Behörden Spiegel
newsletter
Netzwerk Sicherheit

Nr. 433 Berlin und Bonn 19. Dezember 2012 ISSN 1867-2000

Meldungen

Polizeigesetz in Diskussion

(BS) Das geplante Polizeigesetz in Sachsen-Anhalt sieht mehrere neue Zugriffsrechte vor, die zu Diskussionen führen. So sollen zukünftig etwa im Falle eines Sprengstoffanschlages Telefonate unterbrochen werden dürfen, eingelieferte Betrunkene in der Zelle gefilmt werden oder auch unter bestimmten Umständen die Möglichkeit eines Bluttests auf HIV oder Hepatitis B und C möglich sein.

Das Netz steht

(BS) "Nach Jahren der Planung und konkreter Vorbereitungen, aber auch nach Rückschlägen und neuen Anläufen ist das digitale Funknetz in Schleswig-Holstein jetzt fertig und in Funktion", so die Meldung aus dem schleswig-holsteinischen Innenministerium. Alle Behörden und Organisationen mit Sicherheitsaufgaben (BOS) wie Polizei, Feuerwehr, Rettungsdienste oder THW können ihre Kommunikation von analog auf digital umstellen. Während die Landespolizei bereits im Probebetrieb digital funkt, werden die anderen Organisationen voraussichtlich ab 2014 nachziehen. "Das Netz steht", sagte Schleswig-Holsteins Innenminister Andreas Breitner heute in Kiel. 77 Funkmasten mussten neu gebaut werden, 84 bestehende Masten und Anlagen wurden unter der Leitung von Dataport, dem landeseigenen IT-Dienstleister, nachgerüstet.

Inhalt/Themen

Salafistische Spur gilt als sicher

(BS) Als vor einer Woche ein Schüler eine blaue Tasche meldete, die ihm auffällig auf dem Gleis 1 des Bonner Hauptbahnhofes schien, wurde rasch und professionell reagiert. Der Hauptbahnhof Bonn war innerhalb kürzester Zeit geräumt und die Sicherheitskräfte begaben sich ans Werk. Danach begann allerdings ein Ermittlungswirrwar, das erneut ein erschreckendes Bild auf die Parallelität und Konkurrenz von Sicherheitsbehörden wirft.

Es waren die Bonner Ermittler des Staatsschutzes, die sofort an der vermutlich richtigen Stelle waren, als sie vorrübergehend Omar D. in Gewahrsam nahmen. Auch der Komplize Abdirazka B. war schnell ermittelt. Beide haben Verbindungen zu den islamistischen Al-Shabaab-Milizen in Somalia. Sie sollen zudem eine Bonner Gruppe namens "Al Shabaab" geführt haben. Der schnelle Zugriff galt vielen wohl als zu rasch. Zudem konnte sich kein Nachweis einer terroristischen Tat ermitteln. So wurde der Verdächtige Omar D. wieder auf freien Fuß gelassen. Mittlerweile sucht ihn die Bundesanwaltschaft.

Offensichtlich waren politische Kräfte im Spiel, als es um die Interpretation des mittlerweile als eindeutig identifizierten terroristischen Anschlagsversuchs mit einer gefährlichen Bombe ging. Denn es dauerte drei Tage, bis nicht nur die Ermittlungsergebnisse vorlagen, sondern auch die Politik bereit war einen islamistischen Anschlagsversuch zu identifizieren. Warum diese Zurückhaltung? Winfried Bosbach, CDU-Innenpolitiker aus dem Bundestag, hatte von Anfang an darauf getippt und er lag richtig.

War ein islamistischer Terroranschlag nicht gewünscht? NSU- und NPD-Verbot standen im Wege? Warum müssen drei Tage nach einem Anschlag vergehen, um klare Indizien, identifizierte Täter und mögliche Motive, Racheakt der salafistischen Szene aufgrund des Einsatzes der Bonner Polizei vor drei Monaten im Ortsteil Lamersdorf, zu nennen.

Geradezu unverständlich wirkt der Konflikt zwischen dem Bonner und Kölner Polizeipräsidium. Die Bonner sind mit 150 islamistischen gewaltbereiten Tätern bundesweit gut ausgestattet. Nach Ulm und Hamburg herrscht hier eine salafistische Extremistenszene. Der Organisationsplan des NRW-Innenministeriums sieht bei Abwehrmaßnahmen gegen terroristische Anschläge vor, dass das Polizeipräsidium Köln in solchen Fällen ein Lagezentrum einrichtet. Hier sind Spezialisten gebündelt, doch die Kenntnisse über einzelne Personen, ihr Verhalten und ihre Bewegungen liegen in Bonn. Es mag ja sinnvoll sein bei Großlagen die großen Präsidien in Stellung zu bringen, doch salafistischer Extremismus ist in Bonn ein Alltagsthema und der Staatsschutz ist da nahe dran. Jedenfalls hat die Führung durch das Lagezentrum in Köln nicht optimal funktioniert.

