische Infrastrukturen**.

Die ZCB arbeitet dabei eng mit den **Polizeibehörden** zusammen. Denn: Nur wenn die **Spezialisten** von Justiz und Polizei **eng kooperieren**, kann eine **schnelle und effektive Strafverfolgung** gewährleistet werden.

Auch sind die Mitarbeiter der ZCB in **nationalen** und **internationalen Gremien** präsent, um die **Zusammenarbeit** über Bayern hinaus zu stärken. Beispielsweise war ein Staatsanwalt für drei Monate zu **Interpol in Singapur** abgeordnet. Dort werden die Aktivitäten der internationalen Polizeiorganisationen im Kampf gegen Cybercrime gebündelt. Die reibungslose **Zusammenarbeit** von Polizei und Staatsanwaltschaften auch **über Ländergrenzen** hinweg ist natürlich essentiell. Denn gerade im Internet machen Kriminelle nicht vor nationalen Grenzen Halt.

Die Ermittlungsarbeit im Internet ist **aus vielen Gründen besonders komplex**. Hier spielen die **ständig wachsenden technischen Möglichkeiten eine besonders große Rolle**. In **kaum einem anderen Kriminalitätsbereich** ist es für unsere Strafverfolger entscheidender, an **Strukturen, Netzwerke und Hintermänner** zu gelangen.

Daher **brauchen wir Spezialisten**, die sich **mit dem Internet** und **den Machenschaften der Cyberkriminellen und ihren Netzwerken** auskennen.

In **diesem und im nächsten Jahr** werden wir die ZCB daher noch einmal um **insgesamt 24 Stellen** verstärken; darunter sind nicht nur Staatsanwälte, sondern auch **IT-Forensiker**.

Durch diese **erhebliche personelle Aufstockung** werden wir unsere **Schlagkraft vor allem im Kampf gegen die Kriminalität im sog. Darknet und gegen Kinderpornographie noch einmal deutlich erhöhen**. Diese nach meiner Kenntnis deutschlandweit einmalige Verstärkung kommt zudem auch dem **Schutz der bayerischen Wirtschaft** und unserer **kritischen Infrastrukturen** vor **Wirtschaftsspionage, Computersabotage und Erpressung** zugute.

Keine Frage: Aufgrund der Möglichkeiten des Internets, insbesondere des **Darknets** sowie **digitaler Währungen,** sind oft nur wenige oder keine Ermittlungsansätze gegeben. Dies führt dazu, dass viele Straftaten **nicht aufgeklärt** werden können. Dies ist jedoch kein Grund, den **Kopf in den Sand** zu stecken. Sondern **Ansporn**, die vorhandenen Möglichkeiten auszuschöpfen. Und das tun wir.

Die **Arbeit** der ZCB möchte ich Ihnen an **einigen kleinen Beispielsfällen** demonstrieren, die bereits Gegenstand der öffentlichen Berichterstattung waren:

In einem Verfahren gaben sich die Täter im Rahmen ihrer Verkaufsanzeigen auf gängigen Internetportalen für PKWs als **Notare** aus. Sie spiegelten den Geschädigten wahrheitswidrig vor, Fahrzeuge aus einer polnischen Insolvenzmasse als Treuhänder zu verwalten.

Zur Täuschung verwendeten die Täter **unterschiedliche Namens- und Adressdaten** vermeintlicher Notare und erstellten auch **passende Homepages**.

Auf Grund des Irrtums, der Kontakt finde mit Notaren statt, **verzichteten die Geschädigten auf Besichtigungen der Fahrzeuge**.

In Folge der **grenzüberschreitenden Ermittlungen** konnte einer der Täter in Deutschland, der andere in Rumänien festgenommen werden, bevor er sich - wie geplant - nach Thailand absetzen konnte.

In einem anderen Verfahren geht es um **illegale Streaming-Plattformen**. Der Haupttäter sowie mehrere Unterstützer konnten festgenommen werden. Der Täter hatte das Sendesignal eines Pay-TV-Anbieters über das Internet verbreitet und hierfür monatliche Gebühren verlangt.

Die ZCB geht auch erfolgreich gegen sog. **Fake-Shops** vor. Nach **akribischen und technisch anspruchsvollen Ermittlungen** konnten die mutmaßlichen Betreiber mehrerer Fake-Shops identifiziert und verhaftet werden. Nach den bisherigen Ermittlungen sollen die Beschuldigten mindestens **75 Fake-Shops** im Internet eröffnet und dort hochwertige Konsumgüter angeboten haben.

In einem anderen Fall waren die Fake-Shops **äußerst professionell aufgemacht**. Der Täter verwendete Bilder und Artikelbeschreibungen seriöser Online-Händler. Auch wurde eine **Telefonnummer für Kundenrückfragen** angeboten, die zu einem extra eingerichteten Online-Sekretariat führte. Der Schaden belief sich auf eine **knappe halbe Million Euro**.

Dieser Täter wurde zwischenzeitlich zu einer Freiheitsstrafe von 5 Jahren und 5 Monaten verurteilt.