Und wieso muss auf Videoaufnahmen aus einem McDonalds zurück gegriffen werden? Es sind die Aufnahmen, die zur Täterüberführung maßgeblich beitragen werden. Das Gleis 1 des Bonner Hauptbahnhofes wurde zwar videoüberwacht, die Kameraeinstellung war auf den Notruf gerichtet, aber es fand keine Aufzeichnung statt. Welchen Sinn machen Videoaufnahmen, wenn sie nicht gespeichert werden. Völlig offen ist auch noch die Frage im Streit zwischen Bundespolizei und Deutscher Bahn, ob die Speicherkapazität bei der Bahn für eine Aufzeichnung vorhanden war, ob die Bundespolizei dies jemals verlangt hatte und letztlich ob die Kameras wohlmöglich defekt waren. Solcherlei Details tun sich erst im Ernstfall auf!

Mehr Videoüberwachung sinnvoll

(BS) Der grüne Bundestagsabgeordnete und Experte für Innere Sicherheit, Wolfgang Wieland, brachte es auf den Punkt. Was bringt die Videoüberwachung, wenn die Bilder nicht aufgezeichnet werden. Ihre eindeutige nachweisbare präventive Maßnahme können sie dann nicht entfalten. Eines ist doch völlig klar, kriminelle Delikte oder gar terroristische Anschläge vermögen sie nicht zu verhindern, doch die Wahrscheinlichkeit einer schnellen Aufklärung und Identifizierung der Täter kann präventive Wirkung zeigen. Es ist doch ein übertriebener Reflex, zur Sicherung vermeintlicher Bürgerrechte eine umfangreichere Videoüberwachung von öffentlichen Räumen nicht zulassen zu wollen. Die gemachten Aufnahmen von Videokameras im öffentlichen Raum unterliegen den Datenschutzbestimmungen, ihre Auswertung und auch Speicherdauer ist streng geregelt. Die Aufnahmen können aber zu einer schnelleren Tataufklärung und Täteridentifizierung führen. Unschuldige sind davon völlig unbehelligt.

Gerade der versuchte Terroranschlag auf dem Bonner Hauptbahnhof zeigt ja das ganze Dilemma. Nur durch Videoaufnahmen eines privaten Schnellrestaurants konnte zumindest vermutlich ein Täter identifiziert werden. Das Schnellrestaurant hat die Videokameras aber nicht wegen der Abwehr terroristischer Anschläge installiert, sondern zum Schutz seiner Räumlichkeiten vor Diebstahl und Randale. Jetzt streiten sich Deutsche Bahn und Bundespolizei, warum auf dem wichtigsten Gleis 1 des Bonner Hauptbahnhofes die Aufnahmen nicht gespeichert wurden. Es ist illusionär zu glauben, dass jemand in einer Zentrale in Köln 20 Bildschirme gleichzeitig verfolgen kann und verdächtige Objekte identifiziert. Nur die Aufzeichnung der Aufnahmen bringt Ergebnisse. Man kann die Zeitspanne der Aufzeichnung bzw. die Löschung der gemachten Aufnahmen sinnvoll limitieren, auf 12, 24 oder 48 Stunden. Sollte es jedoch dann aber zu einem Vorfall kommen, ist die Polizei in der Lage unmittelbar nach einer Gewalttat oder einem Anschlag die Videoaufnahmen auszuwerten.

Es spricht also doch viel für mehr Videokontrolle im öffentlichen Raum. Sie dient ja nur der Rückfallposition für den Fall eines Ereignisses, das die Polizei dann ermitteln muss.

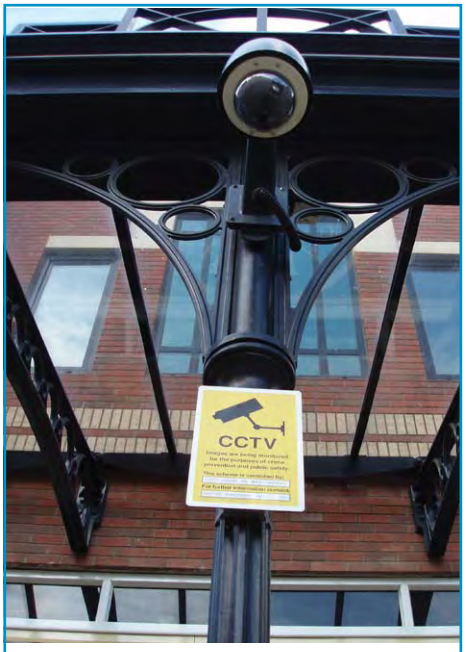
Welche Aufregung macht sich da breit? Um was für Bürgerrechte soll es dabei gehen, wenn zeitlich befristet Videoaufnahmen für den Fall eines besonderen Vorkommnisses gespeichert werden. Es ist ja überhaupt nicht vorgesehen, diese seriell auszuwerten. Das geschieht aber mittlerweile mit Hilfe der Gesichtserkennung bei Facebook. Hier kann jeder individuelle Nutzer eine Aufnahme eines an ihm vorbeigehenden Passanten mit seinem Smartphone machen und per Internetabfrage feststellen, wer die Person ist und seine meist ja dann noch freiwillig eingestellten Daten identifizieren. Hier ist Handlungsbedarf der Justizpolitik angesagt. Doch hier herrscht derzeit Schweigen.

Es ist überhaupt befremdlich, wie derzeit die Justizpolitik mit der hiesigen Polizei umzugehen pflegt. Es macht ja gerade den Eindruck, als unterstelle die Justizministerin und auch mancher Landesjustizminister der Polizei die böse Absicht, wenn sie einmal an Videoaufnahmen oder andere Daten gekommen sei, würde sie diese gnadenlos auswerten und verwenden, doch es handelt sich hier um Beamte, die streng gebunden an Datenschutzrichtlinien sich orientieren müssen. Zudem: Die Möglichkeit eines Missbrauchs besteht auch bei der Dienstwaffe, doch niemand unterstellt, dass ein Polizist mit seiner Waffe aus dem Polizeipräsidium herausgeht und damit wild in der Gegend rumballert. Warum sollte er das nun anders bei ihm zur Kenntnis gekommenen Daten tun?

Das Vertrauen in die Mitarbeiter der Sicherheitsbehörden muss gestärkt werden, nicht ständig durch immer neue Verdachtsmomente und mögliche Missbrauchsmöglichkeiten unterminiert werden.

Wir sollten da mal dringend auf dem Teppich bleiben! Das gilt meiner Ansicht nach für die Justiz. Ihre Urteile sind in der Öffentlichkeit immer weniger vermittelbar und mancher Richterspruch mit Bezug zur Rockerkriminalität lässt da doch viele Fragen offen. Hier sind die Baustellen, um die sich die Bundesjustizpolitik kümmern sollte! Klartext gesprochen: Gibt es wohlmöglich Richter und Staatsanwälte, die aus durchaus nachvollziehbarem Eigenschutz Urteile bei Verfahren gegen Hells Angels finden, die nicht die Konsequenz zeigen, die das Recht eigentlich zuließe? *R. Uwe Proll*

Chefredakteur Behörden Spiegel



Die britische Stadt Middlesbrough hatte als erste in Europa eine umfassende Videoüberwachung zum Schutz der Bevölkerung eingeführt. Grund für diese Maßnahme war der signifikante Anstieg der Kriminalität, nachdem die bedeutendste Fabrik der Stadt schloss. Die hohe Arbeitslosigkeit, verbunden mit einem Antsieg von Gewaltdelikten unter Alkoholeinfluß, ließ die Stadt immer weiter in das soziale Abseits sinken, so dass sich auch kaum neue Unternehmen in dieses "Milieu" locken ließen. Die Geschäftszeilen der Innenstadt drohten ebenfalls zu verwaisen. Durch die Videoüberwachung konnte diese Spirale aufgefangen werden, so dass die Bewohner Middlesbroughs sie durchweg als positiv empfanden. Foto: BS/D. Frank

Beispielhaftes Schulungskonzept an Elektrofahrzeugen

(BS) Landes- und Bundesregierung fördern mit Blick auf die Klimaschutzziele die Elektromobilität, im Jahr 2020 sollen bundesweit eine Million Elektrofahrzeuge im täglichen Verkehr unterwegs sein.

"Mit den steigenden Zulassungszahlen erhöht sich aber auch das Risiko, dass Elektrofahrzeuge an einem Unfall oder sogar an einem schweren Unfall beteiligt sein können", sagte der baden-württembergische Innenminister Reinhold Gall in Stuttgart. Deshalb habe die Projektgruppe "POLIZEI-ONLINE - Notfallkonzeption Elektromobilität" ein bundesweit einmaliges Schulungsprogramm für Polizei, Feuerwehr und Rettungsdienste entwickelt, das auch das richtige Vorgehen bei Unfällen mit Hybrid- und Wasserstofffahrzeugen umfasse.

Zwar seien die Elektrofahrzeuge nach Angaben der Fahrzeugindustrie sicherer als herkömmliche Fahrzeuge. Jedoch würden die neu entwickelten und eingebauten Fahrzeugkomponenten wie die Fahrzeugbatterien oder andere Hochvoltkomponenten ein andersartiges Gefahrenpotenzial bergen, wenn beispielsweise der Kühlkreislauf oder die Hochvoltkabel beschädigt werden.

"Wenn Polizei und Feuerwehr durch das Schulungsprogramm ein Elektrofahrzeug frühzeitig erkennen, können diese möglichen Gefahren minimiert werden. Weiterhin vermindert fundierte Sachkenntnis das Risiko für die Einsatzkräfte und gewährleistet ein vorausschauendes und sicheres Vorgehen", betonte Gall.