Dass sich eine Spezialeinheit wie die ZCB auch um solche Fälle von Fake-Shops kümmert, hat durchaus seine Berechtigung. Denn durch Fake-Shops wird nicht nur der individuelle Kunde, sondern auch das **Vertrauen in den Online-Handel insgesamt** beeinträchtigt.

Wie sie sehen, gehen wir die **bestehenden Herausforderungen an**. Klar ist aber auch, dass sich laufend neue technische Phänomene ergeben, die **neue Herausforderungen** mit sich bringen. Um diesen Entwicklungen effektiv begegnen zu können, braucht es eine **intensive Zusammenarbeit aller Beteiligten**.

Dann müssen wir uns auch durch die regelmäßigen Nachrichten über neue *Viren, Würmer und Trolle* nicht verunsichern lassen.

Meine sehr geehrten Damen und Herren,

neben dem beschriebenen Kampf gegen Cyber-Crime darf ich Ihnen **schlaglichtartig folgende der vielen Maßnahmen aus dem Bereich IT / Cyber-Sicherheit** nennen, die die Bayerische Staatsregierung getroffen hat:

- Schon seit vier Jahren setzen wir unsere **Strategie für Cybersicherheit** um. Das heißt:

- Nutzer sensibilisieren,
- Staat, Wirtschaft und Wissenschaft vernetzen,
- Wirtschaft vor Spionage und Sabotage schützen.

Vergangenen Monat haben wir im Kabinett die **zweite Stufe der Strategie BAYERN DIGITAL** beschlossen. Wir werden in den nächsten fünf Jahren **3 Milliarden Euro investieren und rund 2.000 Stellen schaffen**!

1 Milliarde Euro nehmen wir für die **Gigabit-Infrastruktur** in die Hand. 2 Milliarden Euro setzen wir für die **digitalen Kernthemen** ein:

- **Wir machen digitale Kompetenz zum Markenzeichen unserer Jugend** – unter anderem mit digital unterstütztem Unterricht, , mehr Fortbildung unserer Lehrkräfte, mehr Studienangeboten für Software-Entwickler und für Informatik als Querschnittsfach. Bildung „made in Bayern“ ist und bleibt das **beste Rüstzeug für unsere Jugend.**

- Wir starten mit den Verbänden der bayerischen Wirtschaft eine **„Transformationsoffensive Digitalisierung“** - für Weiterbildungen auf allen Ebenen des mittelständischen Unternehmens.

– **Wir investieren dort, wo in der digitalen Welt die Musik spielt:** in Künstliche Intelligenz, Assistenzrobotik, 3D-Druck, intelligente Hardware -

  und natürlich in IT-Sicherheit. Mit unserem **Masterplan BAYERN DIGITAL II** entwickeln wir unsere **Strategie für Cybersicherheit** weiter: mehr Forschung für die IT-Sicherheit, modernste Ausstattung für unsere Polizei, Ausbau der Ermittlungseinheiten.

Noch ein **konkretes regionales Beispiel:** Wir in der Bayerischen Staatsregierung unterstützen auch, dass rund um die Universität der Bundeswehr ein **Cybercluster in München** entsteht. Dazu gehört unter anderem:

- Ab Januar 2018 startet hier der **Studiengang Cybersicherheit**. Und:

- Auf dem Campus wird eine neue **Zentrale Stelle für Informationstechnik** gebaut.

Meine Damen und Herren,

unsere bayerische Strategie für Cybersicherheit ist **kein Luxus,** sondern folgerichtig. Der Staat legitimiert sich, indem er **Recht und Sicherheit garantiert**. Wir in Bayern, wir in der Bayerischen Staatsregierung sind uns dieser Verpflichtung sehr bewusst. Unser Credo heißt **„Sicherheit durch Stärke“**. Das gilt in der virtuellen Welt genauso wie auf öffentlichen Plätzen.

Außerdem ist uns klar: Nur mit Cybersicherheit können die **bayerischen Unternehmen ihre Stärken auch in Zukunft auf den Weltmärkten ausspielen.**

Anrede!

Ich habe es oben schon angedeutet: Beim Thema Cybersicherheit ist eine **enge Zusammenarbeit ganz wichtig.** Mit Zusammenarbeit meine ich dabei aber **nicht nur den Staat, die Politik, die Behörden.** Bei der **Cybersicherheit** brauchen wir auch das Engagement der **Wissenschaft, der IT-Unternehmen und der Anwender** in den Unternehmen. **Cybersicherheit ist eine Aufgabe für unser ganzes Gemeinwesen.**

Liebe Organisatoren des Cyber-Dialogs,

ich danke Ihnen daher sehr herzlich, dass Sie hier und heute die **Könner und Vordenker aus diesem Bereich zusammenbringen**. Solche Foren sind ganz wichtig, um gemeinsam stark zu sein und gemeinsam das Ziel **"Sicherheit im Netz" zu erreichen!**

Ich wünsche Ihnen in diesem Sinne **viel Erfolg** für den weiteren Verlauf der Tagung!