Das Schulungsprogramm führe mit umfassenden Texten, Übersichtsskizzen und Bildmaterial in die Thematik ein, weise auf die verschiedenen möglichen Gefahren hin und vermittle außerdem das taktisch richtige Vorgehen. Es sei vorgesehen, dass alle Einsatzkräfte, die unmittelbar mit der Unfallaufnahme, der Rettung von Personen, der Brandbekämpfung und der Bergung von Fahrzeugen betraut seien, dieses Lernprogramm absolvierten.

"Baden-Württemberg nimmt mit diesem Programm bundesweit eine Vorreiterrolle ein. Ich gehe davon aus, dass auch bei Behörden in anderen Bundesländern ein großes Interesse an dem von unserer Projektgruppe entwickelten Programm besteht", so Gall weiter.

Aktuell liege sogar schon eine Übernahmeanfrage der Interkantonalen Polizeischule in Hitzkirch/Schweiz für den Einsatz in der Schweizer Polizei vor. Für die Polizei des Landes werde es im internen elektronischen Informationssystem POLIZEI-ONLINE abrufbar sein.

An der Projektgruppe beteiligt sind:

- das Innenministerium Baden-Württemberg
- die Landesagentur für Elektromobilität und Brennstoffzellentechnologie (e-mobil BW GmbH)
- die Landesfeuerwehrschule in Bruchsal
- der TÜV Süd
- das Medienzentrum POLIZEI-ONLINE der Polizeiakademie in Freibur
- das Weiterbildungszentrum Ulm
- die Forschungsstelle für Brandschutztechnik am Karlsruher Institut für Technologie

Organisierte Kriminalität im Internet

(BS) "Cyber Crime ist eigentlich nichts Neues. Es ist nur eine neue Definition von Kriminalität, die mit anderen Mitteln verübt wird." Peter Vahrenhorst, Cyber Crime Kompetenzzentrum des Landeskriminalamtes (LKA) Nordrhein-Westfalen, eröffnete im September dieses Jahres das Diskussionsforum "Herausforderung Cyber Crime" des Behörden Spiegel in Kooperation mit BITKOM auf der security essen 2012.

Delikte wie Warenkreditbetrug, Beleidigung, Mobbing, Kinderpornographie, Schutzgelderpressung und Wirtschaftsspionage würden im Internet nur "anders" ausgeführt.

Das Internet habe aber auch neue Deliktsfelder entstehen lassen: Skimming, Phishing, Carding, Schadsoftware, Botnetze, DDoS-Attacken, Account Takeovers und die Underground Economy seien hierfür nur einige Beispiele. "Diese neuen Phänomene entwickeln sich stetig weiter, sie sind flexibel, dynamisch und vor allem anonym", so Vahrenhorst.

Außerdem hätten sich mit dem Internet neue Tätertypologien ergeben. "Im Internet herrscht ein großes Gefahrenpotenzial.

Es herrscht aber leider auch ein hohes Dunkelfeld über begangene Straftaten und Delikte", so Vahrenhorst weiter. Daher sei der optimale Informationsaustausch sowie Zusammenarbeit und Kooperation zwischen der Wirtschaft und Industrie sowie den Behörden und Organisationen mit Sicherheitsaufgaben das Ziel zur Bekämpfung der Internetkriminalität. Die Polizei sehe dabei vor allen Dingen zwei großen Herausforderungen.

"Wir brauchen eine flächendeckende Grundkompetenz hinsichtlich Cyber Crime bei der Polizei, aber eben auch spezielle Fachkompetenz", so Vahrenhorst.

16. Europäischer Polizeikongress

(BS) Im Rahmen des 16. Europäischen Polizeikongresses, der am 19. und 20. Februar 2013 unter dem Titel "Schutz und Sicherheit im digitalen Raum" im Berliner Congress Center (bcc) tagt, werden die Gefahren im Internet und die polizeilichen Maßnahmen in mehreren Fachforen diskutiert. Ein Forum widmet sich der "Organisierten Kriminalität im Internet", ein weiteres der "Digitalen Forensik". Der "Europäischer Polizeikongress" ist eine international ausgerichtete Fachkonferenz, die sich als Informationsplattform für Polizeien, Sicherheits- und zivile Behörden versteht. Weitere Informationen und Anmeldung auf der Page: www.european-police.eu

Der Zwang des Faktischen

(BS) Unter dem Titel "IT und Polizei: Anforderungen an die Informationstechnologie und Herausforderung Cyber Crime" fand in Wiesbaden die Abschlussveranstaltung der Reihe "Polizeitage 2012", einer Kooperation der Gewerkschaft der Polizei (GdP) und des Behörden Spiegel, statt.

In seiner Eröffnung stellte Horst Westerfeld, Staatssekretär im Hessischen Ministerium der Finanzen sowie Bevollmächtigter der Hessischen Landesregierung für E-Government und Informationstechnologie, zunächst die auch von der Ständigen Konferenz der Innenminister und Innensenatoren der Länder (IMK) geforderte Kompetenz gegen Internetkriminalität in den Vordergrund. "Es müssen Kompetenzen zusammengelegt werden, damit die Polizei ihre Aufgaben im Cyberraum erfüllen kann", so der Staatssekretär.

Das Netz sei ein Raum der viele verschiedene Angriffspunkte biete. Es gäbe dort schon jetzt viel Kriminalität, der die Polizei entgegentreten müsse. "Dabei stehen wir jedoch noch am Anfang der Möglichkeiten von Cybercrime. Wir brauchen mehr Ressourcen und mehr Kompetenz diesem entgegenzutreten", so Westerfeld.

Das Netz böte aber eben auch riesige Chancen. Ohne das Netz sei keine Wirtschaftsentwicklung mehr möglich. Die physikalischen Netze seien für die Wettbewerbsfähigkeit eines Wirtschaftsstandorts wichtig. Daher müsse der Sicherung der Netze auch Priorität gelten.

Bernhard Lammel, Abteilungsleiter 3 "IuK-Einsatz und Cybercrime" im Landeskriminalamt Hessen (HLKA), betonte, dass Cybercrime kein Nischenthema mehr sei und auch kein exklusives Spezialistenthema. Cybercrime sei Alltag, der jeden betreffe.

Nach der Neuorganisation im HLKA arbeiteten in der neuen Abteilung IuK Einsatz und Cybercrime derzeit 80 Personen. Unter dem Motto "Vernetzte Kompetenz im Team" sei die neue Abteilung gut gestartet. Dennoch plane man in Hessen bereits weiter. Mit dem Projekt "System 120" wolle man die Kompetenz im Landeskriminalamt personell aufstocken und die guten Einzelaktionen in Hessen systematisch zusammenbringen. "Wir müssen eine gemeimsame Linie in Hessen finden", so Lammel. Dazu bedürfe es u.a. der Fachkompetenz in der polizeilichen Fläche und dem Ausbau vertikaler und horizontaler Kompetenz. "Eine Grundkompetenz Cybercrime schon in der polizeilichen Ausbildung zu erlernen, ist zwingend notwendig. Da müssen wir ran", sagte Lammel.

Moderiert von Behörden Spiegel-Chefredakteur R. Uwe Proll diskutierten Nancy Faeser, Innenpolitische Sprecherin der SPD-Fraktion im Hessischen Landtag, Alexander Bauer, MdL, Innenpolitischer Sprecher der CDU-Fraktion im Hessischen Landtag, Dr. Frank Blechschmidt, MdL, FDP, Mitglied im Innenausschuss und Jörg Bruchmüller, Landesvorsitzender Hessen der Gewerkschaft der Polizei, in Wiesbaden über die Herausforderungen der Internetkriminalität für die Polizei.

Nach Nancy Faeser seien die Möglichkeiten und Gefahren des Netzes in der Gesellschaft angekommen. So würde etwa an Schulen bereits frühzeitig an der Medienkompetenz gearbeitet. In der Polizei sei die Herausforderung Cybercrime dagegen noch nicht unbedingt angekommen. Es seien hier erweiterte Möglichkeiten für die Polizei bei Facebook notwendig. "Die Polizei muss sich hinsichtlich der Fahndung und der Strafverfolgung dem Cyberraum anpassen. Die Politik rennt dort noch hinterher", so Faeser. Doch der Bürger komme bei Straftaten als erster zur Polizei. Daher sei eine breite Fortbildung in der polizeilichen Facharbeit notwendig. Dies gelte aber auch bei Richtern. Viele Verfahren würden aus Kapazitätsmangel bei Richtern eingestellt. Zudem werde eine Partnerschaft mit Privaten gebraucht.

Wie Dr. Blechschmidt betonte, müsse man aber auch Transparenz für sich selbst schaffen, um beim Thema Internet und Cybercrime mitreden zu können. Es gehe hier um die Eigenverantwortung, die gesellschaftliche Verantwortung und letztlich auch um das Finden von Grenzen, etwa bei Facebook. Der Polizei müsse Facebook

Staatssekretär Horst Westerfeld bei den Polizeitagen in Wiesbaden. Foto: BS/Archiv

für ihre polzeiliche Arbeit zur Verfügung stehen. "Verbrechen und Verbrecher entwickeln sich weiter. Aber die Cybercrime entwickelt sich schneller als die Polizei", gab Dr. Blechschmidt zu bedenken.

Die Voratsdatenspeicherung sei in diesem Feld ein "Zwang des Faktischen", so Dr. Blechschmidt. Man dürfe der Polizei die Möglichkeit der Ermittlung nicht nehmen. Die Voratsdatenspeicherung müsse in Grenzen und bei verantwortungsvollem Umgang damit möglich sein. Aber auch sie sei kein Allheilmittel. Der rechtliche Rahmen müssen sich ebenso entsprechend weiterentwickeln.

"Wir müssen der Polizei mit Maß und Ziel Instrumente geben", fügte Bauer hinzu. Dabei lohne sich auch der Blick auf die europäische Ebene. Im Vergleich zu anderen europäischen Ländern habe Deutschland in manch einer Hinsicht Nachholbedarf.

Laut Bruchmüller sei die Herausforderung Cybercrime ein strukturelles Problem. "Wir brauchen nicht nur eine Linie in Deutschland, sondern eine Linie weltweit", so Bruchmüler. Flexible Strukturen, Portabilität und eine Nachhaltigkeit im Fundus Fachwissen seien notwendig. Zudem müsse aus dem Nebeneinander zwischen Polizei und Wirtschaft ein Miteinander werden.

"Wir laufen der Lage derzeit hinterher. Es ist eine Ohnmacht vorhanden. Dennoch können wir vieles verbessern. Außerdem machen wir noch nicht alles, was wir machen könnten", so Bruchmüller in Einstimmigkeit der Diskussionsrunde abschließend.

Stärkung der Zusammenarbeit durch Übung

(BS) Am 5. und 6. Dezember 2012 haben Luxemburg, das Saarland, Rheinland-Pfalz, das Königreich Belgien und Frankreich eine grenzüberschreitende Krisenmanagementübung für den Fall eines Unfalls im französischen Kernkraftwerk Cattenom durchgeführt.

Hierbei handelte es sich um den zweiten Teil einer Reihe von drei aufeinanderfolgenden strategischen Übungen, die auf drei miteinander zusammenhängenden Szenarien basieren.

Während der erste Teil den Beteiligten die Möglichkeit gab, nicht nur die Ansprechpartner in den verschiedenen Regionen, sondern auch Abläufe und Entscheidungsmodalitäten in den einzelnen Ländern besser kennenzulernen, gab dieser zweite Teil Gelegenheit, die nationale und grenzüberschreitende Zusammenarbeit weiter zu verstärken.

Der permanente Austausch zwischen den Leitern der Krisenstäbe der verschiedenen Regionen ermöglichte eine gute Koordinierung sowohl der vorgesehenen Maßnahmen als auch der diesbezüglichen Kommunikation.

Während dieses zweiten Teils, bei dem die Erweiterung der Notfallmaßnahmen im Mittelpunkt stand, konnten die Entscheidungen auf der Grundlage des während des ersten Teils aufgebauten Vertrauens getroffen werden.

Die Nutzung leistungsfähiger Kommunikationsmittel (Internet, Audiokonferenzen ...) sowie die Verwendung des Englischen als gemeinsame Kommunikationssprache ermöglichte kürzere Reaktionszeiten und damit schnellere Entscheidungsabläufe.

Die Übung ist demnach ihrer wichtigsten Aufgabe, nämlich der Stärkung der Zusammenarbeit zwischen den Krisenstäben, gerecht geworden, so dass bei tatsächlichen Problemen, unabhängig davon, ob es sich um einen Störfall im Kernkraftwerk Cattenom oder um andere Ereignisse wie Natur- bzw. Umweltkatastrophen in der Großregion handelt, angemessen reagiert werden kann.

Während des dritten und letzten Teils der Übung, der für Frühjahr 2013 vorgesehen ist, soll das, was während des ersten Teils begonnen und während des zweiten Teils vertieft wurde, gefestigt werden.

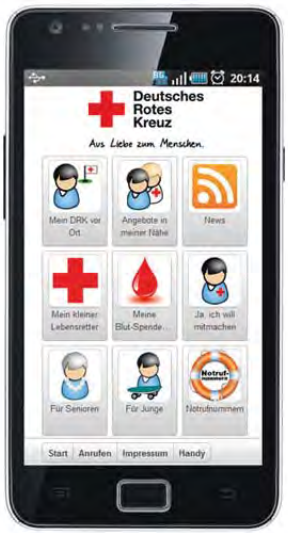
Die App für Notfälle

(BS) In wenigen Schritten zum richtigen Ansprechpartner: Das Deutsche Rote Kreuz stellt ab sofort die Smartphone-App "MeinDRK" zur Verfügung. Die kostenfreie Anwendung gibt einen umfassenden und aktuellen Überblick über rund 22.000 Angebote und Dienstleistungen des Roten Kreuzes. Mit dem "Kleinen Lebensretter" haben Nutzer der App zudem jederzeit eine Anleitung zur Leistung von Erster Hilfe in Notfallsituationen griffbereit.

Das übersichtliche Menü der Startseite bietet eine schnelle und nutzerorientierte Übersicht der DRK-Angebote. Über "Mein DRK vor Ort" lassen sich postleitzahlengenau sämtliche Leistungen und Einrichtungen des DRK in der näheren Umgebung abrufen. Ein weiterer Klick führt den App-Nutzer zum richtigen Ansprechpartner, liefert Infos zu Kosten, Öffnungszeiten und weiteren Informationen der entsprechenden Einrichtung. Wer nach einer konkreten Lösung für sein Problem sucht, kommt mit dem Icon "Angebote in meiner Nähe" am schnellsten zum Ziel.

Das Tool listet die Ergebnisse der Postleitzahlensuche nach speziellen Lösungsangeboten auf, beispielsweise in der Altenhilfe oder Gesundheitsvorsorge.

Wie man in lebensbedrohlichen Situationen helfen kann, zeigt der "Kleine Lebensretter": Er beschreibt anschaulich Erkennungsmerkmale und Sofortmaßnahmen zum Beispiel bei Herzinfarkt, Schlaganfall oder einer Vergiftung. Außerdem kann man sein Erste Hilfe-Wissen unterwegs auffrischen. Der "Kleine Lebensretter" ist offline verfügbar und benötigt keine Netzverbindung. Eine zusätzliche Telefonliste mit Notrufnummern der Rettungsdienste, regionalen Giftnotrufzentralen, dem Apothekennotruf oder psychologischen Beratungsstellen liefert die passende Anlaufstelle für jeden Notfall.



Die Funktion "Für Senioren" bildet Angebote in der näheren Umgebung für ältere Menschen ab – zum Beispiel in Sachen Beratung, Pflege, Bewegung oder hauswirtschaftliche Hilfen. Nach dem gleichen Prinzip finden Kinder, Jugendliche und junge Familien im Tool "Für Junge" Infos rund ums Freiwillige Soziale Jahr, Babysitterkurse oder Schwangerschaftsberatung.

Wer im Deutschen Roten Kreuz aktiv werden will, findet neben dem Blutspendekalender den richtigen Ansprechpartner für ein Engagement im Bundesfreiwilligendienst, als Helfer im Katastrophenschutz oder im Jugendrotkreuz. Im News-Bereich informiert das DRK regelmäßig über Auslands- oder Katastropheneinsätze und versorgt die Nutzer mit aktuellen Gesundheitstipps.

"MeinDRK" steht für iPhone- und Androidgeräte im Apple AppStore und im Google Play-Store zur Verfügung.

Wer die Rotkreuz-App auf sein Smartphone laden will, ruft die Webadresse für Android: DRK-intern.de/rotkreuz-app/google-play oder für iPhone: DRK-intern.de/rotkreuz-app/iphone auf.

Safety and Security in Cyber-Space

Schutz und Sicherheit im digitalen Raum

Polizei in sozialen Netzwerken – ePolice – Ausrüstung und Ausstattung

16. Europäischer Polizeikongress

19.–20. Februar 2013, Berliner Congress Center

www.european-police.eu

Dienstag, 19. Februar 2013

08:00 **Eröffnung der Ausstellung**

08:20 **Eröffnung des 16. Europäischen Polizeikongresses**
R. Uwe PROLL, Chefredakteur und Herausgeber des Behörden Spiegel, Berlin/Bonn

08:30 **Konventionen zur Freiheit und Sicherheit im Internet**
Dr. Hans-Peter FRIEDRICH, Bundesminister des Innern, Berlin

09:00 **Die Französisch-Deutsche Sicherheitspartnerschaft – 50 Jahre Élysée-Vertrag**
Manuel VALLS*, Innenminister Frankreich, Paris

09:30 **Beitrag aus der Wirtschaft**
N.N., AGT International

10:00 **Operative Tätigkeit im Rahmen der neuen Aufgaben des EC3 – Strafverfolgung in Sozialen Netzwerken**
Troels OERTING, Assistant Director, European Cybercrime Centre (EC3), Europol, Niederlande, Den Haag

10:30 Kaffee-Pause

11:00 **Panel I-VIII**

12:30 Lunch

13:30 **Das INTERPOL DIGITAL CRIME CENTRE im INTERPOL GLOBAL COMPLEX for INNOVATION – IGCI Singapur**
Noburo NAKATANI, Exekutivdirektor des IGCI, INTERPOL, Singapur

14:00 **Beitrag aus der Wirtschaft**

14:30 **Cyber Mobilization**
Dr. Hans-Georg MAASSEN, Präsident Bundesamt für Verfassungsschutz, Köln/Berlin

15:00 Kaffeepause

15:45 **Beitrag aus der Wirtschaft**

16:15 INITIALVORTRAG: **Aktivitäten der europäischen Polizeien in Sozialen Netzwerken**
Dr. Sebastian DENEF, Fraunhofer Institut für Angewandte Informationstechnik FIT

16:45 HIGH-LEVEL DEBATE **Polizei in Sozialen Netzwerken**
Moderation:
Dr. August HANNING, Präsident des Bundesnachrichtendienstes (BND) a. D., Sts a. D. und Programm- & Herausgeberbeirat des Behörden Spiegel, Berlin
Teilnehmer:
Axel BROCKMANN, Polizeipräsident Hannover
Michael HARTMANN, MdB, Innenpolitischer Sprecher der SPD-Bundestagsfraktion, Berlin
Dieter SCHNEIDER, Präsident Landeskriminalamt Baden-Württemberg, Stuttgart

17:45 **Beitrag aus der Wirtschaft**

18:15 **Exkurs Polizei in sozialen Netzwerken: Australien – Projekt eyewatch**
Joshua J. MAXWELL, Chief Inspector, Manager Project eyewatch, New South Wales, Australia

18:45 **Abendempfang**

Mittwoch, 20. Februar 2013

08:00 **Eröffnung der Ausstellung**

08:20 **Fortführung der Konferenz**

08:30 **Justizielle Zusammenarbeit im Bereich der Strafverfolgung von Verbrechen im Cyber-Raum**
Michèle CONINSX*, Präsidentin des Eurojust-Kollegiums, Eurojust, Niederlande, Den Haag

09:00 **Sichere IT-Infrastrukturen bei der Polizei**
Dr. Dieter ROMANN*, Präsident Bundespolizeipräsidium, Potsdam

09:30 **Beitrag aus der Wirtschaft**
Dr. Ralf HINKEL, Vorstand Mobotix AG, Langmeil

09:50 **Lagebild Cyber Crime**
Jürgen MAURER, Vizepräsident Bundeskriminalamt, Wiesbaden

10:20 Kaffeepause

10:40 **Beitrag aus der Wirtschaft**

11:00 DISKUSSIONSRUNDE DER LANDESINNENMINISTER
Moderation:
R. Uwe PROLL, Chefredakteur und Herausgeber des Behörden Spiegel, Berlin/Bonn
Teilnehmer:
Lorenz CAFFIER, Minister des Innern, Mecklenburg-Vorpommern, Schwerin
Frank HENKEL, Senator für Inneres und Sport, Berlin
Joachim HERRMANN, Bayerischer Staatsminister des Innern, München
Ralf JÄGER*, Minister für Inneres und Kommunales, Nordrhein-Westfalen, Düsseldorf
Dr. Dietmar WOIDKE, Minister des Innern, Brandenburg, Potsdam

12.15 **Verleihung des 1. Zukunftspreises Polizeiarbeit – Themengebiet: Soziale Netzwerke**

12:30 Lunch

13:30 **Beitrag aus der Wirtschaft**
David MÜLLER, Key Account Manager, Panasonic Computer Products Europe, Wiesbaden

13:50 **Digitale Bedrohungen für Regierung und Wirtschaft**
Klaus-Dieter FRITSCHE, Staatssekretär, Bundesministerium des Innern, Berlin

14:20 **Beitrag aus der Wirtschaft**

14:40 **Ausblick: Was plant die EU im Kampf gegen digitale Bedrohungen?**
Stefano MANSERVISI*, Generaldirektor Inneres, Europäische Kommission, Belgien, Brüssel

15:10 Kaffeepause

15:30 **Panel IX-XVI**

17:00 **Ende der Veranstaltung**

Moderation: Reimar Scherz, Programm- und Herausgeberbeirat, Behörden Spiegel, Bonn

*Referent angefragt

Goldsponsor: AGT International

Innovationspartner: PAN AMP

Bronzesponsoren: 3M, Capgemini, SCHÖNHOFER SALES AND ENGINEERING GMBH, TASER, Dräger, esri Deutschland, ORACLE, SS8, DPolG, rola, IBM, JitWatch GmbH, steria mummert consulting, bdk Bund Deutscher Kriminalbeamter

Silbersponsoren: MOBOTIX, Panasonic ideas for life

Mit Unterstützung von: Bundesministerium des Innern, Bundeskriminalamt, BUNDESPOLIZEI FEDERAL POLICE

Impressum

Herausgeber und Chefredakteur von "Behörden Spiegel Newsletter Netzwerk Sicherheit" und verantwortlich: R. Uwe Proll.

Redaktionelle Leitung: Patricia B. Linnertz. Redaktion: Benjamin Bauer, Hartmut Bühl (Brüssel), Franz Drey, Julian Einhaus, Jörn Fieseler, Dorothee Frank, Guido Gehrt, Carsten Köppl, Lora Köstler-Messaoudi, Gerd Lehmann. Redaktionsassistenz: Kerstin Marmulla (Bonn), Sonja Bechthold (Berlin). ProPress Verlagsgesellschaft mbH, Am Buschhof 8, 53227 Bonn, Telefon: 0049-228-970970, Telefax: 0049-228-97097-75, E-Mail: redaktion@behoerdenspiegel.de; www.behoerdenspiegel.de. Registergericht: AG Bonn HRB 3815. UST-Ident.-Nr.:DE 122275444 - Geschäftsführerin: Helga Woll.

Vorsitz Herausgeber- und Programmbeirat: Dr. August Hanning, Staatssekretär a.D.; Reimar Scherz, BrigGen. a.D. Der Verlag hält auch die Nutzungsrechte für die Inhalte von "Behörden Spiegel Newsletter Netzwerk Sicherheit". Die Rechte an Marken und Warenzeichen liegen bei den genannten Herstellern. Bei direkten oder indirekten Verweisen auf fremde Internetseiten ("Links"), die außerhalb des Verantwortungsbereiches des Herausgebers liegen, kann keine Haftung für die Richtigkeit oder Gesetzmäßigkeit der dort publizierten Inhalte gegeben werden.